

Toolkit for managing digital collections

Originally published - April 2023

**Updated with minor changes to introduction and presentation -
September 2024**

Digital Collections Toolkit Working Group

London Museum Documentation Network

Original content created by the London Museum Documentation Network is [licensed under a Creative Commons Attribution-NonCommercial 4.0 International License \(CC BY-NC 4.0\)](#)

The toolkit includes content quoted from the Spectrum collections management standard, under license from Collections Trust. This content is subject to Collections Trust's standard [licensing terms here](#). See the Introduction section for more information.

Contents

Toolkit for managing digital collections	1
I. Authors, editors and contributors.....	8
1. Introduction	11
1.1. About the toolkit.....	11
1.1.1 Foreword.....	11
1.1.2 How to navigate the toolkit.....	12
1.1.3 What is out of scope?.....	13
1.1.4. Who should use the toolkit?	13
1.2. Introduction to digital preservation.....	13
1.2.1. Why is digital preservation important?	13
1.2.2. Core principles of digital preservation	14
1.3. Definition of digital collection objects	15
1.3.1. Managing digital collection objects.....	16
2. Getting Started.....	21
2.1. First steps in safeguarding an existing digital collection	21
2.2. Develop a strategy for managing and digitally preserving your digital collection.....	22
2.2.1. A note on current cultural policy	22
2.2.2. Assess your museum's strategic readiness.....	23
2.2.3 Assess your museum's operational readiness.....	25
2.2.4. Assess the risks.....	25
2.2.5. Decide which standards and best practice models you wish to implement	26
2.2.6. Build a business case for developing organisational readiness	27
2.3. Setting up equipment and resource for managing digital preservation	27
2.3.1. Setting up a dedicated workstation	28
2.3.2. Setting up a digital quarantine environment.....	28
2.3.3. Staff roles and responsibilities.....	28
2.3.4. Resource requirements for digital preservation.....	29
3. Object entry.....	30
3.1. Spectrum suggested procedure	30
3.2. Preparing for Object entry (if known in advance)	31
3.2.1. Prepare for the arrival of the objects at your museum.....	31
3.3. Different methods of digital and physical entry	36
3.3.1. Virtual entry - unmanaged.....	36
3.3.2. Virtual entry - file transfer platform method.....	38
3.3.3. Physical digital storage method.....	39
3.3.4. Physical entry.....	40

3.4. Creating an entry record and receipt	40
3.4.1. Make a record of the objects as soon as they arrive.....	40
3.4.2. Check and note the objects' condition, and any associated risks	42
3.4.3. Processing newly-arrived objects.....	42
3.4.4. Tag the objects with a temporary label marked with the Entry number or Loan in reference number.	42
3.4.5. Record the first location of the objects.....	43
4. Acquisition and accessioning	44
4.1. Spectrum suggested procedure	44
4.2. Assessing potential acquisitions.....	46
4.2.1. Make a case for the proposed acquisition	46
4.2.2. Evaluate the proposal	48
4.3. Obtaining title and recording rights.....	48
4.3.1. Obtain title to the objects and written evidence of this.....	48
4.3.2 Record copyright or other associated rights if known.....	48
4.4. Receiving objects not already with you	49
4.4.1. Plan for the arrival of the objects.....	49
4.5. Processing new acquisitions.....	49
4.5.1. Label or mark each object, or group of objects, with a unique object number	49
4.5.2. Managing very large acquisitions	49
4.5.3. Record initial information about the acquisition and the objects acquired.....	50
5. Location and movement control	51
5.1. Spectrum suggested procedure	51
5.2. Identifying and describing locations	52
5.2.1. Give each display and storage location a unique name or number.	52
5.3. Recording locations of objects.....	53
5.3.1. Record the location of all objects	53
5.4. Moving objects	56
5.4.1. Obtain and record authorisation for all moves	56
5.4.2. Check the objects' condition to make sure they are fit to be moved.....	56
5.4.3. If transport is involved, establish, and agree the most appropriate means.....	56
5.4.4. Transport objects, and then confirm their safe arrival.....	57
6. Inventory	58
6.1. Spectrum suggested procedure	58
6.2. Checking you have core information.....	59
6.2.1. Do you have core information for every object (or group)?.....	59
6.3. Producing an inventory.....	63

6.4. Metadata	64
6.4.1. Technical metadata.....	64
6.4.2. Descriptive metadata	65
6.4.3. File headers	65
6.4.4. Metadata standards	65
6.4.5. Extracting metadata for use in documentation.....	66
6.4.6 Accessing complex metadata.....	66
7. Cataloguing.....	67
7.1. Spectrum suggested procedure	67
7.2. Creating catalogue records.....	68
7.2.1. Create a record for each object, or group of objects, accessible by object number	68
7.3. Recommended data structure for digital collections.....	84
7.3.1. Cataloguing recommendations for museums with a CMS and DAMS.....	84
7.3.2. Cataloguing recommendations for museums with a CMS but no DAMS	84
7.4. File and folder names	84
7.4.1. Rules for file/folder names.....	85
8. Object exit.....	87
8.1. Spectrum suggested procedure	87
8.2. Arrange for the objects to be at the agreed pick-up point at the agreed time	87
8.2.1. Different methods of digital and physical exit.....	87
8.2.2. Digital exit process.....	88
8.3 Update location records	92
8.4. Record information about the exit.....	92
9. Loans in (borrowing objects)	93
9.1. Spectrum suggested procedure workflow.....	93
9.2. Loan research.....	94
9.2.1. Make the case for borrowing the objects and obtain authorisation.....	94
9.3. Exchanging further information.....	95
9.3.1. Complete and send a facilities report to the lender	95
9.4. Agreeing the loan.....	95
9.4.1. Create and sign the loan agreement	95
9.5. Preparing to receive the loan.....	96
9.5.1. Schedule and prepare for the arrival of loaned objects.....	96
9.6. Monitoring the loan	96
9.6.1. Monitor and report the condition of the objects during the loan.....	96
9.7. Return and closure	96
9.7.1. Carry out a final condition report on the objects	96

9.7.2. Return the objects to the lender.....	97
10. Loans out (lending objects).....	98
10.1. Spectrum suggested procedure.....	98
10.2. Assessing the request.....	99
10.2.1. Consider the request.....	99
10.3. Requesting further information.....	100
10.3.1. Request further information from the borrower	100
10.3.2. Consider the request.....	100
10.4 Agreeing the loan.....	101
10.4.1 Record the final conditions of the loan and create the loan agreement.....	101
10.5. Preparing for the loan.....	102
10.5.1. Check and record, with images, the condition of objects for loan	102
10.5.2. Carry out any necessary conservation work, including bespoke mounts and frames	102
10.5.3. Confirm that all security conditions have been met.....	102
10.6. Sending the objects.....	102
10.6.1. Make arrangements for sending the objects and confirm their safe arrival	102
10.7. Monitoring the loan.....	102
10.7.1. Monitor the condition and location of the objects during the loan.....	102
10.8. Arranging for return.....	102
10.8.1. Confirm the arrangements for the return of the objects, and plan their return to you.....	102
11. Documentation planning.....	104
11.1. Spectrum suggested procedure.....	104
11.2. Writing your documentation plan.....	105
11.2.1. Create your documentation plan.....	105
12. Condition checking and technical assessment	107
12.1. Spectrum suggested procedure.....	107
12.2. Carrying out a check/assessment.....	108
12.2.1. Virus scanning.....	108
12.2.1.2. Digital files held on physical digital devices.....	109
12.2.2. Fixity checking	110
12.2.3. File format validation	111
12.2.4. Monitoring formats	111
12.2.5. Monitoring storage.....	112
13. Collections care and conservation.....	113
13.1. Spectrum suggested procedure.....	113
13.2. Agreeing conservation work	115
13.2.1. Scope of the work to be carried out	115

13.2.2. Reach agreement on the work to be carried out.....	115
13.3. Carrying out conservation work	116
13.3.1. Carry out the agreed conservation work	116
13.4. Recording conservation work.....	117
13.4.1. At the time, or as soon as possible, record details of the job and the work on each object	117
13.4.2. Add relevant information from the conservation record to your documentation system.....	117
14. Valuation.....	118
15. Insurance and indemnity.....	118
16. Emergency planning for collections.....	119
16.1. Spectrum suggested procedure.....	119
16.2. Creating an emergency plan	120
17. Damage and loss	121
18. Deaccessioning and disposal	122
18.1. Spectrum suggested procedure.....	122
18.2 Deaccessioning objects	123
18.2.1. If in doubt, seek advise	123
18.3. Disposing of objects.....	123
18.3.1. Are the objects to be destroyed?	124
18.3.2. Approach potential recipients directly or advertise the disposal appropriately.....	124
18.3.3. Agree terms with the new owner and transfer legal title to them	124
19. Rights management	125
19.1. Spectrum suggested procedure.....	125
19.2 Researching rights associated with your collection.....	126
19.2.1 Research the rights associated with objects, reproductions and information in your collection	126
19.3. Getting permission from other rights holders (Rights in).....	127
19.3.1. Ask the rights holder, or their agent, for permission to use their material in the way you want	127
19.3.2. Record information about the permission (which might be a formal licence)	128
20. Reproduction.....	129
20.1. Spectrum suggested procedure.....	129
20.2. Make the reproduction.....	129
20.2.1 Access and re-use copies.....	129
21. Use of collections	131
22. Collections review.....	131
23. Audit.....	132
23.1. Spectrum suggested procedure.....	132
23.2. Auditing objects	133

23.2.1. Verify the physical presence of each object and the accuracy of associated core inventory information	133
A.1. Glossary	134
A.2. Other Glossaries.....	139
A.3. Bibliography	140

I. Authors, editors and contributors

Digital collections toolkit working group

Sophie Walker, Information Manager, BFI, *Chair*

Marion Crick, Head of Collections Management, Victoria and Albert Museum

Gordon McKenna, Standards Manager, Collections Trust

Rob Scott, Collection Systems Manager, BFI

Tom Smith, Collections Systems Manager, IWM

Elisabeth Thurlow, Digital Preservation and Access Manager, University of the Arts London

Pam Young, Head Registrar (Documentation and Systems), Victoria and Albert Museum

Arran Rees, Research Associate, University of Leeds

Edited by

Kevin Bolton, Archive, Library and Museum Consultant, Kevinjbolton Ltd

Kindly supported by The National Archives (UK)

Other contributors

Emily Dodd, Head of Collections Management, Imperial War Museum

Lucy Wales, Digital Preservation and Data Manager, BFI

Patricia Falco, Time-based Media Conservation, Acquisitions, Tate

Participants in feedback workshop, May 2021

Foteini Aravani, Digital Curator, Museum of London

Gabriella Arrigoni, TaNC researcher, Victoria and Albert Museum

Paul Beard, Documentation Officer, Horniman Museum

Helen Brown, Exhibition and Collection Officer, Chatham Historic Dockyard Trust

Becky Brumhill, Image Management Officer (DAMs Manager), Amgeuddfa cYmru - National Museum Wales

Patricia Falcao, Time-based Media Conservation, Acquisitions, Tate

Amy Foulds, Collections and Library Manager, Museum of the Home

Melanie Gardner, Keeper of Fine and Decorative Art, Tullie House Museum and Gardens

Charlotte Goss, Collections Systems Manager, Royal Air Force Museum

Melinda Haunton, Archive Service Accreditation Manager, The National Archives

Anna Hawkins, Museum Collections Manager, University of Edinburgh

Gabrielle Heffernan, Curatorial Manager, Tullie House Museum and Art Gallery Trust

Penny Hutchins, Records Officer, National Army Museum

Nienke Jelles, Registrar, Zeeuws Museum

Frances Liddell, PHD student, University of Manchester
William Lowry, Digital Collections Manager, Museum of London
Kelly Martin, Documentation Officer, Tyne and Wear Archives and Museums
Meg McKavanagh, Head of Collections, Museum of Brisbane
Victoria Mulford, Digital Engagement Officer, Chatham Historic Dockyard Trust
Sarah Norville, Documentation and Railway Heritage Manager,
Lizzie O'Neill, Digital Collections Manager, The Hunterian, University of Glasgow
Elsa Price, Curator of Human History, Tullie House Museum and Gardens
Jo Pugh, Digital Development Manager, The National Archives
Arran Rees, Research Associate, University of Leeds
Taniah Simpson, Collections Services Manager, National Museums Liverpool
Claire Sleightholm, Assistant Curator, Tullie House Museum and Art Gallery Trust
Auke Slotegraaf, Project lead, Centre for Astronomical Heritage
Elisabeth Thurlow, Digital Preservation and Access Manager, University of the Arts London
Jonathan Whitson Cloud, Knowledge and Information Manager, Horniman Museum and Gardens
Pam Young, Collections Documentation and Procedures Manager, Victoria and Albert Museum

Participants in feedback workshop, November 2022

Sarah Brown, Deputy Director, Collections Trust
Fiona Campbell, Digital Content Editor, National Museums Liverpool
Helen Dafter, Archivist (Digital Preservation), Postal Museum
Emily Dodd, Head of Collections Development & Information, Imperial War Museum
Stephanie Fletcher, Assistant Curator, University of Salford Art Collection
Rosie Forrest, Head of Collection Information & DAM, National Galleries of Scotland
Flora Fyles, Collections Registrar, Museum of London
Corinna Gardner, Senior Curator of Design and Digital, Victoria & Albert Museum
Anna Hawkins, Museum Collections Manager, University of Edinburgh
Shannon Hoerder, Senior Documentation Officer, Victoria & Albert Museum
Nathalie Kane, Senior Curator of Design and Digital, Victoria & Albert Museum
Janna King, Documentation Assistant, Wakefield Council Museums & Castles
Somaya Langley, Digital Preservation Manager, Science Museum Group
William Lowry, Digital Collections Manager, Museum of London
Kelly Martin, Collections Information Manager, Tyne & Wear Archives & Museums
Duncan McColl, Digital and Special Collections Archivist, Art Gallery of New South Wales (AGNSW)
Kieran O'Leary, Digital Preservation Manager, National Library of Ireland

Lizzie O'Neill, Digital Collections Manager, The Hunterian, University of Glasgow

Lindsey Pickles, Registrar, Wakefield Council Museums & Castles

Ana Rita Pimenta Carneiro, PhD student - Conservation and restoration (Artificial Intelligence and cataloguing), Catholic University of Porto, School of Arts

Ana Cecilia Rocha Veiga, Associate professor - School of Information Science, Federal University of Minas Gerais (UFMG, Brazil)

Claire Sedgwick, Registrar, National Museums Liverpool

Luke Stempien, Collections Manager, Canadian Museum of Immigration at Pier 21

1. Introduction

1.1. About the toolkit

1.1.1 Foreword

Digital Collection Objects (DCOs) are considered part of a museum's collection and like physical objects, are subject to the same *suggested procedures* described in Spectrum¹. This toolkit is designed to provide museum professionals with a suite of practical, tried and tested tools and workflows, taken from the digital preservation community and adapted and interpreted for them, within the framework of Spectrum's suggested procedures.

Throughout this toolkit you will find content quoted from Spectrum, including procedure definitions and suggested procedures. This content is subject to Collections Trust's standard licensing terms². For clarity, content from Spectrum is presented within a dark border, as in the example below.

Example text indicating Spectrum content.

The aim of this toolkit is to ensure museum professionals are provided the correct information to enable them to identify, retrieve, store, preserve and access all types of DCO, both now and in the future.

This toolkit provides guidance on how museum professionals can provide and plan for the long-term management and care of and access to DCOs. All advice is in accordance with current digital preservation best practice and has been tried and tested within the international museum, archive, and library community.

Using Spectrum's collection management suggested procedures as a starting point, the toolkit looks at the existing workflow for physical collections and asks the question: 'Is the workflow for managing DCOs different from the workflow stipulated in Spectrum?' If the workflow is the same for digital as they are for physical objects, then only Spectrum is required as reference. If the workflow is different for digital collections, then this toolkit should be used as a starting point.

Digital collections are very fragile, in some ways more so than physical collections. According to the UNESCO *Charter on the Preservation of Digital Heritage* "digital heritage is at risk of being lost and that its preservation for the benefit of present and future generations is an urgent issue of worldwide concern".³

Museums are starting to collect a range of DCOs that are challenging our traditional definitions of the museum object. Sometimes intangible, sometimes partly or entirely physical, sometimes networked, sometimes interactive and always changing. As the museum sector starts to acquire and collect our digital heritage in increasing complexity and variety, we are discovering significant barriers that enable us to document, interpret, locate, access, interact

¹ Collections Trust. [Spectrum standard](#). Accessed 2023.

² [Spectrum licensing](#). Accessed 2024.

³ [Charter on the Preservation of Digital Heritage](#), United Nations Educational, Scientific and Cultural Organization (UNESCO). Accessed 2023.

with, preserve, and interpret these collections. In some cases the governance and copyright frameworks, designed for physical objects, are not fit for purpose.

This toolkit attempts to unpick some of the digital preservation concepts, tools and protocols that are key to understanding how a GLAM organisation may preserve DCOs now and in the long term. Managing and preserving DCOs can be achieved, to some degree, with moderate resources and budget, but organisations should be pragmatic about the type of DCO that can be managed in their organisation, within the constraints of available staff time, expertise, resource and infrastructure, to ensure their collection or potential collection is not exposed to short and long term risks. DCOs require just as much, if not more, skills, capacity, planning and resources as physical objects. The IT infrastructure required can be expensive, and the skills and time to monitor and proactively preserve digital collections over time should not be overlooked.

Although this toolkit will offer solutions to some challenges, it is not currently possible to provide all the solutions to the management of more complex DCOs. At the time of writing, there is no developed strategy for acquiring, using, displaying, and preserving some complex digital heritage now and in the long term. In fact, for the more complex cases, a partnership approach may be more feasible, where museums pool expertise, time and infrastructure to co-acquire, manage and preserve the DCO for the nation.

1.1.2 How to navigate the toolkit

Each of the 21 Spectrum procedures has a separate chapter within the toolkit. For some procedures, it is possible to follow the Spectrum suggested procedure only, but for other procedures, the further actions described in the toolkit are recommended when managing digital collections. Within each chapter there is a table listing the workflow of the corresponding Spectrum suggested procedure. For each Spectrum suggested procedure step the question is asked if the step is different for digital collections.

When the steps are different for digital collections, the table references a section in the toolkit, which outlines exactly how the steps for managing digital collections are different.

When the steps are the same, the corresponding action in the Spectrum suggested procedure should be followed as it is with physical collections.

Where a process required for managing DCOs cannot be neatly fitted into existing Spectrum headings, further sections have been added at the end of the chapter. These processes are unique to managing digital collections and there is no equivalent process for managing physical collections. Please note we are not promoting a 'one size fits all' approach and expect museums to use and adapt the processes depending on their needs.

Any technical or digital preservation terms and processes referenced in the toolkit, have been defined in [A.1. Glossary](#).

A bibliography of recommended further reading is referenced throughout the toolkit and fully listed in [A.3. Bibliography](#).

1.1.3 What is out of scope?

Digital material, sometimes referred to as [digital assets](#), that are not part of the museum's registered collection, are out of scope for this document. For example, digital photographs and other reproductions of physical museum objects, which are described in the *Spectrum Reproduction* procedure⁴.

However, [supporting digital files](#) that accompany some DCOs, are the exception to this rule and are in scope, as without supporting files, some DCOs could not be accessed, operated or understood.

1.1.4. Who should use the toolkit?

The toolkit will be useful to any museum or GLAM professional with whole or part responsibility for managing DCOs.

1.2. Introduction to digital preservation

1.2.1. Why is digital preservation important?

Digital collections are very fragile, in some ways more so than physical collections. The risk of our digital heritage disappearing is very real and extremely urgent. According to the UNESCO *Charter on the Preservation of Digital Heritage* "digital heritage is at risk of being lost and that its preservation for the benefit of present and future generations is an urgent issue of worldwide concern".⁵

In the last 30 years, digital technologies have been produced, evolved and replaced at a rapid rate and collecting organisations have lacked sufficient time, knowledge, resource and support to develop preservation strategies to adequately preserve all of this heritage. As Susanna Corder, Documentary Curator at the London Transport Museum, in the introduction to the Digital Preservation chapter of *Contemporary Collecting: An ethical toolkit for museum practitioners*⁶ says: "Some museums, due to misconceptions or restriction of resources, consider digital preservation as an afterthought, rather than an integral part of the curatorial process...The digital is now part of our everyday lives and this should be reflected in our collections."

In the Conclusion to the project report for "Preserving and sharing born-digital and hybrid objects from and across the National Collection"⁷, the authors characterise the risks and fragility of our digital heritage as not just a technical problem. Is it a systemic issue, meaning that digital producers have no standardised way of maintaining a meaningful digital archive. There is a profusion of technologies being created all the time that digital preservation experts

⁴ Collections Trust. [Reproduction - suggested procedure](#). Accessed 2023.

⁵ [Charter on the Preservation of Digital Heritage](#), United Nations Educational, Scientific and Cultural Organization (UNESCO). Accessed 2023.

⁶ [Contemporary Collecting: An ethical toolkit for museum practitioners](#). Ellie Miles, Susanna Corder, Jen Kavanagh. Published by London Transport Museum. 2020. p.30. Accessed 2023.

⁷ [Preserving and sharing born-digital and hybrid objects from and across the National Collection](#). Project report. January 2022. Accessed 2023.

cannot hope to preserve in time and there is a lack of support from the cultural sector in evolving policy and collecting practices or even recognising digital heritage as heritage at all.

Doing nothing is not an option. Unlike some types of physical objects, a DCO which is not selected for active digital preservation at an early stage in its existence will very likely be lost or unusable in a few years' time.

1.2.2. Core principles of digital preservation

Digital Preservation is the series of actions carried out to preserve and ensure continued long-term access to and use of Digital Collection Objects (DCOs) both now and in the future. The NDSA Levels of Digital Preservation⁸, is a trusted resource for digital preservation practitioners coordinated by the Library of Congress. NDSA describes five core areas at the heart of digital preservation. These are:

- **Storage** - Digital storage technologies present several risks to the long-term preservation of DCOs. These risks can be reduced by using a digital storage strategy that involves one or more storage systems and at least two copies of the digital files.
- **Integrity** - [Fixity checking](#) and [virus scanning](#) are two digital preservation processes that ensure that the digital integrity of the DCO remains unchanged throughout the life of the digital files. This helps detect corruption or loss.
- **Control** - DCOs can easily be changed or deleted accidentally due to human error. Procedure and workflow should be in place to ensure that digital information is protected from unauthorised change that can occur when the digital file is accessed or used as well as accidental deletion.
- **Metadata** - Contextual information is required to understand the DCOs and for it to be useful, so managing this metadata is also a fundamental aspect of digital preservation.
- **Content** - [File formats](#), software and systems used to support access to DCOs can become [obsolete](#) over time. It is important that there are strategies in place to monitor file formats and when necessary, carry out [format migration](#) to help mitigate against these risks.

NDSA describes 4 levels of digital preservation. Level 1 is the minimum level that it is recommended all organisations managing digital material try to achieve. This toolkit will guide you to achieve digital preservation to at least NDSA level 1 standard. This standard is achievable within the capacity and resources of small to medium sized museums. Bill Lowry, Digital Preservation Manager at the Museum of London, gives a useful overview of what level 1 means in practice in the 'Getting Started in Digital Preservation' chapter of *Contemporary Collecting: An ethical toolkit for museum practitioners*, published by the London Transport Museum and supported by the Arts Council⁹.

⁸ [Levels of Digital Preservation](#). NDSA. Accessed 2023.

⁹ [Contemporary Collecting: An ethical toolkit for museum practitioners](#). Ellie Miles, Susanna Cordner, Jen Kavanagh. Published by London Transport Museum. 2020. p.31. Accessed 2023.

1.3. Definition of digital collection objects

The term Digital Collection Object (DCO) describes a wide range of different digital object types. What all these objects have in common is that some or all of its elements require a digital environment, such as a software application, specific hardware or the live web, to be accessed and understood by humans. DCOs can comprise entirely of digital elements, entirely of physical components or a combination of the two. Examples of DCOs that are in an entirely physical state include [physical digital devices](#), such as a USB stick, or hardware that is integral to the DCO, such as a computer.

Examples of DCOs that are in a part physical/part digital state include digital files that are accompanied by hardware used to provide access to the files and hybrid digital/physical art installations including digital video and physical objects.

No DCO can operate in isolation and must be used together with the correct digital environment for the intended meaning, concept or purpose of the object to be conveyed and understood by humans. Individual components of a DCO can also have differing needs in terms of their management and care, as with any multi-part object. Indeed in the case of physical components, many aspects of Spectrum suggested procedures may directly apply to them unchanged, while digital components will require a combined collections management and digital preservation approach.

Another defining characteristic of a DCO is that its digital and physical form will change overtime if it is to exist in perpetuity. Due to the fragility of the digital medium, the [bits](#), the digital data that makes up the DCO, must be transferred from one digital format to another overtime, to ensure the DCO can continue to be accessed and enjoyed into the future.

It is worth noting, that in the case of some complex social media or system examples, the term 'object' does not fit. In these examples, the term 'ecosystem' is more relevant. This is due to the networked, interdependent and changeable nature of this ecology of systems, applications, files and other digital components.

1.3.1. Managing digital collection objects

When planning the management and documentation of a DCO it may be useful to consider two further properties of the object:

1.3.1.1. Difficulty in managing

Different factors affect how easy or difficult it may be to manage and document a Digital Collection Object (DCO). Commonly used formats such as TIFF files, PDF or MOV files can be easily accessed and the software needed to play them is readily available, so managing and preserving these DCOs is relatively straightforward, even in large numbers. Similarly, self-contained software packages, such as Microsoft Word files, would be straightforward to manage if they can be run on common operating systems, such as Windows or Mac OS.

However, DCOs made up of multiple digital elements, such as DPX files, or less common formats, such as HTML/CSS files, will require more specialist resources and expertise to ascertain how the DCO will be managed and preserved now and in the long term. Some DCOs are dependent on the live web, social interaction or specific hardware drivers to function, so similarly these digital objects require specialist expertise or resources to manage. Video games and other digital objects that depend on emerging media to operate, are equally difficult to manage and preserve long term and it is recommended that only organisations that have the capacity and resource to solely, or in partnership, take on the long term management and preservation of this type of DCO.

In the table below, are listed different types of DCO and a definition of the DCO type, an example of that type of DCO and the level of resource required to manage and preserve the DCO now and in the long term:

Type	Definition	Examples	Level of resource required to manage/preserve
Commonly used single digital files.	• A single digital file in a commonly used contemporary format. • Can be easily accessed on software/hardware readily available.	• TIFF files. • PDF files. • MOV files.	Little expertise or resources required.
Self-contained software that depends on generic operating systems.	• Self-contained software package that depends on generic operating systems such as Windows XP or Mac OS 10. • A software package is a set of files “packaged” together that can freely move between storage environments without losing either intrinsic value as a DCO, or the ability to access and use their content. • Unlike other DCOs software packages they often have the capacity to create additional files or data through their usage.	• Docx (Word) files. • Xlsx (Excel) files.	Little expertise or resources required.

Less common format/software/hardware.	• Less common formats. • Requires a less common software/hardware to use it.	• Simple self-contained website e.g. HTML/CSS files. • CAD files and software.	Requires more specialist expertise and resources to manage.
DCO containing multiple digital elements/files.	• May consist of multiple related digital elements or files. • The digital elements or files need to work together to render the whole DCO and without one, the intrinsic value as a collection object is lost.	• Media stored as a sequence of separate files e.g. Moving image DPX sequences. • CAD files	Requires more specialist expertise and resources to manage.
DCO with complex digital dependencies .	• DCOs that are dependent on complex hardware (auxiliary object), software or other digital environments to operate effectively. • For example, a software package which requires management of dependencies to move between storage environments. • Examples of dependencies include additional software packages such as playback software and hardware drivers, specific operating system versions, internet access for externally hosted dependencies, connection to a specifically configured database, or installation in an environment distributed across multiple servers. • DCOs that interact with the live web and/or online social networks.	• Website with external dependencies e.g. externally hosted JavaScript libraries. • Audio software with hardware driver dependencies. • An application which utilises a separately installed database to operate.	Requires more specialist expertise and resources to manage.
Video games.	• The combination of the unique copyright issues, the complex hardware dependencies, the emerging technologies used and the interactive nature of this DCO, makes managing and preserving video games very challenging. • As preserving video games is an emerging discipline, there is a lack of best practice guidance and support.	• <i>In the Eyes of the Animal</i>, Marshmallow Laser Feast, 2015. An immersive virtual reality animation with haptics and sound, experienced using a VR headset and “rumble pack”.	Requires significant specialist resources to manage across organisations.
Legacy digital formats.	• Legacy digital formats that have become or very soon to become obsolete. • The Digital Preservation Coalition maintain a “<i>Bit List</i>” of <i>digitally endangered</i>	• <i>Sonic the Hedgehog</i>. • Nintendo GameCube. • Universal Media Disk.	Requires more specialist expertise and resources to manage and may require expertise from a third party.

	<i>species</i>¹⁰, that flag up any digital formats that are at risk of obsolescence. Any formats categorised as “Endangered”, “Critically endangered” and “Practically extinct” should be considered part of this category.	• Digital Betacam.	
--	---	--	--

¹⁰ [The “Bit List” of Digitally Endangered Species. Digital Preservation Coalition](#). Accessed 2023.

1.3.1.2. Physicality

The physical nature of a DCO can vary from being purely digital, to purely physical to partly digital and partly physical.

An important question when managing a DCO is to consider to what degree any physical component should be considered part of it. Factors to consider include:

- How much intrinsic value do the physical aspects of the object lend to it?
- Does the object lose any meaning if only the digital (or physical) components of the object are preserved?
- Would preserving the physical aspects of the object allow you to better reflect the intended experience of the object?
- Does your organisation have access to sufficient expertise in preserving both physical and digital components of the object?

There is no one-size-fits-all answer to these questions, but an overall stance on some of these questions is something you should consider addressing as part of your collecting policy and digital preservation strategy. However, these questions should also be considered individually as part of assessing any new digital acquisition. Note that due to the changing form of the DCO, it may have one category at the point of acquisition but move to another category when digitally preserved and stored.

Category	Definition	Examples
Digital only	The object has no physical component and is a purely digital thing.	• Digital photographs, e.g. TIFF or JPEG files. • Digital artworks, e.g. Photoshop PSD or Illustrator AI files. • Digital documents, e.g. PDF files. • Digital architectural designs, e.g. AutoCAD files.
Stored on a physical digital device that is not part of the DCO	The DCO is stored on a physical digital device, but the device does not lend significant meaning to the object, and the meaning or intrinsic value of the object would not be lessened by removal from the physical carrier.	• Digital photographs supplied on a USB drive. • Moving image media supplied on an LTO data tape.
Stored on a physical digital device considered part of the DCO	The DCO is stored on a physical digital storage device that it could be theoretically separated from, but the carrier is also considered to be an intrinsic part of that object.	• Video game stored on DVD/Blu-ray media or ROM cartridge.
Physical/digital hybrid	The DCO includes physical components which it cannot be separated from without significantly impacting either the	• Digital audio-visual installation to be displayed on the original hardware.

	usability or intrinsic meaning and value of the object itself.	• Computer hardware e.g. PCs, tablets, phones, video games consoles, 360 video headsets. • A multimedia art installation incorporating digital projection and /or audio recording alongside tangible components made as part of the artwork or found objects incorporated into the installation.
--	--	---

2. Getting Started

The guidance in this section is designed to be used by museum professionals just getting started with digital collections. This chapter does not correspond with a Spectrum procedure.

2.1. First steps in safeguarding an existing digital collection

This section is aimed at organisations that already have acquired DCOs but as yet have no formal procedures for managing them. The checklist below should be considered as a starting point, focussing on a list of priority actions that are essential to ensure the existing digital collection is secure and identifiable in the short term. Implementing this set of actions below will buy your organisation a little time. However, in the medium term, it is highly recommended that the museum develops procedures and strategy, based on recommendations in the toolkit, for managing its digital collections to ensure they will survive into the future.

The Digital Preservation Coalition provides free training to all members of the GLAM community. See the DPC website for more details: [Novice to Know How](#).

Order of Priority	Activity	Risk to digital collection if not actioned
1	Without digitally or physically accessing or moving any digital files, update your organisation's existing <i>Documentation plan</i> with details of what digital collections your organisation holds and where they are stored. For further information go to Section 11.2. Writing your documentation plan .	You will not know approximately what DCOs you hold and where they are located.
2	Set up the equipment you will need for managing your digital collections. For further information go to Section 2.3. Setting up equipment and resource for managing digital preservation .	Digital information could be lost or deleted.
3	From an appropriate workstation or PC, without moving any digital files yet, follow the protocol for virus scanning every digital file in the collection from their separate digital locations. For further information, go to Section 12.2.1. Virus scanning .	A virus or malware compromises digital file/s or the whole IT network.
4	Consult documentation to make sure each digital file has a checksum. If a pre-entry checksum has not been provided, generate a checksum as soon as it is safe to do so, then carry out a fixity check. For further information, go to Section 12.2.2. Fixity checking .	There is no evidence that information in the digital file has changed e.g. information is corrupted, missing, or damaged.
5	As an optional step, download a tool to safely analyse digital files held on older physical digital devices . Visit COPTR, an online registry of digital preservation tools for more information about the best digital preservation tool to use for this purpose, See Section 12.2.1.2. Digital files held on digital devices for further information.	

6	Once the virus scanning and fixity checks have been actioned, transfer digital files and supporting digital files that form part of your digital collection into a secure backed up digital location. For more information go to Chapter 5. Location and movement control .	Your DCOs and supporting digital files are deleted or corrupted and cannot be retrieved.
7	Once it is safe and possible to access the digital files, carry out a more detailed inventory. For further information, go to Section 6.2.4. Producing an inventory in the <i>Inventory</i> chapter.	You will not know what DCOs you hold, where they are located.
8	Using file copying software, transfer the digital files into long term digital storage. The <i>Digital Preservation Handbook</i> , produced by the Digital Preservation Coalition, has a useful section on Storage ¹¹ . For an overview of best practice for creating and storing digital preservation copies, see Section 5.3.1.1. Digital preservation rules for creating and storing digital preservation copies . For more information about transferring digital files without losing data or damaging the digital file, go to Section 5.4.4.1. File copying software .	Your DCOs and supporting digital files become corrupted or damaged over time and there is no copy to fall back on.

2.2. Develop a strategy for managing and digitally preserving your digital collection

A strategy for defining how you will collect, document, store, digitally preserve, and access your museum's digital collection is essential. Your strategy should consist of a mixture of policies, procedures and plans for the application of procedures.

There is no one-size-fits-all approach to a digital collections strategy, rather a series of best practice approaches that can be selected depending on the size and nature of the collection and your museum's mandate. The sections below will help you define your museum's current capacity, resource, and capability for managing digital collections and provide a set of outputs for each activity. The National Archives have produced guidance¹² in this area that is available on their website.

2.2.1. A note on current cultural policy

The project report for a Towards a National Collection funded project *Preserving and sharing born-digital and hybrid objects from and across the National Collection*¹³, calls for current cultural policy to change to better accommodate the acquisition, preservation and use of DCOs in all their growing complexity and to enable and support museum professionals to experiment with collecting and preserving more complex DCOs, recognise digital preservation as a unique discipline and guarantee DCOs are supported by the right technical and organisational infrastructure.

¹¹ [Storage. Digital Preservation Handbook. Digital Preservation Coalition](#). Accessed 2023.

¹² [Developing a digital preservation strategy and policy](#). The National Archives. Accessed 2023.

¹³ [Preserving and sharing born-digital and hybrid objects from and across the National Collection](#). Project report. January 2022. Accessed 2023.

2.2.2. Assess your museum's strategic readiness

To develop a strategy for managing a digital collection, it is useful to assess your museum's current and potential capacity to develop and manage its current and future digital collections. If your museum has ambitions to establish a digital collection or to collect more or different digital heritage in the future, a review of this kind will also help identify any areas for future development. To understand your museum's strategic readiness, you should take the following steps.

Make use of *The Digital Cultural Compass*¹⁴ free tracker tool to make an initial assessment of your organisation's overall digital readiness. This is a tool which was commissioned by ACE as part of Culture is Digital, which allows you to assess your overall digital readiness and then track progress to digital maturity.

Review the organisation's existing Collections Management Policy framework, which all accredited museums should already have.

Collections Development: Arts Council England has produced a template for a Collection Development Policy (which documents the principles of what the museum acquires) which is available through the Collections Trust *Acquisition and Accessioning* resources.¹⁵ The museum's digital collections should be outlined within the description of the current collection and themes for future collection as this establishes them as collection objects, rather than [digital assets](#) in the museum's ownership.

Collections Documentation: This part of the policy framework should document the museum's commitment to recording information about the DCOs.

Collections Care: The Collections Care policy should document the organisational commitment and approach to storing, preserving and conserving DCOs. This could either be a standalone document - such as a digital preservation policy¹⁶ - or part of a wider collections care policy. Either way, in deciding your policy you will most likely need to consider these questions:

- Who is responsible for digital preservation and for setting and ensuring the standards of digital collections care are maintained?
- What are the standards for the different categories of DCO in your collection?
- How will you monitor that these standards are being maintained?
- When might you consider digital preservation treatment for DCOs?
- Who will be involved in agreeing the scope of any proposed digital preservation work?
- Who can authorise digital preservation work?
- Who can carry out digital preservation work, and what are your criteria for selecting external specialists where needed?

¹⁴ [Digital Cultural Compass](#). Arts Council England and National Lottery Heritage Fund. Accessed 2023.

¹⁵ [Collections Development Policy Template](#), Collections Trust. Accessed 2023.

¹⁶ [Institutional Policies and Procedures](#). Digital Preservation Coalition. Accessed 2023.

- How should digital preservation work be documented?
- Who should have permission to access, amend and delete DCOs?

You should have a written procedure that explains the steps to follow when managing and carrying out [digital preservation actions](#). Spectrum's suggested procedure provides a useful starting point, but it is recommended your own procedure meet the following minimum requirements:

Recommended requirements	Why this is important
Appropriate authorisation is given for any digital preservation actions.	No digital preservation actions happen without the knowledge of those responsible for the DCOs.
You record all digital preservation actions carried out. ¹⁷	You have a full history of digital preservation actions carried out, and can find this information easily when required.
You update objects' catalogue records with any new information gained as a result of digital preservation actions.	New information gained is appropriately recorded.
You schedule, where necessary, any further digital preservation actions, condition checks or periodic review of actions required. ¹⁸	You can plan your digital preservation activity (where appropriate) and ensure that DCOs are available when needed.

¹⁷ [Examples of preservation actions](#). Digital Preservation Coalition. *Digital Preservation Handbook. Digital preservation actions*. Accessed 2023.

¹⁸ [Examples of preservation actions](#). Digital Preservation Coalition. *Digital Preservation Handbook. Digital preservation actions*. Accessed 2023.

2.2.3 Assess your museum's operational readiness

If you do have an existing digital collection, review the information compiled in the digital collections section of the museum's documentation plan, including the format and type of DCOs you hold and the reason for acquisition. This information will help you start to define the technical, ethical, and curatorial requirements of managing these DCOs now and in the future, so they can be accessed and enjoyed by the public in the manner and context that the museum and the artist or producer intended.

There are a number of assessment frameworks and maturity models available for free online, which will help your museum assess its technical infrastructure, staff capacity and expertise and processes to check its readiness.

The Digital Preservation Coalition's *Rapid Assessment Model (RAM)*¹⁹, is an excellent light touch tool for organisations of all sizes to self-evaluate their governance framework, policies and technical infrastructure and ascertain their readiness for managing DCOs. It is recommended that smaller organisations with less resources aim for level 2 and larger organisations with more resources aim for level 4. *Levels of Digital Preservation* and the accompanying assessment²⁰ created by the National Digital Stewardship Alliance (NDSA) is excellent for a more focussed look on the technical requirements of preserving DCOs in accordance with digital preservation best practice.

Outputs you will have produced at this stage will be

- An assessment of operational readiness for managing digital collections. This will form part of the status description within a business case for improving digital collections management.

2.2.4. Assess the risks

If your organisation has an existing digital collection, it is an essential part of your collection's business plan to carry out an assessment of the risks that the collection is exposed to if the organisation were to do nothing to manage or preserve the collection. A risk assessment is a good way of establishing and advocating for the urgency and importance of following digital preservation best practice and identifying the areas of the collection in most need of resource and staff attention. Any significant risks should be added to the museum's risk register. The digital collection should be added to the museum's business continuity plan so there is a plan of action after salvage in the event of an emergency.

The Digital Preservation Coalition has published a table of risks²¹ and financial costs that organisations are exposed to if digital preservation is not carried out, as well as benefits to the organisation when successful digital preservation has been achieved. This table of risks can be used to assess your own collection to produce an organisational risk register for your digital collections or incorporated into your existing collections risk register.

¹⁹ [Rapid Assessment Model \(RAM\)](#), The Digital Preservation Coalition. Accessed 2023.

²⁰ [Levels of Digital Preservation](#). National Digital Stewardship Alliance. Accessed 2023.

²¹ [What are the risks of not preserving digital material?](#) Digital Preservation Coalition. Accessed 2023.

Collections Trust and SHARE Museums East have produced a guide for incorporating potential risks into a risk assessment and risk management plan.²²

The output you will have produced during this stage is a risk register for your DCOs which can be reviewed on a regular basis.

2.2.5. Decide which standards and best practice models you wish to implement

At present, best practice models have been developed primarily for the archive sector. Two models which can be reused for museum collections are described below.

2.2.5.1. Open Archival Information System (OAIS)

The Open Archival Information System (OAIS)²³ is an international model widely used by the archive sector to ensure that digital files are described consistently, information is shared and kept together to ensure long term preservation and access.

The OAIS Reference model describes an information model for structuring digital files and their metadata. The “Submission Information Package (SIP)” is the package of all the digital files, [supporting digital files](#) and metadata that make up the DCO sent from the “producer” to the “archive”. It includes the following information objects:

- Content Information: this includes the data object and its representation information.
- Preservation Description Information: contains information necessary to preserve its affiliated content information (such as information about the item's provenance, unique identifiers, a [checksum](#) or other authentication data, etc.)
- Packaging Information: holds the components of the information package together.
- Descriptive Information: metadata about the object which allows the object to be located at a later time using the archive's search or retrieval functions.

The “Archive Information Package (AIP)” is the package of all the digital files, supporting digital files and metadata that make up the DCO that is received by the archive. An AIP contains both metadata that describes the structure and content of an “archived essence” and the “actual essence” itself.

²² [Assess and Manage Risk in Collections Care](#), Collections Trust, Norfolk Museums Service and SHARE Museums East. Accessed 2023.

²³ The Consultative Committee for Space Data Systems. [The Open Archival Information System](#). Accessed 2023.

2.2.5.2. Trustworthy Repositories Audit and Certification (TRAC)

TRAC²⁴ is a framework used by archival repositories to help them certify as a trustworthy digital repository and comply with OAIS. This is not a standard that you are required as a museum to work towards, however, some sections are useful in describing what good looks like for a digital archive. To be a “trustworthy” repository, there must be a “mission to provide reliable, long-term access to managed digital resources to its Designated Community, now and into the future”. There is also very practical guidance on how this could be done, that might be a useful resource.

The following chapters are the most useful:

- *Digital object management - Ingest: acquisition of content.*
- *Digital object management - Ingest: Creation of the AIP.*
- *Preservation planning.*
- *AIP preservation.*
- *Information management.*
- *Access management.*

The output you will have produced at this stage will be a proposed standard framework for your organisation. The achievement of this standard framework will form the bulk of your business plan for managing DCOs.

2.2.6. Build a business case for developing organisational readiness

The outputs created in the preceding steps in this section will provide you with the building blocks for creating a strategy and plan for managing your collection of DCOs. The next stage of developing the plan is providing the business case for implementing the digital collection management and preservation plan. The Digital Preservation Coalition have a useful resource²⁵ for building a business case for digital preservation. This should be used in conjunction with the internal organisational information you have produced in previous steps to create your own project proposal.

2.3. Setting up equipment and resource for managing digital preservation

The National Archives have a very useful guidance on what equipment and software you may require to manage your museum’s digital preservation processes and workflows²⁶.

It is recommended that you use [write blockers](#) if possible to protect the integrity of data within the digital files that make up the DCO.

²⁴ [Trustworthy Repositories Audit and Certification: Criteria and Checklist](#), National Archives and Records Administration. Accessed 2023.

²⁵ Digital Preservation Coalition. [Digital Preservation Business Case Toolkit](#). Accessed 2023.

²⁶ [Digital Preservation Workflows: Introduction](#). The National Archives. Accessed 2023.

2.3.1. Setting up a dedicated workstation

Set up a dedicated computer workstation/s and for managing all types of digital and storage formats that the museum is currently or intends to access, acquire and/or preserve. For further guidance, *Digital Preservation Workflows*²⁷, produced by The National Archives has a useful section on setting up workstations and further resources to access.

2.3.2. Setting up a digital quarantine environment

It is recommended that a dedicated digital quarantine environment is made available to save all digital files yet to be virus scanned and checked. Used to temporarily store digital files not stored on [physical digital devices](#), that have not yet been virus scanned and could corrupt or damage other digital files or the IT network. It can be used to quarantine digital files before they have been virus scanned and fixity checked and transferred to a more long term storage solution.

The server, workstation, PC or other digital environment should sit outside the museum's main IT network to safeguard against a virus compromising the whole IT network. A digital quarantine environment should be a temporary storage location for files not yet fully processed. Once the digital files have been processed and confirmed as secure and safe, they should be transferred to a more permanent digital location, either within the IT network or on a digital preservation storage medium such as an LTO tape.

2.3.3. Staff roles and responsibilities

Agreeing who is responsible for managing and preserving DCOs within the museum can be challenging. However, it is worthwhile to take time to audit staff skills and formalise roles and responsibilities especially when there is no one role dedicated to managing this collection, to ensure responsibility doesn't fall between the gaps. Although digital preservation actions are associated with different Spectrum procedures in this toolkit, it cannot be assumed that the role in the museum that would normally manage that procedure will automatically have the skills to manage that procedure for a digital collection.

Where it might be reasonable to assume that a registrar or curator may lead on digital acquisitions and disposals as the skills involved are not very different, when it comes to managing digital preservation, staff who are responsible for conservation in the museum may need support from other internal or external parties. For example, IT and registration might have additional skills to write a facilities report for a digital loan. It is recommended that the IT department take a bigger role in decision making (for example, it is recommended to have one or more IT representatives when making decisions about acquiring digital collections) and external legal advice may be required when dealing particularly knotty IP and copyright questions and issues.

Succession planning is particularly important to ensure that essential information required to maintain servers and to continue to enable access to digital collections is not lost when the staff member managing the collection leaves or falls ill. It is recommended that a document holding this important information is accessible to one or two other colleagues, but due to the sensitivity of the information, is not readily accessible to all staff. For particularly sensitive information like passwords, it might be prudent to tell one or two trusted colleagues rather than write it down.

²⁷ [Guidance for Digital Preservation workflows](#). The National Archives. Accessed 2023.

2.3.4. Resource requirements for digital preservation

The management of digital collection objects requires a long-term commitment from senior management, requiring an investment of both time and money.

There is not room here to discuss in detail the costs of running the equipment, hardware, software, and staff costs, to manage digital collections within a museum. Although it is possible to acquire some open-source tools to manage some digital preservation actions, the staff time required to support their use should not be underestimated. Digital preservation systems that automate the digital preservation workflows described in this toolkit do save aspects of staff time, but of course these come at a cost, and will themselves require significant staff time to implement and manage.

The time it takes to establish, implement and embed digital preservation activities within the culture of the museum also cannot be underestimated. This will require a long-term commitment, including ensuring adequate staffing levels are in place to support long-term digital collections management and that staff are equipped with relevant skills to support the preservation of digital collection objects.

3. Object entry

Spectrum definition - logging all objects coming into your care for whatever reason, including loans, enquiries and potential acquisitions.

For digital collections, this means logging the DCOs - including the digital files and, if they are intrinsic to the DCO, any [physical digital device](#).

3.1. Spectrum suggested procedure²⁸

Spectrum suggested procedure workflow	Is the step in the workflow different for digital collections?
Preparing for object entry (if known in advance)	
Prepare for the arrival of the objects at your museum.	Yes. See Section 3.2.1.
Creating an entry record and receipt	
Make a record of the objects as soon as they arrive.	Yes. See Section 3.4.1.
Check and note the objects' condition, and any associated risks.	Yes. See Section 3.4.2.
Give (or send) the owner a copy of the entry record.	No.
Processing newly-arrived objects.	Yes. See Section 3.4.3.
Tag the objects with a temporary label marked with the <i>Entry number</i> or <i>Loan in reference number</i> .	Yes. See Section 3.4.4.
Record the first location of the objects.	Yes. See Section 3.4.5.
If the objects are planned acquisitions or incoming loans, return to the relevant procedure.	Yes. For acquisitions, see Chapter 4. Acquisition and accessioning . For loans see Chapter 9. Loans In (borrowing objects) .

²⁸ Collections Trust. [Object entry - Suggested procedure](#). Accessed 2023.

If objects arrive unexpectedly and are offered for acquisition, consider this offer.	No.
If an owner leaves objects for identification, carry this out within the agreed time.	No.
If objects arrive anonymously, deal with them according to your object entry policy.	No.

3.2. Preparing for Object entry (if known in advance)

3.2.1. Prepare for the arrival of the objects at your museum

<i>Order of Priority</i>	<i>Activity</i>	<i>Risk to digital collection if not actioned</i>
1	Prepare a full list of the digital formats and hardware that the museum has the capacity, expertise, and resources to digitally store and/or preserve that can be circulated to prospective lenders and acquisitions sources. Ensure the requirements are in accordance with your digital preservation strategy. Although the collection policy may describe the type of digital collections the museum intends to collect, it is unlikely to state the exact digital formats or hardware specifications as this information may change with time.	The museum acquires digital files and hardware it cannot digitally preserve in the long term or is missing vital information required to monitor the digital formats and plan for future digital preservation. This means the bits making up the DCO will either become damaged or the digital format or hardware will become obsolete , inaccessible, and unusable.
2	It is recommended that you communicate with the donor and other stakeholders, what level of digital preservation can be achieved at your museum for specific digital file formats or technology. For example, for a video game using emerging technologies such as virtual reality software, it may only be feasible to achieve bit-level preservation, which means the software could not be accessed or experienced by the public in the intended way, now or in the long term. NSDA provides a useful framework for levels of digital preservation. For further information, see <i>Levels of Digital Preservation</i>²⁹.	Reputational risk if the level of digital preservation achieved long term is not what the donor or other stakeholders expected.
3	Negotiate the terms and conditions of the loan or acquisition with the donor/lender. See Section 3.2.1.1. Recommended questions for donors and lenders for details with a list of recommended questions.	Reputational risk if the organisation does not formally agree terms and conditions, and a missed opportunity to establish expectations.

²⁹[Levels of Digital Preservation](#). National Digital Stewardship Alliance (NDSA). Accessed 2023.

4	Negotiate the terms and conditions of the loan or acquisition with the depositor, rights holders, and any other agents responsible for licencing, patenting, distribution, rights and producing all aspects of the DCO. See Section 3.2.1.2. Recommended questions for agents. below for details with a list of recommended questions. For some DCOs, such as video games and other proprietary software, the stakeholder group will be very complex, so allow plenty of time to identify, contact and agree terms with each of these agents prior to the acquisition or loan. All terms agreed should be made in accordance with the museum's acquisition and loans policies.	Preserving, accessing, copying or other activities carried out in the museum on the DCO, could risk a breach of copyright, patent, contract, or intellectual property law if terms and conditions have not been established or documented.
5	It is recommended that you carry out due diligence to identify any organisations or individuals that are depicted in the DCO to ensure they are aware of the long term legacy of digital objects. As Susanna Corder writes in the introduction to the <i>Digital Preservation</i> section of <i>Contemporary Collecting: An ethical toolkit for museum practitioners</i>, "The digital creates a different sphere of record and potential access that could in some cases outlive an object or a collection. It is important to ensure that those connected to... an object or account, understand this long term legacy".	Possible reputational risk if these individuals or organisations are not aware of the length of time that the museum could potentially preserve and maintain access to the DCO. Risk of the donor declining to donate further digital heritage.
6	Send a list of metadata that should be provided by every donor and lender, for each digital file, as described in Section 3.2.1.3 Metadata requirements to be provided by donors and lenders. The information is required to ensure the digital components of the DCO can be accessed, stored, managed, and digitally preserved now and in the future. The information is separated into two categories: technical metadata and descriptive metadata. It is recommended that the lender/s or donor/s send the metadata in an electronic format in the same folder as the digital files making up the acquisition.	Metadata describes and keeps safe fundamental information about the digital files and the DCO. Without this information, the museum may not be able to identify, access, preserve or carry out any other essential preservation, documentation or collections management activity.
7	When the information for the acquisition or loan has been received, have it ready for when the DCOs arrive.	Without the information, it will be more difficult to carry out an inventory and keep track of what has been received.

3.2.1.1. Recommended questions for donors and lenders

- Does the donor/lender grant permission to migrate data from the DCO to a new preservation format?
- Does the donor/lender grant permission for the museum to extract all technical metadata embedded in the DCO?
- Is the donor/lender aware of any personal or sensitive metadata and are there terms and conditions attached to this? For example a geolocation attached to a photograph, or the player's ranking or nickname in a video game.

- Are both parties (donor and museum) clear as to exactly what aspects of the DCO will be acquired? Is the organisation clear as to the boundaries of what is being collected/preserved and what is not?
- With the donor, ascertain provenance and ownership of each element of the digital object. Is ownership recognised and can it be transferred to the museum?
- With the donor, negotiate the digital preservation approach and what that means regarding access to, interpretation and authenticity of the DCO.
- Negotiate access requirements that are suitable for how the museum intends to display/use/share or intends museum visitors/users to interact with the DCO.
- Working with the artist/producer to select the most appropriate and preservable version/s or manifestation/s of the DCOs for acquisition. If relevant and appropriate, request to acquire the [source code](#).
- In consultation with the producer and other stakeholders, map out all the technical dependencies required to preserve and access the DCO now and in the future. Research the availability and cost of purchasing and maintaining any software/hardware ([auxiliary object](#)) required to preserve and make DCO accessible and ensuring that this software/hardware can be maintained now and in the future.
- Look at collecting ephemera and user documentation that will enrich the interpretation and understanding of the DCO and feasibility of collecting and preserving this.
- Agree method of transfer and the pre-transfer protocol (e.g. fixity checking and metadata to be supplied).
- Consult with user communities and other stakeholders who have contributed or developed the DCO, possibly producing user testimonies to understand the DCO's significance to that community or wider society.
- Communicate with the donor to ascertain the production history of the DCO, i.e. how files were created, prior [format migrations](#) and emulations and the relationships between files to be supplied.
- Is the donor providing any acquired or supporting software or auxiliary hardware in an executable format? If the format is not executable, can software be sourced from another collection or can it be created from the source code?
- If the DCO is evolving and relies on community interaction or interaction with the internet, will the DCO continue to be "live" and networked when acquired into the museum?

3.2.1.2. Recommended questions for agents

The following information should be agreed in writing with each agent:

- Name of the agent.
- Role of the agent e.g. Copyright holder or software licencing.
- What are the restrictions on how the DCO is stored, preserved, displayed, and accessed throughout its life at the museum?
- What aspect of the DCO does the restriction apply?
- Start and end date of each restriction.
- Date that each restriction is to be reviewed (if applicable).
- Are there any agreed actions for the museum to ensure compliance with the stated restrictions?

3.2.1.3. Metadata requirements to be provided by donors and lenders

The information outlined in the table below is required to ensure the digital components of the DCO can be accessed, stored, managed, and digitally preserved now and in the future. The information is separated into two categories: [technical metadata](#) and [descriptive metadata](#).

All information described below as technical metadata can be automatically generated by the vendor, donor, or lender by creating a [filelist](#) of all digital files and folders³⁰ to be lent, donated or purchased. All information described below as descriptive metadata might be recorded in the digital file or folder, supplied in a separate [XML](#) file, or may be provided in a separate analogue or electronic document. Ideally the metadata file should be electronic and saved in the same folder as DCOs making up the acquisition or loan.

Also in the table below is a column indicating what metadata should be embedded in the digital file and what can be recorded in a separate file. The benefit of having technical metadata embedded in the digital file is that the metadata stays with the digital file at all times and is therefore less likely to get lost.

Information Type	Description	Example	Metadata Type	Embed in a digital file? Y/N	Essential/ Very useful?
Original filename and folder names	The name assigned to the digital files and the folder the files are supplied in. It is the name assigned by the creator of the file, prior to entry and not to be confused with any in-house file/folder name assigned after entry.	Chickens_v2_2015.mov map_of_british_isles.tif	Technical metadata	Yes	Essential
File size	The size of each digital file for each DCO in megabytes (MB), gigabytes, terabytes (TB) or petabytes (PB). This information is very useful during resource planning to calculate the total size of the deposit and the digital storage capacity required.	• 3 TB • 304 GB	Technical metadata	Yes	Very useful
File format	The file extension of each digital file. This information is required to inform future digital preservation actions.	• TIFF • REP • PDF • X3D	Technical metadata	Yes	Essential

³⁰ [See Section 2.1 of The National Archives' Digital Preservation Workflows](#) which provides a summary of software to undertake this, including DROID and Fido. Accessed 2023.

Checksum	A checksum for each digital file. This information is essential for use later on to carry out future fixity checks to confirm the integrity of the digital file after internal or external transfer. For further information see Section 12.2.3. Fixity checking .	120EA8A25E5D487BF687096440019	Technical metadata	Yes	Essential
Checksum type	The algorithm used to generate the checksum. The museum needs to know this so it can run another checksum on entry using the same algorithm.	MD5	Technical metadata	Yes	Essential
Copyright holder/s	Copyright holder/s that hold the copyright to all or part of the DCO.	Apple	Descriptive metadata	Yes	Essential
Terms and conditions	Record any terms and conditions agreed by the acquisition source or lender that describes how the museum must document, store, preserve, display, and otherwise use or re-use the DCO during its life at the museum. See step 2 for further information.	"The DCO must be exhibited using x hardware in accordance with the setup guide accompanying the work."	Descriptive metadata	No	Essential
Digital dependencies	Describe any technology (software or hardware), information or other factors that are required to ensure the DCO can be accessed, preserved, stored and experienced in the way the creator intended. It is a dependency if the DCO cannot be accessed, used, preserved or shared without it.	Technology dependencies example: virtual reality games require a virtual reality headset. Information dependency example: Metadata recording the encryption key to access the source digital files . Other examples: Some DCOs are constantly changing and evolving and need to be connected to the internet or an online social network.	Descriptive/technical metadata	No	Essential (if exists)
Authenticity	Proof that the digital files that make up the DCO are authentic. This may be particularly important for digital artwork.	A digital signature	Descriptive metadata	Yes	Very useful

3.3. Different methods of digital and physical entry

The details of object entry are not explicitly described in Spectrum, as this level of detail is not required for managing physical objects. However, it is necessary to describe them for digital collections, as there are a variety of ways in which the source digital files and any [supporting digital files](#) that make up the Digital Collection Object (DCO) may enter the museum. The list below outlines common methods of digital and physical/digital entry:

- 3.3.1. [Virtual entry - unmanaged](#):** Digital files may enter the museum using an unmanaged virtual method i.e. downloaded from an online source, an email attachment, or an encrypted URL link e.g. Vimeo. It is recommended that only trusted secure digital sources are used.
- 3.3.2. Virtual entry - [file transfer platform](#):** Digital files are uploaded and transferred onto a dedicated file transfer platform which manages and organises the stages of [file transfer](#), fixity, [file format validation](#), and receipt of files from the depositor to the museum.
- 3.3.3. Physical entry - digital storage:** Digital files arrive on a [physical digital device](#) e.g. hard drive or USB stick that is not considered part of the acquired DCO.
- 3.3.4. Physical entry:** The DCO has physical components e.g. a computer terminal or a video games console.

3.3.1. Virtual entry - unmanaged

<i>Order of Priority</i>	<i>Activity</i>	<i>Risk to digital collection if not actioned</i>
1	1.1. Use a dedicated workstation, ideally not connected to the museum IT network. You will need to temporarily connect the computer to the internet to receive the incoming digital files. 1.2. Ensure a digital quarantine has been set up and create a dedicated folder for each digital acquisition or loan event, so all the files received go into the same folder. 1.3. Create a separate folder in the acquisition folder for any problem digital files that will need to be re-supplied by the donor or lender e.g. corrupted files. 1.4. If the digital files are received with their own folder structure, this should be maintained. For further information see Section 2.3.2. <i>Setting up a digital quarantine environment</i>.	If files are not saved into a digital quarantine environment before they have been identified, scanned or fixity checked, the digital files could corrupt the IT network or other digital files saved in the same location.
2	2.1. Download and immediately save all source digital file, supporting digital files and original folders into the prepared folder in the digital quarantine location. 2.2. It is recommended that the download process is carried out twice to ensure the digital files are not corrupted at the point of download. 2.3. It is vital that no digital files are accessed until after a virus scan and a fixity check have been completed and no errors or issues have been found.	If the digital files are not saved into a dedicated folder for the acquisition, digital files could be easily mislaid, lost, deleted or not correctly documented.

3	Pointing the virus scanning software to the prepared folder in the digital quarantine location, without moving any digital files yet, follow the protocol for virus scanning. For further information, go to Section 12.2.1. Virus scanning .	A virus or malware compromises digital file/s or the whole filename IT network.
4	4.1. Consult the filelist provided by the donor or lender and check that each digital file and supporting digital file has a checksum and a checksum type. If a pre-entry checksum has not been provided, contact the donor or lender to request it. 4.2. If this is not possible, generate a checksum as soon as it is safe to do so. 4.3. Compare the checksums of the two downloaded copies. If the checksums match, delete one of the copies. 4.4. Compare the pre-entry and post-entry checksums. If they match then proceed onto step 5. For further information, go to Section 12.2.2. Fixity checking. 4.5 An optional step but recommended step, carry out file format validation. For further information go to Section 12.2.3. File format validation.	There is no evidence that information in the digital file has changed e.g. information is corrupted, missing, or damaged.
5	Once the fixity checks and virus scanning are complete, transfer digital files with errors to the folder for problem files. For further information on safely transferring digital files without losing data or damaging the digital file, go to Section 5.4.4.1. File copying software in the <i>Location movement and control</i> chapter.	These digital files are opened by mistake and corrupt other digital files or compromise the IT network.
6	6.1. If not already generated, generate a complete filelist of all digital files received. For more information, see Section 6.2.5. Extracting metadata for use in documentation. 6.2. Export the filelist to a CSV file. Include the date the filelist was run in the filename and save in the acquisition folder. 6.3. Compare the filelist provided by the depositor with the post-entry filelist and contact the donor if there are any discrepancies and arrange for correct files to be supplied if required.	No evidence that the right digital files and supporting digital files have been received.

3.3.2. Virtual entry - file transfer platform method

Order of Priority	Activity	Risk to digital collection if not actioned
1	1.1. The depositor uploads all source digital file and supporting digital files that form part of the acquisition or loan, onto the file transfer platform. 1.2. Using the dedicated workstation, using the filelist supplied by the donor/lender, check that all source digital file and supporting digital files used to ensure long term access and preservation of the DCO have been uploaded and no errors found during scanning and fixity checks. 1.3. If this is not the case, contact the depositor to arrange for the right files to be supplied.	The DCOs received do not match the DCOs authorised for donation or loan.
2	2.1. Ensure a digital quarantine has been set up and create a dedicated folder for each digital acquisition or loan event, so all the files received go into the same folder. For more information about how to manage file and folder names, see Section 7.4. File and folder names. 2.2. If the digital files are received with their own folder structure, this should be maintained. For further information, see Section 2.3.2. Setting up a digital quarantine environment.	If files are not saved into a digital quarantine environment before they have been identified, the digital files could mislaid or be lost.
3	3.1. The files are automatically virus scanned, fixity checked and validated. If any of these checks fails, the depositor must supply an alternative file that meets the stipulated technical specification.	N/A
4	4.1. Generate a complete filelist and export the filelist to a CSV file . Include the date the filelist was run in the filename and save in the acquisition folder. For more information, see Section 6.2.5. Extracting metadata for use in documentation .	No evidence that the right digital files and supporting digital files have been received.
5	5.1. Transfer the source digital files and any supporting files from the file transfer platform to the dedicated folder in the digital quarantine location. For further information on safely transferring digital files without losing data or damaging the digital file, go to Section 5.4.4.1. File copying software in the <i>Location movement and control</i> chapter.	If files are not saved into a digital quarantine environment before they have been identified, the digital files could mislaid or be lost.

3.3.3. Physical digital storage method

<i>Order of Priority</i>	<i>Activity</i>	<i>Risk to digital collection if not actioned</i>
1	1.1. The physical digital device is delivered to the museum using an agreed transport method. 1.2. Ideally the contents of the physical digital device should be transferred to a digital quarantine location on the same day the device arrives at the museum. 1.3. However, if this is not possible, the device should be labelled with an object entry number. See Section 3.4.2. Check and note the objects' condition, and any associated risks. below for creating an object entry receipt for DCOs that arrive at the museum on a physical digital device.	The physical digital device could be mislaid or the DCO and supporting files held on the device not identified or lost.
2	2.1. Use a dedicated workstation, not connected to the museum IT network, and ensure all the appropriate software has been installed. 2.2. If using a Write blocker³¹, ensure this is installed on your workstation before you proceed. 2.3. Ensure a digital quarantine has been set up and create a dedicated folder for each digital acquisition or loan event, so all the files received go into the same folder. For further information, see Section 2.3.2. Setting up a digital quarantine environment. 2.4. Create a separate folder in the acquisition folder for any problem digital files that will need to be re-supplied by the donor or lender e.g. corrupted files. 2.5. If the digital files are received with their own folder structure, this should be maintained.	The metadata or digital files held on the device could be corrupted or deleted.
3	3.1. Place the physical digital device into the appropriate reader or port on your workstation. 3.2. Pointing the virus scanning software to the device, without moving any digital files yet, follow the protocol for virus scanning every digital file on the device. For further information, go to Section 12.2.1. Virus scanning in the chapter on <i>Condition checking and assessment</i>.	A virus or malware compromises digital file/s or the whole IT network.
4	Consult the filelist provided by the donor or lender and check that each digital file and supporting digital file has a checksum and a checksum type. If a pre-entry checksum has not been provided, contact the donor or lender to request it. If this is not possible, generate a checksum as soon as it is safe to do so, then carry out a fixity check. For further information, go to Section 12.2.2. Fixity checking in the chapter on <i>Condition checking and assessment</i>. An optional step here is file validation. For further information go to Section 12.2.3. File format validation.	There is no evidence that information in the digital file has changed e.g. information is corrupted, missing, or damaged.

³¹ [Example of open source Write Blocker software for USB](#). Accessed 2023.

5	5.1. Once virus scanning and fixity checking has been carried out and it is safe to access the digital files, generate a filelist of the contents of the physical digital device. For more information, see Section 6.2.5. Extracting metadata for use in documentation. 5.2. Compare the pre-entry and post-entry filelists and check everything has been received in the correct format.	It is important to generate a filelist immediately to provide evidence of exactly what was received. Without a post-entry filelist, there is no proof of what digital files have been received.
6	6.1. Transfer all source digital file and supporting digital files and original folders that have passed virus scanning and fixity checks, into the prepared folder in the digital quarantine folder. For further information on safely transferring digital files without losing data or damaging the digital file, go to Section 5.4.4.1. File copying software in the <i>Location movement and control</i> chapter.	Although these digital files have been checked for viruses, the digital quarantine environment is an excellent place to hold all digital files that have not yet been fully documented and are still being tracked using the original file or foldername and the object entry or loan in number. If the digital files were not moved to the digital quarantine environment, there is a risk the files will be deleted or lost.

3.3.4. Physical entry

Step #	Step-by-step instructions
1	Follow the Spectrum <i>Object entry</i> procedure.

3.4. Creating an entry record and receipt

3.4.1. Make a record of the objects as soon as they arrive

Once all the digital files for the acquisition have been saved in the dedicated folder for the acquisition in the digital quarantine environment, the next steps can be taken below:

3.4.1.1. Digital files held in digital quarantine environment

<i>Order of Priority</i>	<i>Activity</i>	<i>Risk to digital collection if not actioned</i>
1	1.1. Compile a list of any digital files that are corrupted, in an incorrect format, do not meet the agreed specification, are not complete or any other issues. 1.2. Make arrangements with the lender, agent or acquisition source to delete/return the incorrect files and arrange re-supply of the correct digital files. 1.3. If digital files have been deleted or replaced, generate a new filelist, record the date in the filename and save in the acquisition folder. For more information, see Section 6.2.5. Extracting metadata for use in documentation.	If you acquired DCOs that are not to the agreed specification, the museum may not have the resource, expertise, or capacity to digitally preserve the DCO in the long term.
2	2.1. Create an entry record and receipt, listing all digital files and physical components that make up the whole acquisition or loan. 2.2. Attach a filelist produced immediately post-entry of all digital files received, including the original filename and file format. Next to each file describe any physical digital devices that the files arrived on and the title or object name of the DCO that the files relate to.	We do not have a record of what and when a DCO arrived.

3.4.1.2. Unchecked digital files held on physical digital devices

As explained in the previous section, although it is highly recommended that digital files arriving on [physical digital devices](#) are transferred to a digital quarantine environment on the same day the device arrives at the museum, this process should be followed if this is not possible.

<i>Order of Priority</i>	<i>Activity</i>	<i>Risk to digital collection if not actioned</i>
1	1.1. Record a description of the physical digital device and any external reference numbers. 1.2. Describe the contents of the DCO as described by the donor or lender, but state that the device has not yet been accessed and the content not yet been inventoried or checked.	If you acquired DCOs that are not to the agreed specification, the museum may not have the resource, expertise or capacity to digitally preserve the DCO in the long term.

3.4.2. Check and note the objects' condition, and any associated risks

For digital collections, condition checking involves carrying out [file format validation](#), [fixity checks](#) and [virus scanning](#) to confirm the integrity of the [source digital files](#) and other supporting files and ensure they are lossless, not corrupt, and behave correctly. This process has been described in the sections above, as digital files cannot be accessed until these checks have taken place.

3.4.3. Processing newly-arrived objects

<i>Order of Priority</i>	<i>Activity</i>	<i>Risk to digital collection if not actioned</i>
1	1.1. Follow the protocol described in Section 6.4. Producing an inventory to run a file format profiling tool, to check the digital files received are in a recognised format.	It is not possible digitally to preserve DCOs when we do not know what digital format and version they are on.

3.4.4. Tag the objects with a temporary label marked with the Entry number or Loan in reference number.

3.4.4.1. Digital files held in digital quarantine environment

<i>Order of Priority</i>	<i>Activity</i>	<i>Risk to digital collection if not actioned</i>
1	1.1. Append the folder name for the acquisition or loan with the <i>Entry number or Loan in reference number</i> . 1.2. It is essential that all the original file and folder names and the original order/structure of the folders/files is retained until the digital files are fully accessioned.	We cannot identify the digital files as the filenames do not describe the content.

3.4.4.2. Checked and unchecked physical digital devices

The [physical digital device](#) holding the source digital files for the DCO/s, should always be retained and stored at the museum as a backup copy. Before storing the devices, do the following:

<i>Order of Priority</i>	<i>Activity</i>	<i>Risk to digital collection if not actioned</i>
1	Mark the <i>Entry number or Loan in reference number</i> on the physical device.	We cannot track or identify the DCO.
2	Ensure all museum numbers are removed from the digital storage device if the DCO files are ever deleted from the device.	If the museum numbers are not removed, resource and storage space is being used up to manage a device with nothing on it.

3.4.4.3. Physical entry - standard process

Refer to the Spectrum *Object entry* procedure.

3.4.5. Record the first location of the objects

<i>Order of Priority</i>	<i>Activity</i>	<i>Risk to digital collection if not actioned</i>
1	Follow the protocol for creating a complete inventory in Section 6.4. Producing an inventory in the <i>Inventory</i> chapter.	You do not know what you hold.
2	Follow the protocol described in <i>Location and movement control</i> to transfer digital files from the digital quarantine environment to the dedicated digital collection storage environment . For more information about transferring digital files without losing data or damaging the digital file, go to Section 5.4.4.1. File copying software in the <i>Location movement and control</i> chapter.	Your DCOs and supporting digital files become corrupted or damaged over time and there is no copy to fall back on.
3	For an overview of best practice for creating and storing digital preservation copies, see Section 5.3.1.1. Digital preservation rules for creating and storing digital preservation copies .	Your DCOs and supporting digital files become corrupted or damaged over time and there is no copy to fall back on. The source digital files will be used for access, putting them at further risk of corruption or accidental deletion.

4. Acquisition and accessioning

Spectrum definition - taking legal ownership of objects, especially (but not always) to add to your long-term collection through the process of accessioning: the formal commitment by your governing body to care for objects over the long term.

For digital collections, this means acquiring and accessioning the DCOs - including the digital files and, if they are intrinsic to the DCO, any [physical digital devices](#).

4.1. Spectrum suggested procedure³²

Spectrum suggested procedure workflow	Is the step in the workflow different for digital collections?
Assessing potential acquisitions	
Make a case for the proposed acquisition.	Yes. See Section 4.2.1.
Evaluate the proposal.	Yes. See Section 4.2.2.
Obtaining title and recording copyright	
Obtain title to the objects and written evidence of this.	Yes. See Section 4.3.1.
Record copyright or other associated rights if known.	Yes. See Section 4.3.2.
Receiving objects not already with you	
Plan for the arrival of the objects.	Yes. See Section 4.4.1.
Processing new acquisitions	Yes. See Section 4.5.
Label or mark each object, or group of objects, with a unique object number.	Yes. See Section 4.5.1.
Record initial information about the acquisition and the objects acquired.	Yes. See Section 4.5.2.

³² Collections Trust. [Acquisition and accessioning - Suggested procedure](#). Accessed 2023.

If the objects were a gift, send acknowledgement to the donor.	No.
Accessioning new acquisitions	
If the objects are to be part of your accessioned collection, create a formal, tamperproof record that the objects have been accessioned.	No.

4.2. Assessing potential acquisitions

4.2.1. Make a case for the proposed acquisition

The acquisition proposal should be made in writing following the requirements for digital collections outlined in your acquisition policy. Resource and planning factors normally recorded in the proposal for the acquisition will have variations for DCOs and will include the following considerations:

- Are both parties (donor and museum) clear as to exactly what aspects of the DCO will be acquired? Is the organisation clear as to the boundaries of what is being collected/preserved and what is not? This is particularly important for social media, websites, databases and other digital eco-systems.
- Provenance and ownership of each element of the digital object. Can the owner/s be identified, is the concept of ownership recognised and can ownership be transferred to the museum?
- Proposal for digital storage and security of the object.
- The digital preservation approach and what that means regarding access to, interpretation and authenticity of the DCO.
- Rights clearances and legal and ethical issues relating to sensitive and personal data and content.
- Negotiate access requirements that are suitable for how the museum intends to display/use/share or intends museum visitors/user to interact with the DCO.
- Working with the artist/producer to select the most appropriate and preservable version/s or manifestation/s of the DCOs for acquisition. If relevant and appropriate, request to acquire the [source code](#).
- In consultation with the producer and other stakeholders, map out all the technical dependencies required to preserve and access the DCO now and in the future, such as [auxiliary objects](#). Research the availability and cost of purchasing and maintaining any software/hardware required to preserve and make DCO accessible and ensuring that this software/hardware can be maintained now and in the future.
- Look at collecting ephemera and user documentation that will enrich the interpretation and understanding of the DCO and feasibility of collecting and preserving this.
- Agree method of transfer and the pre-transfer protocol (e.g. [fixity checking](#) and [metadata](#) to be supplied).
- Consult with user communities and other stakeholders who have contributed or developed the DCO, possibly producing user testimonies to understand the DCO's significance to that community or wider society.
- Communicate with the donor to ascertain the production history of the DCO, i.e. how files were created, prior [format migration](#)s and emulations and the relationships between files to be supplied.
- Research to see if other collecting organisations are also preserving aspects of this DCO and work together to ensure the whole work is preserved.
- Is the donor providing any acquired or supporting software or auxiliary hardware in an [executable format](#)? If the format is not executable, can software be sourced from another collection or can it be created from the source code?
- If the DCO is evolving and relies on community interaction or interaction with the internet, will the DCO continue to be "live" and networked when acquired into the museum?

- Consider any ethical implications of acquiring the DCO. This is particularly an issue when acquiring social media or other personal or sensitive data.
- Consider the environmental impact of the DCO. NFTs are particularly damaging to the environment. For the further resources around the climate and museums, see the Museums Associations Climate resources bank³³

Refer to the *Decision Tree*³⁴ in the *Digital Preservation Coalition Handbook*.

For further questions to consider, also refer to the technical constraints decision trees published in the *Decisions Models Report*³⁵, produced as part of the *Preserving and sharing born-digital and hybrid objects from and across the National Collection* project.

Some useful ethical factors to consider when acquiring digital heritage are summarised by Arran Rees, Researcher at the University of Leeds, in the *Tops tips for ethical digital preservation* chapter of *Contemporary Collecting: An ethical toolkit for museum practitioners*³⁶.

Collecting some digital heritage, such as video games and community generated works, authorship may be difficult to track down. In the Executive Summary of the project report for *Preserving and sharing born-digital and hybrid objects from and across the National Collection*³⁷, the report highlights new challenges:

“To address the heritage of contemporary digital culture, museums recognise the need to liaise with new interlocutors in the technology and the creative industries, and to address barriers to collecting associated with privacy issues, intellectual property rights as well as the inaccessibility and invisibility of cloud-based services.”

In the project report for the project “*Preserving and sharing born-digital and hybrid objects from and across the National Collection*”, it is recommended that the curator also considers collecting any complementary documentation or ephemera that may support the interpretation and understanding of the DCO in the future, particularly if the museum is not confident that the DCO will be fully preserved in the manner the producer or community intended. The report authors remind us that the window of opportunity for gathering this documentation is particularly short for digital products, artwork and video games. The report also suggests the importance of liaising with communities who may have been central to the production or evolution of the digital object or may hold an important knowledge

³³ Museums Association. [Climate Resources Bank](#). Accessed 2023.

³⁴ Digital Preservation Coalition. [Decision Tree, Digital Preservation Coalition Handbook](#). Accessed 2023.

³⁵ [Preserving and sharing born-digital and hybrid objects from and across the National Collection. Decision Models Report](#). Gabi Arrigoni, Victoria and Albert Museum, Natalie Kane, Victoria and Albert Museum, Stephen McConnachie, British Film Institute, Joel McKim, Birkbeck University. January 2022. pp.13-16. Accessed 2023.

³⁶ [Contemporary Collecting: An ethical toolkit for museum practitioners](#). Ellie Miles, Susanna Cordner, Jen Kavanagh. Published by London Transport Museum. 2020. p.37. Accessed 2023.

³⁷ [Preserving and sharing born-digital and hybrid objects from and across the National Collection](#). Gabi Arrigoni, Victoria and Albert Museum Natalie Kane, Victoria and Albert Museum Stephen McConnachie, British Film Institute Joel McKim, Birkbeck University. 2022. p.4. Accessed 2023.

about how the digital object or eco-system has been used, developed, interacted, experienced or fetishised within a society, community or sub-culture. Their experiences, memories and narratives may help illustrate the social value of a digital object within our culture and in turn define its socio-historical significance and reason for collecting.

If it is likely that the acquisition candidate will be turned down on grounds of it being outside the museum's current collections policy, refer to further guidance in the Collections policy decision tree published in the *Decisions Models Report*, produced as part of the *Preserving and sharing born-digital and hybrid objects from and across the National Collection*³⁸ project.

4.2.2. Evaluate the proposal

The group or board which normally considers acquisitions may not have the appropriate knowledge or skills to assess the proposal in respect to special needs for DCOs, particularly in relation to ancillary materials and tools required for ongoing storage, preservation and access. In these circumstances, the proposal for storage and preservation of the object should be evaluated and approved in writing by the appropriate professional within the organisation (for example, this may be a member of staff within the IT department, or an external expert who can supplement the knowledge of collections care staff)

4.3. Obtaining title and recording rights

4.3.1. Obtain title to the objects and written evidence of this

Property law pre-dates digital technology and references physical chattels. For this reason, it is important that the document used to transfer title references the physicality of the digital components of the collection object, as well as the name of the object. This is likely to be in the form of the file list provided with the object attached to the transfer of title document and the physical carrier for the files if that is regarded as part of the object. For further details of how to record each component, see [Chapter 3. Object entry](#).

4.3.2 Record copyright or other associated rights if known

DCOs may have a wider range of applicable intellectual property rights attached than copyright. These may often include database rights and design rights, and sometimes patents and trademarks. The purpose of the acquisition recorded in the proposal should inform the rights clearance approach taken by the museum with the rights holders. For further guidance, see the *Legal chapter*³⁹ of the Digital Preservation Coalition Handbook and [Chapter 19. Rights management](#) for further details.

³⁸ [Preserving and sharing born-digital and hybrid objects from and across the National Collection. Decision Models Report](#). Gabi Arrigoni, Victoria and Albert Museum, Natalie Kane, Victoria and Albert Museum, Stephen McConnachie, British Film Institute, Joel McKim, Birkbeck University. January 2022. p.19. Accessed 2023.

³⁹ Digital Preservation Coalition. [Legal Chapter, Digital Preservation Coalition Handbook](#). Digital Preservation Coalition. Accessed 2023.

4.4. Receiving objects not already with you

4.4.1. Plan for the arrival of the objects

Planning for the arrival of potential digital acquisitions, should be consistent with planning for the arrival of digital objects for other purposes. For more detailed information on these processes, see [Chapter 3. Object entry](#).

4.5. Processing new acquisitions

4.5.1. Label or mark each object, or group of objects, with a unique object number

DCOs cannot usually be physically marked, therefore the method for attaching the object number will differ to that of physical objects. The following methods may be used and appropriateness will vary according to the DCO:

1. Your digital asset management or preservation system may allow you to store files within a named folder. If so, following guidance in [Section 7.4. File and folder names](#).
2. If the [physical digital device](#) on which the object is stored is intrinsic to the object, then the object number may be physically marked on the sleeve or box in which the object is permanently stored.

4.5.2. Managing very large acquisitions

It is worth having a plan in place to manage very large acquisitions of digital objects. Although it is common practice to go through large physical acquisitions before they enter the museum, the donor or agent may not have the equipment on site to access or play the DCOs so this might not be possible.

The archive sector has a practice called post-entry appraisal which might be a useful principle to employ in these circumstances. The digital objects are brought on site and assigned a corporate asset number, to make it clear they are not yet part of the registered collection. When the curator is able to access the DCOs, an appraisal is carried out to agree what DCOs will be accessioned and what DCOs will be returned to the donor.

4.5.3. Record initial information about the acquisition and the objects acquired

Unit of Information	Why is this important for digital collections?	Referenced in Spectrum or PREMIS?	Min Req? Yes/No
<i>Object identification information</i>	See Section 6.3. Checking you have core information for details of object identification information for DCO and their corresponding digital and physical components.	N/A	N/A
<i>Acquisition information</i>	Same principles apply as with physical collection. See <i>Record initial information about the acquisition and the objects acquired</i> section of the Spectrum <i>Acquisition and accessioning</i> procedure. Acquisition information must be associated with the catalogue record for the source digital files, which make up the DCO as the point of object entry. Acquisition information must not be associated with a catalogue record for any digital preservation derivative files created after object entry to preserve the DCO.	N/A	N/A
<i>Part of object restriction applies:</i> ● <i>Use restriction</i> ● <i>Use restriction start date</i> ● <i>Use restriction end date</i> ● <i>Use restriction note</i>	Same principles apply as with acquired physical objects. However, the rights associated with a DCO tend to be more complex and may prohibit or restrict even basic collections management activities such as migration, duplication, storage and public access. Therefore these units of information are essential when the DCO is in copyright or under another right restriction. The part or aspect of the DCO in which the restriction applies must be described. For example, the software of a videogame or soundtrack of a film. See <i>Rights management</i> section for information requirements for managing generic rights information relating to DCOs.	Spectrum <i>Object Use information</i>: ● <i>Use restriction</i> ● <i>Use restriction date</i> ● <i>Use restriction note</i>	Yes (when the object is in copyright or other rights)
<i>Object owner's contribution information</i>	Same principles apply as with physical collection.	N/A	N/A

5. Location and movement control

Spectrum definition - keeping a record of where all the objects in your care can be found, and updating the location each time an object is moved.

For digital collections, this means recording the locations of the DCOs - including the digital files and, if applicable, any [physical digital devices](#). It also involves the storage of the digital files.

5.1. Spectrum suggested procedure⁴⁰

Spectrum suggested procedure workflow	Is the step in the workflow different for digital collections?
Identifying and describing locations	
Give each display and storage location a unique name or number.	Yes. See Section 5.2.1.
Record key information about each location.	No.
Maintain your location system.	No.
Recording locations of objects	
Record the location of all objects.	Yes. See Section 5.3.1.
Moving objects	
Obtain and record authorisation for all moves.	Yes. See Section 5.4.1.
Check the objects' condition to make sure they are fit to be moved.	Yes. See Section 5.4.2.
Check whether there are any specific risks or recommendations associated with handling or moving the objects.	No.
Find out whether there are any access problems anywhere along the route and assess any handling issues or other risks.	No.
Arrange any conservation or packing needed to make the objects safe for the move.	No.

⁴⁰ Collections Trust. [Location and movement control - suggested procedure](#). Accessed 2023.

If transport is involved, establish, and agree on the most appropriate means. If no transport is involved, move objects (then go to 'Update object location records').	Yes. See Section 5.4.3.
Arrange insurance or indemnity for objects being transported.	No.
Prepare appropriate documentation to accompany objects being transported.	No.
Transport objects, and then confirm their safe arrival.	Yes. See Section 5.4.4.
Update movement and object location records.	No.
Return to the linked procedure that prompted the move.	No.

As with physical collection objects, the museum acting as legal custodian must put suitable procedures and systems in place to ensure that all DCOs in its care can be accounted for and accessed throughout its life within the museum.

Accessibility becomes a vital factor with regards to managing DCOs within a museum collection. If a DCO cannot be opened, identified, transferred, or stored, it cannot enter the museum collection or be preserved in any way. Therefore, the short- and long-term access needs of DCOs require ongoing review, planning and management.

5.2. Identifying and describing locations

5.2.1. Give each display and storage location a unique name or number.

5.2.1.1. Physical digital devices

Some digital files related to Digital Collections Objects (DCOs) are stored on a [physical digital device](#) such as a hard drive or USB stick. Any such devices that are not considered part of the accessioned collection (only what they contain is accessioned) operate as digital storage units. For this reason, the physical digital device should be documented and managed in much the same way as other physical housing and not as objects in their own right, e.g. an acid-free box.

Each digital device used to store the DCOs should be recorded as part of the location of the DCO and allocated a unique location name or number. Create a unique name or number for the digital device, when the device is actively holding a copy of the DCO. Document the location name or number as [obsolete](#) if/when the device becomes "inactive" and no longer holds a copy of the DCO.

It is also recommended to label the physical digital device with the object numbers of the DCOs currently held on it.

An exception to this rule should be made for digital devices that are considered part of the DCO, e.g. if an artist has decorated the USB stick that the digital artwork arrived on. In these cases, the device should be considered a physical component of the DCO. See *II. Physical components of the DCO* below.

5.2.1.2. Physical components of the DCO

For DCOs which have a physical presence or have physical components considered to be part of the accessioned collection, follow Spectrum procedure.

5.2.1.3. Digital files with no physical storage

If the digital files are held on a server, record the file path to the server or folder on which the [source digital files](#) are held. If the digital files are held in archival digital storage and retrieved using a DAMs or Digital Preservation system, create a digital location for the archival storage to prove that the digital files are being managed and tracked within this workflow.

5.3. Recording locations of objects

5.3.1. Record the location of all objects

The main aim of location control for digital collections is to ensure that the [bits](#) that render the Digital Collection Object (DCO) at the point of object entry continue to be retrievable, auditable, and accessible and continue to provide a faithful render of the DCO over its lifetime at the museum.

Bits are organised and stored on a digital file or a piece of hardware (e.g. iPhone or computer), which render them to create the DCO. In 1 to 10 years' time, the digital carrier will become [obsolete](#) and will no longer be able to render the bits to provide access to the DCO. At that point, the bits will be [migrated](#) onto a new digital preservation format which will also need to be audited and tracked. Therefore, it is not enough to just account for the [source digital files](#) but the museum must also account for all [digital preservation derivatives](#) created to digitally preserve and continue to provide access to the DCO.

If the museum were to only manage and track the source digital files, but those files were obsolete and were no longer able to provide access to the DCO and the derivatives had been mislaid, then the museum would no longer be able to access or preserve the DCO. So the purpose of location control for digital collections should be to track the bits, not the digital [file formats](#) that temporarily render those bits.

As access to a DCO is not implied as it is with most physical objects, the museum must also have a system in place to identify which derivative is currently being deployed to provide the most faithful render of the DCO. It must also describe any hardware, software, metadata, or other files that the digital files are dependent upon to enable access to the DCO.

How a location is described depends on how the digital files are stored and the systems and procedures in place to manage and retrieve digital files in the museum.

5.3.1.1. Digital Preservation rules for creating and storing digital preservation copies

For further information, see the “Storage” chapter of the *Digital Preservation Handbook*⁴¹. DPC have also created a very useful video⁴², describing this process.

No.	Activity	Risk is not actioned
1	As a minimum, make 2 complete copies of each source digital file, as soon as the files have been virus and fixity checked. Ideally, make at least 3 exact preservation copies of each source digital file.	Digital files are at greater risk of corruption or bit rot .
2	- Ensure the copies are stored in locations that are geographically separate, e.g. a server on different sites. - Ensure the copies are held on different types of storage media, using a mix of online systems and offline media.	In the event of a natural disaster the servers holding all the copies of the collection could be damaged or destroyed and the whole collection would be lost.
3	- Run regular fixity checks on all DCOs in the collection to continually monitor the digital integrity of all the copies. - For further information, see Section 12.2.2. Fixity checking.	Copies become corrupted and unusable if no action is taken.
4	Continue to monitor storage technologies for risk of obsolescence and make a plan to migrate to new storage technologies. For further information see Section 12.2.5 Monitoring storage.	Storage media used to store the collection becomes obsolete, rendering the digital collection store on it inaccessible.

⁴¹ [Storage. Digital Preservation Handbook. Digital Preservation Coalition](#). Accessed 2023.

⁴² [Basics of fixity checking. Digital Preservation Coalition](#). Accessed 2023.

5.3.1.2. Location control process by storage medium

Below is a summary of the different processes for managing location control for DCOs. The process is different, in accordance with the physical and digital makeup of the DCO and how various copies and [digital preservation derivatives](#) have been stored.

Storage medium	Definition	Process for recording locations
Digital file stored on a digital storage environment	All digital files or software files that make up the DCO are not stored on a physical digital device but stored 'virtually' on the museum's digital collection storage environment , e.g. an IT server or a digital preservation infrastructure.	Museums using a non-specialist storage solution (e.g. server) - record the persistent file path for the location of the digital file on the server. e.g. Digital collections/Permanent collection/D02250 Museums with a dedicated digital preservation infrastructure/system - A location is not required once the file has been ingested into the system if the system is able to track and retrieve files at all times and provide an audit trail of these digital files. However, it is useful to record the name of the system used to track the digital files.
Digital file stored on a physical digital device	Some digital files related to DCOs are stored on a physical digital device such as a hard drive or USB stick. Any such devices that are not considered part of the accessioned collection, operate as digital storage units, holding a copy of the DCO files.	The same rules apply as recording the locations of physical objects stored in physical housing, e.g. an acid-free box. Each digital device used to store the DCOs should be recorded as part of the location of the DCO and allocated a unique location name or number. Uniquely describe the physical digital device as the current location of the digital file. Ensure that the current location of the digital carrier is also described.
Physical digital devices or hardware considered part of the DCO	The DCO may be a physical device or piece of hardware, which may or may not have software installed onto it, e.g. iPhone 1 with iOS software installed, a Dot matrix computer or a USB stick containing 3 TIFF files, decorated with a design.	For the acquired hardware, the same rules apply as recording the locations of other physical objects.
DCO containing physical components	A DCO that is made up of separate physical and digital components, e.g. Art installation with MOV file to be played on a screen as part of a physical installation with a set of vases.	For the set of vases, the same rules apply as recording the locations of other physical objects.

5.4. Moving objects

For DCOs) with physical components or containers, the same rules apply as with other physical objects. When transferring DCOs on a [physical digital device](#) between organisations as part of a loan or new acquisition, hard-drives are the most reliable medium. TB hard-drives are the best option to safeguard against downloads failing, when the internet connection is not reliable.

For DCOs without physical components or physical digital devices, the concept of moving does not directly apply. [File transfer](#) is the closest equivalent [digital preservation action](#), which involves creating an exact copy of a file/s in location 'x' to be transferred to a new location 'y'. The file is not moved as the file is not removed from location 'x' to appear in location 'y'. It is copied to ensure that if the transfer of the file did not work, it can be repeated and the information in the file is not lost. It is digital preservation best practice to create at least 3 exact copies of the [source digital file](#).

File transfers are subject to a similar process of authorisation and checks that are required prior to a physical move, see sections below for details.

5.4.1. Obtain and record authorisation for all moves

The transfer of files relating to the DCO may be subject to authorisation, depending on the level of risk to the organisation and to the DCO. Consider who in the organisation has the expertise and seniority to authorise digital preservation actions and housekeeping.

5.4.2. Check the objects' condition to make sure they are fit to be moved

For information about the actions to be taken to ensure the digital files making up the DCO are safe from viruses, data loss, corruption, [bit rot](#), [obsolescence](#) and other risks, see [Chapter 12. Condition checking and technical assessment](#) and [Chapter 13. Collections care and conservation](#).

Before the digital file is transferred, carry out the following checks:

- Check the digital files have been virus-checked. If not, follow the protocol described in [Section 12.2.1. Virus scanning](#).
- Check documentation for a [checksum](#) and [checksum type](#). If there is no checksum, generate one before proceeding. See [Section 12.2.2. Fixity checking](#).
- Ensure an inventory of all source digital files and supporting files have been carried out. See [Chapter 6. Inventory](#) for further details.
- Check that all the digital files required to access the DCO that form one copy are collated and put together in one digital folder.

5.4.3. If transport is involved, establish, and agree the most appropriate means

Establish the safest and most secure method of [file transfer](#) to ensure the following:

- The digital files and supporting files are transferred with no data loss or corruption.
- The digital files are secure from hackers and file corruption. You may want to think about encrypting the digital files.
- The digital files that make up the DCO can be put together and accessed in the correct order.
- The digital files can be interpreted, accessed, and rendered in the intended way.

5.4.4. Transport objects, and then confirm their safe arrival

5.4.4.1. File copying software

Before transferring, or copying, digital files from one digital location to another, it is recommended you use file copying software that will create an exact copy of the digital file and will ensure all [technical metadata](#), including dates are not altered. Some software also carries out a [fixity check](#) to provide evidence that the digital file is exactly the same. There are plenty of free open source tools available online. An application called *Exactly* produced by AVPreserve⁴³ is a good example.

The *Digital Preservation Workflows*⁴⁴ resource produced by The National Archives, provides useful information about this process, and recommends tools used in the GLAM sector for this purpose.

5.4.4.2. File integrity checks

If the file copying software does not include a fixity checking function, immediately after the [file transfer](#) has taken place, the new copy of the digital file should be fixity checked. For further information, see [Section](#)

[12.2.2. Fixity checking.](#)

⁴³ [Exactly. AVPreserve](#). Accessed 2023.

⁴⁴ [Preserve - Digital Preservation Workflows](#). The National Archive. Accessed 2023

6. Inventory

Spectrum definition - making sure you have the basic information to be accountable for the objects in your care, and tackling the backlog if you do not.

For digital collections, this means capturing a minimum level of [Metadata](#) about the DCOs. For the digital files, some of this metadata can be extracted from the files.

6.1. Spectrum suggested procedure⁴⁵

Spectrum suggested procedure workflow	Is the step in the workflow different for digital collections?
Having the primary procedures in place	
Checking you have core information	
Do you have core information for every object (or group)?	Yes. See Section 6.3.1.
Create a plan for tackling any inventory backlog.	No.
Producing an inventory	Yes. See Section 6.3.
Go around the locations you are inventorying and list every object (or group) in them.	No.
Does the object have a number marked on it or on a label?	No.
Create or update records for objects that have accession numbers.	No.
Checking discrepancies	
Try to identify objects with temporary numbers.	No.
Mark or label any objects identified this way with its number.	No.
Update or add core information (including location).	No.

⁴⁵ Collections Trust. [Spectrum. Inventory - suggested procedure](#). Accessed 2023.

Resolving outstanding problems	
Decide how to deal with unidentified objects.	No.
Metadata	Not part of Spectrum. See Section 6.4.

6.2. Checking you have core information

6.2.1. Do you have core information for every object (or group)?

The following units of information should be recorded in the museum's core inventory as a minimum requirement and are vital to ensure the museum's digital collection is managed in accordance with Spectrum and digital preservation best practice. For digital components, some of the information required for a basic inventory can be extracted from the [technical metadata](#) in the file, by creating a [filelist](#) (see section 6.1 above). The table below indicates which data can be extracted from the file and which information will need to be verified using a different source.

The whole DCO should have a separate catalogue record in your CMS or the system you use for documenting the accessioned collection. Separate digital and physical elements that make up the DCO should have separate catalogue records that are linked in a "parent/child" relationship. For further information see [Section 7.2.1. Create a record for each object, or group of objects, accessible by object number](#) in the *Cataloguing* section of this resource.

Some of the information requirements are the same as the core information requirements stipulated in Spectrum, but some are unique to digital collections.

6.2.1.1. Object identification Information - Digital collection object (Level 1)

Unit of Information	Description	Example	Equiv. info. req. in Spectrum Core inventory	Can you extract this from the technical metadata?
Object number	Object number of the DCO.	C-25315	<i>Object number</i>	No
Current folder name	This is the folder name of the folder holding all the digital files relating to one DCO. This should conform to the museum's inhouse filename conventions and reference the object number of the DCO.	C_25315.In_the_Eyes_of_the_Animal.Marshmallow_Laser_Feast	N/A	Yes
<i>Object name</i>	Name of collection/ Digital Collection Object (DCO)	Immersive virtual reality art installation	<i>Object name</i>	No

Number of digital files	Number of digital files that make up the collection or DCO, including metadata and other supporting files required to render the DCO as perceived by the artist, designer or producer. Only count the number of digital files from that version or copy of the DCO.	8	<i>Number of objects</i>	Yes
Number of physical components	Number of physical components that make up the collection or single DCO. This should include the hardware and other physical components used to create the DCO as perceived by the artist, designer or producer.	3		No
Brief description	Brief description of the DCO as experienced by the user. This is not absolutely essential for simple DCOs such as TIFF files. It becomes more essential when describing more complex DCOs. In some cases, it might be useful to briefly describe, for example, how the DCO will be experienced/played/accessed/viewed.	An immersive virtual reality art installation, where users embody the visual and sensory perspectives of different creatures—a midge, then a dragonfly, followed by a frog, and finally an owl. Set in a real forest, users wear an Oculus Rift VR headset which has been decorated with wood and moss, and a haptic “rumble pack” which allows the users to feel vibrations of the animals they embody.	<i>Brief description</i>	No
Digital dependencies	Record any metadata, hardware (auxiliary objects) or software essential to render or put together the DCO, as perceived by the designer, producer or artist. Examples include: Encryption keys for encrypted files; XML files with metadata explaining how the digital files are put together to form the whole; the make and model of hardware used to access; proprietary software ; source code for the software; artist/maker documentation for object handlers; any other essential equipment (analogue/digital) required, without which the DCO could not be rendered/played/experienced/viewed etc.	• Metadata files • 360 degree video • Oculus Rift VR headset (acquired) • “Rumble” pack (acquired) • Nvidia Quadro P6000	N/A	No
Recorder and recording date	The username and date of the individual who created the catalogue record.	Walkers; 2021-04-25	<i>Recorder and Recording date</i>	No

6.2.1.2. Object identification Information - Digital and physical components (Level 2 and 3)

At the inventory stage, digital and physical components only relate to the acquired digital and physical components, e.g. the [source digital files](#), acquired hardware at the point of entry. At the point of fully cataloguing the DCO, each [metadata](#) file, hardware, software etc essential to render or put together the DCO (as designed in the [Digital dependencies](#) field in the main catalogue record, should have eventually have its own catalogue record. For further information, see [Chapter 7. Cataloguing](#).

Unit of Information	Description	Example	Equiv. info. req. in Spectrum Core inventory	Can you extract this from the technical metadata?
Object number	Unique number used to track the component in the museum.	C-25315.1	<i>Object number</i>	No
Original filename/folder name (digital only)	Filename of the digital file. For source digital files, this is the original filename assigned on entry. For digital preservation derivative , this is the filename assigned by the museum.	In_the_Eyes_of_the_Animal_1_of_8.WAV OR Weird_file_name_given_by_donor 01 chicks2.WAV [as long as there are no illegal characters]	N/A	Yes
Current folder name (digital only)	This is the folder name of the folder holding all the digital files relating to one DCO. This should conform to the museum's inhouse filename conventions and reference the object number of the DCO.	C_25315.In_the_Eyes_of_the_Animal.Marshmallow_Laser_Feast	N/A	Yes
Current location	For digital files stored virtually, this is the persistent file path or if there is a dedicated system or infrastructure for managing digital files, simply record the name of the digital collection storage environment the DCO is being managed within. For digital files stored on physical digital devices and other physical DCOs, this is the current physical location of the device or DCO. For further information, see chapter on <i>Locations and movement control</i> for more information.	Permanent digital archive	<i>Current location</i>	No
Legal Status	Record the legal status of the digital file. If the digital file is the acquired source	British Film Institute	<i>Current owner</i>	No

	digital file, the status would be “permanent collection” or the equivalent status used by your museum to describe the accessioned collection. You may also wish to consider/compare notes with museum sector colleagues on assigning “permanent collection” status to one/all copies of digital preservation derivatives, e.g. if the digital file is an exact copy of the source digital file or when the source digital file becomes obsolete and the bits from the source digital file are transferred to a new preservation format.			
Checksum (digital only)	Record the Checksum for the digital file. For source digital files, ideally this should be provided at acquisition by the acquisition source. For further information, see Section 12.2.2. Fixity checking.	120EA8A25E5D487BF68B 5F7096440019	N/A	Yes
Checksum type (digital only)	The algorithm used to generate the checksum. This is important, so we know how to recreate the same checksum. For further information, see Section 12.2.2. Fixity checking.	MD5	N/A	Yes
File Format (digital only)	Describe the file format of the digital file.	WAV	N/A	Yes
File format profiling tool (digital only)	The name of the file format profiling tool used to recognise the file format.	DROID	N/A	No
Is the file format recognised? (digital only)	Using a file format profiling tool, such as DROID, to scan and identify the file format.	Yes	N/A	No
Size of the digital file or group of files in GB/MB (digital only)	Size of the digital file or the total size of the digital file collection.	30.28 MB	<i>Dimensions</i>	Yes
original/ digital preservation derivatives (digital only)	Record if the digital file is the original source digital file that was originally acquired or if the digital file is a copy of the “original” made post entry for the purposes of digital preservation.	Original	N/A	No
Physical or digital?	Record if the component is in a physical or digital state. Describe the state of that version or copy. If the digital file is held	Digital	N/A	No

	on a physical digital device, record that the element is digital as the acquired DCO element is digital, only the container or device is physical. Consider how to categorise computers and other acquired hardware. You may wish to categorise as physical as it has a permanent physical state. This becomes extremely useful if you need to search all born digital objects for example (for storage/resource planning etc) or for carrying location audits on physical collections.			
Make and model (hardware only)	Describe the make and model of the hardware, e.g. Apple iPhone 8 or Macintosh LC II.	N/A	Yes	No
Recorder and recording date	The username and date of the individual who created the catalogue record.	Walkers; 2021-04-25	<i>Recorder and Recording date</i>	No

6.3. Producing an inventory

Use the digital collections section of the museum's documentation plan, as a starting point to ascertain where the digital collections are held and if they have been fully accessioned. For further information, see [Section 11.2. Writing your documentation plan.](#)

Once the digital files and other components of the DCO have been [virus scanned](#) and [fixity checked](#), follow the steps below to create an inventory, using a [filelist](#). However, please note that disk imaging is an alternative way of copying and listing content of [physical digital devices](#), particularly for older media. Some software, such as [BitCurator](#), can create an exact copy of the contents of the media, including the original metadata.

Order of Priority	Activity	Risk to digital collection if not actioned
1	Using the appropriate workstation or standard PC, make sure a filelist software has been installed, if required.	N/A
2	2.1. Check if a filelist has been created for the set of digital files to be inventoried and the date it was created. 2.2. If a recent filelist does not exist, use a filelist software to create a basic filelist of all files and folders in each location in scope. 2.3. Export the filelist into a CSV file and save somewhere safe. Record the date the filelist was created in the filename. For more information, see Section 6.2.5. Extracting metadata for use in documentation.	We cannot account for the digital files we hold.

3	3.1. Some open source tools for extracting metadata such DROID and Fido will also identify the file formats. 3.2. Export the report to CSV and save it somewhere safe. Record the date the file format profiling tool was run in the filename. 3.3. Flag up any digital file formats that are not recognised file formats. 3.4. Record the file format for each file in the inventory record. 3.5 If you are concerned about file format obsolescence then please see Section 13.3. Carrying out Conservation. 3.6 At this point, you may consider creating access or re-use copies. For more information, see Section 20.2.1 Access and re-use copies.	It is not possible to check if we have all the right information, software or hardware to access the files if we do not know the details of the format.
4	4.1. Check the filelist and accompanying information to check that all the core inventory information listed in Section 6.2. Checking you have core information is present. You may need to open the file manifest or supporting metadata file to access some information. 4.2. If a checksum has not been recorded for the digital file, a checksum will need to be generated immediately. For further information, see Section 12.2.2. Fixity checking.	The digital file loses digital information during or before digital entry into the museum and as no fixity check was carried out, there is no proof that the damage occurred during or prior to entry, therefore the previous owner is not liable.
5	5.1. Using required hardware or software, access each source digital file to check that the DCO is accessible and the contents of the files matches the DCO listed on the object list for the loan or acquisition. 5.2. Check the DCO is complete, there are no issues with the technical integrity and the DCO matches the description in the CMS.	Without checking the DCO with the human eye, we cannot guarantee that we have received the correct DCO and there are no issues with the technical integrity of the DCO.

6.4. Metadata

Just as you would record information about the physical form of an object alongside information about its conceptual and cultural meaning, so too is it important to record information about the digital form which an object takes. This information is called [metadata](#). It is structured data that is either embedded in the digital file itself or contained within a supporting file.

There are two broad types of metadata: Technical metadata, and Descriptive metadata.

6.4.1. Technical metadata

Technical metadata describes technical attributes and descriptions of a digital file or digital object that is created either automatically by the technical device that produced it or manually by a human.

For DCOs with no physical component, this is usually information about the basic properties of the file(s), e.g. [file size](#), number of files, folder structures, or more detailed technical data stored in the files themselves, e.g. file type, format and encoding information. For DCOs with both physical and digital components, the technical metadata is likely to be a combination of both metadata held in the digital files and separate metadata files holding technical descriptions of the storage media/hardware that holds the digital files.

Examples of technical metadata:

- *File size*: the size of each digital file.
- *Number of files*: the number of digital files that make up the DCO.
- *Folder structure*: Structure of the folders holding digital files making up the DCO.
- *Filename*: the name automatically assigned to the file by the device that created it.
- *Created date*: the date the digital file was created.
- *Device*: the device or computer program used to create and encode/decode the file. e.g. make and model of the digital camera, scanner, or phone.
- *Format*: the format of the digital file, e.g. TIFF, PDF, MOV, CAD.

6.4.2. Descriptive metadata

This data is always recorded by a human, and describes the function or conceptual value or meaning of an object and its cultural or social context, e.g. who made it, when it was created and the purpose of its creation, past ownership.

It is either manually added to the digital file or recorded in a separate metadata file that accompanies the DCO or has been recorded elsewhere. It is normally used by a previous owner or user of the digital file to describe meaningful attributes of the file content or file that are required but not part of the [technical metadata](#).

Examples:

- Title of the DCO.
- Creator or artist name.
- Copyright holder.
- Copyright date.

6.4.3. File headers

A lot of important [metadata](#) is held in the file header of a digital file. A file header is a 'signature' placed at the beginning of a file, so the operating system and other software know how to access and render the contents of the digital file. [Descriptive metadata](#) relating to the hold digital file can also be held here.

6.4.4. Metadata standards

There are plenty of online resources available that describe the different [metadata standards](#) available. *What information should I record?*⁴⁶ produced by the Collections Trust, is a good starting point for reviewing what each standard is used for.

⁴⁶ [What information should I record?](#) Collections Trust. Accessed 2023.

6.4.5. Extracting metadata for use in documentation

There may be a lot of metadata either embedded in the [source digital files](#) or in accompanying metadata file, that will be useful when preserving and cataloguing the DCO. This metadata can be used to create basic catalogue records with very little manual intervention. There are many open source applications available that will extract basic [technical metadata](#) from digital files⁴⁷ and export it into a format that can be imported back into your CMS or DAMs. Most collections management systems have a facility for importing data in bulk, to create new or update existing catalogue records. A [CSV file](#)⁴⁸ or [XML file](#) are [file formats](#) commonly used to import metadata into the CMS to create new catalogue records. However, this method only works if there are the right fields in your CMS to record the metadata, so some development may be required to ensure the right fields are available.

In most cases the exported metadata will require interpretation or amendment prior to import into the CMS, to be understood and to ensure the data adheres to in house data standards. Factors to consider:

- Although metadata is structured and consistent for digital files created by the same device, metadata may be inconsistent across different devices.
- Technical metadata should comply with a [metadata standard](#) so the units of information captured will be consistent if the same standard has been applied.

6.4.6 Accessing complex metadata

Due to the volume and variation of metadata held in [file headers](#), it is not always realistic to record all such data in your DAMS or CMS, as the information may be useful for the future, but may not need to be searchable with these databases. This poses the question of what to do with metadata that is not extracted from a file at the point of acquisition.

There are a few options when dealing with this question. The simplest approach is effectively to do nothing, and accept that full access to file header metadata will only be possible when the digital files are accessed. However, this approach takes time and may not be feasible if large quantities of files are involved.

Another option is to create a separate file to store a copy of this metadata, using an [open file format](#) such as XML or JSON. This approach means that the file can be associated with your object record, but stored independently of the object itself, the advantage being that you can retrieve this file and assess its content far faster than the process of retrieving and assessing the digital object itself. In effect this metadata file becomes another form of documentation for your DCO.

⁴⁷ See Step 2.1 of The National Archives. [Digital preservation workflows](#). Accessed 2023.

⁴⁸ [DIRLister is a good example](#). Accessed 2023.

7. Cataloguing

Spectrum definition - managing the information that gives your collections meaning, not as an end in itself but to record and retrieve what is known about your objects.

For digital collections, this means expanding your inventory record to create a comprehensive catalogue record for the DCOs - including the digital files and if applicable, any [physical digital devices](#).

7.1. Spectrum suggested procedure⁴⁹

Spectrum suggested procedure workflow	Is the step in the workflow different for digital collections?
Creating catalogue records	
Create a record for each object, or group of objects, accessible by object number.	Yes. See Section 7.2.1.
Add other important information.	No.
Provide access to records via indexes.	No.
Maintaining catalogue records	
Maintain links or cross-references to relevant information recorded during other procedures.	No.
Keep the catalogue secure, including digital backups and paper copies.	No.
Improving catalogue records	
Add information from documentation projects.	No.
Add information from a collections review.	No.
Add information arising from research, interpretation or other use.	No.
Guidance Notes	
Note 1: Catalogue records	No.

⁴⁹ Collections Trust. [Spectrum, Cataloguing - suggested procedure](#). Accessed 2023.

Computerised databases.	No.
Pre-printed catalogue cards.	No.
Note 2: Object history files	No.
7.3. Data structure for digital collections	Additional requirement for DCO. Not part of the Spectrum procedure.
7.4. File and folder names	Additional requirement for DCO. Not part of the Spectrum procedure.

7.2. Creating catalogue records

7.2.1. Create a record for each object, or group of objects, accessible by object number

The catalogue records described in this chapter should be used to describe the Digital Collection Object (DCO), and all its digital and physical components. Within each catalogue record type, separate units of information have been recommended, which should be captured in the cataloguing system used to document the museum's accessioned collection. If the museum has a Digital Asset Management system (DAM) or a Digital Preservation System, it is recommended that the technical information relating to the digital file is recorded in that system.

7.2.1.1. Overview of catalogue record types

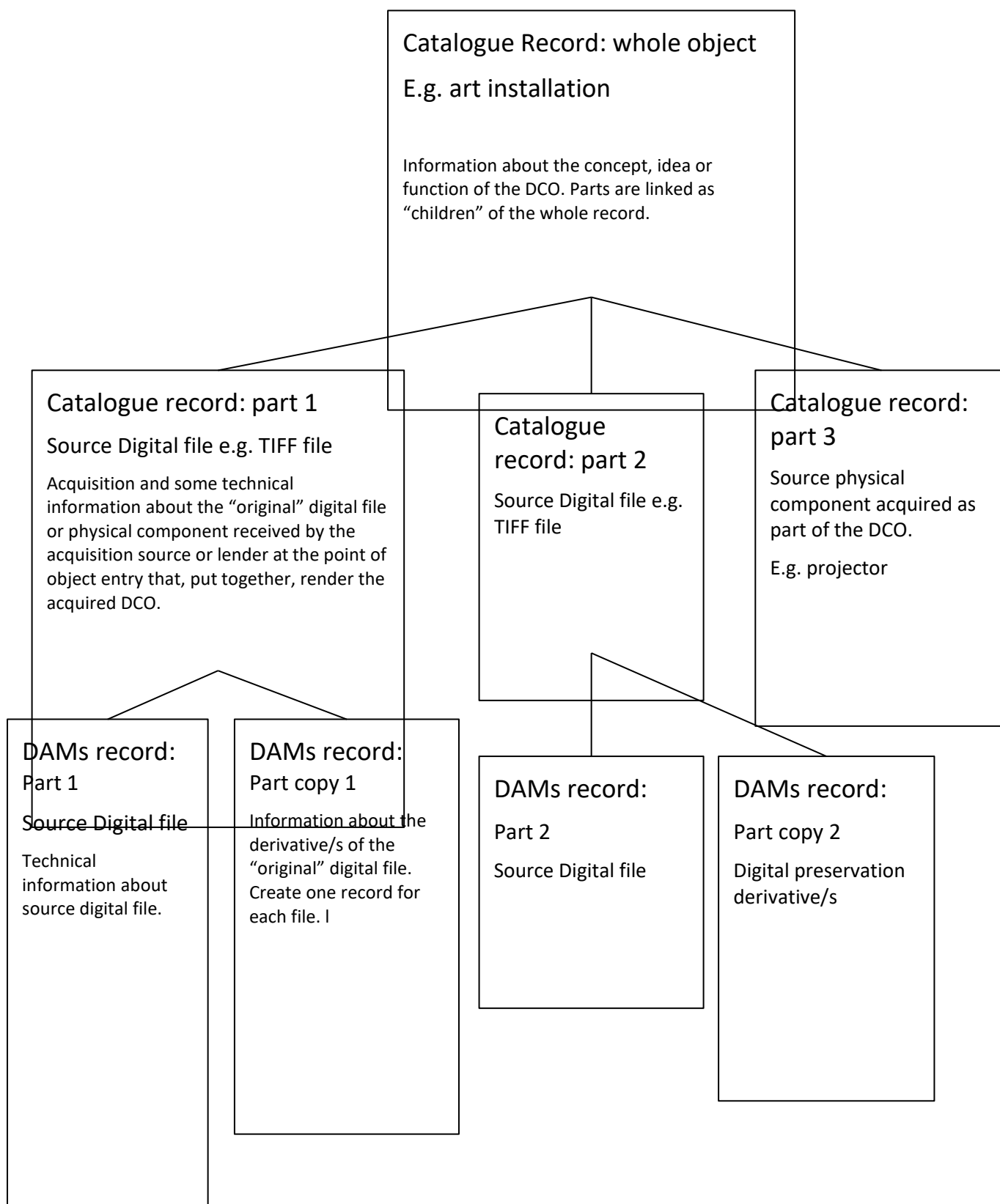
When documenting a physical object, only one catalogue record is often required to record basic identification information, as outlined in the Spectrum *Cataloguing* procedure⁵⁰.

However, there are drawbacks to cataloguing a Digital Collection Object (DCO) in this way. DCOs are often made up of multiple digital and/or physical component parts and is very useful to record the digital preservation and collections management actions carried out on each component in separate records, for example each digital/physical component may have a different physical or digital location that needs to be tracked and each digital component will have at least two digital preservation copies which also need to be tracked. On top of this, the digital components will be [migrated](#) to new digital formats to ensure the DCO can be accessed before the digital format becomes [obsolete](#). These new versions of the DCO will need to be tracked and managed with equal care as they will become the only accessible copy of the DCO when the other formats become obsolete.

For these reasons, a series of linked catalogue/DAMs records is recommended. One record to represent the whole DCO and one record to present each digital and physical component part.

⁵⁰ Collections Trust. [Spectrum, Cataloguing - suggested procedure](#). Accessed 2023.

Below is a basic diagram illustrating how catalogue and DAMs records for the DCO and its original digital and physical component parts, can be linked together. This diagram illustrates a possible record structure for organisations with a CMS and interoperable DAMs. For more information about how the information described below can be captured using a CMS only or the combination of a CMS and a Digital Asset Management System together, see [Section 7.3 Recommended data structure for digital collections](#).



The table below outlines the different types of catalogue record recommended to catalogue a DCO:

Catalogue record type	Part of object	Definition	Example of type of information recorded at this level
Whole object record	Whole Digital Collection Object (DCO)	Create one record representing the whole DCO. What should be described here is information about the concept, idea or function of the DCO as devised by the creator or artist. What is it? Who created it? When was it first created? For further information and a list of essential units of information, see Section 7.2.1.3. Other information / Whole object record.	e.g. object name, creator name, date of (first) creation, brief description. • Mobile phone, Apple, 2007, iPhone (1st Generation) • Personal computer, 1984, Amstrad CPC 464 Computer • Digital photograph • Digital video • <i>In the Eyes of the Animal</i>, Marshmallow Laser Feast, 2015, a 360 degrees virtual reality art installation.
Part record/s record	Digital and physical components that make up the DCO at the point of acquisition	Create a record for each source digital file or physical component received by the acquisition source or lender at the point of object entry that, put together, render the acquired DCO. This excludes supporting digital files and hardware used to enable access to the DCO. See Section 7.2.1.4. Object identification information / Source digital and physical components (part record/s).	Digital properties of each source digital file: file format, file size, date created • TIFF; 300 MB; 2013-01-03 • Acquisition source information. • Pre-entry checksums • Physical or technical characteristics of each physical part: • 4 vases [part of digital art installation]
Part record/s record	Digital preservation derivatives(s)	Create a record for each digital preservation derivative created from the source digital files. See Section 7.2.1.6. Object identification information / Digital preservation derivatives below for a full description and list of essential units of information.	Digital properties of each digital preservation derivative file: file format, file size, date created • TAR; 3 MB; 2019-02-03
Supporting technology record	Supporting digital files and hardware	Create a catalogue record for software, metadata or hardware fundamental to enable the ongoing access and preservation of the DCO.	

7.2.1.2. Object identification information

The units of information described in this section are recommended to be used to identify, manage and digital preserve DCOs now and in the long term. Some of the information units described in the tables below are identified as a minimum requirement, so it recommended to populate them for each catalogue/DAMs record. Any units of information that match directly to a corresponding unit of information in Spectrum have been flagged. Similarly, any units of information matching semantic units outlined in the *PREMIS Data Dictionary for Preservation Metadata Version 3.0*⁵¹ have been flagged. PREMIS is an international standard produced by the Library of Congress, designed for use by the Library and Archive sectors to ensure the correct [metadata](#) is captured to support the long term preservation, use, access and storage of DCOs. Units of information listed in this chapter are designed to be flexible enough to be used in any CMS or DAMs system.

7.2.1.3. Other information | Whole object record

The following units of information should be used to describe the whole Digital Collection Object (DCO); the whole object to be acquired and digitally preserved in the museum over time. The information recorded in the whole object record should relate to the whole object and remain the same overtime, sometimes agnostic of its current and future digital form. Examples of a whole DCO include a digital book, digital map, digital photograph, digital artwork or a moving image work.

Examples of DCO level information:

- Object name.
- Creator/artist name.
- Date of production, creation or first release/publication.
- Description of the DCO as a whole.
- Copyright holder (not copyright restrictions).

Unit of Information	Why is this important for digital collections?	Referenced in Spectrum or PREMIS?	Min Req? Yes/ No	Example
<i>Object number</i>	The unique number assigned to the whole DCO. For information about labelling DCOs, see Section 4.5. Processing new acquisitions in the <i>Acquisition and accessioning</i> chapter.	Spectrum core inventory: • <i>Object number</i>	Yes.	C-25331

⁵¹ Library of Congress. [PREMIS. Data Dictionary for Preservation Metadata v 3.0](#). Accessed 2023.

<i>Object name</i>	When the digital medium is not significant For DCOs made up of a digital medium that does not add significant meaning to the DCO, e.g. a TIFF, it is highly recommended that the object name reflects the concept or intention of the whole digital object rather than terms that describe its current digital format as the digital format will change over time. Avoid terms relating to digital format type, platform or other specific technical attributes. When the digital medium is significant If the digital format or technology is integral to the object's intellectual meaning or significance within the museum, describe the make and version of the digital files or hardware. This category includes DCOs with a permanent physical form as well as DCO with a partly or whole digital form.	Spectrum core inventory: • <i>Object name</i> • <i>Content – object type</i>	Yes.	When the digital medium is not significant • Digital photograph • Digital map When the digital medium is significant • Amstrad CPC 464 computer (Science Museum collection) • iPhone 6 (Victoria and Albert Museum collection)
Number of source digital files and/or component parts	The number of source digital file/s and physical components that make up the accessioned DCO at the point of entry to the museum. This should not include any supporting files or documentation that do not form part of the DCO, such as XML files holding descriptive metadata.	Spectrum core inventory: • <i>Number of objects.</i>	Yes.	6
<i>Brief description</i>	When the digital medium is not significant The description should focus on the whole intellectual entity when played, displayed or experienced by the audience/visitor using the original technology conceived by the creator. Descriptions should be agnostic of its technical or digital form or any physical digital devices. When the digital medium is significant When the digital medium is integral to the meaning of the whole work or integral to our understanding or experience of it, the technology used by the creator to conceive, create, display or access the work should be described. There should be an emphasis on how the acquired version of the work is viewed or experienced by the user.	Spectrum core inventory: • <i>Brief description</i> • <i>Content – description.</i> • <i>Content – concept</i>	Yes.	When the digital medium is not significant “A digital photographic portrait depicting HMR the Queen seated with two Corgi dogs.” When the digital medium is significant “An iPhone 1 sealed in its original packaging. No software installed...” “An immersive interactive art installation set in the forest, where visitors use virtual reality headsets and haptic backpacks to experience augmented reality animation.”

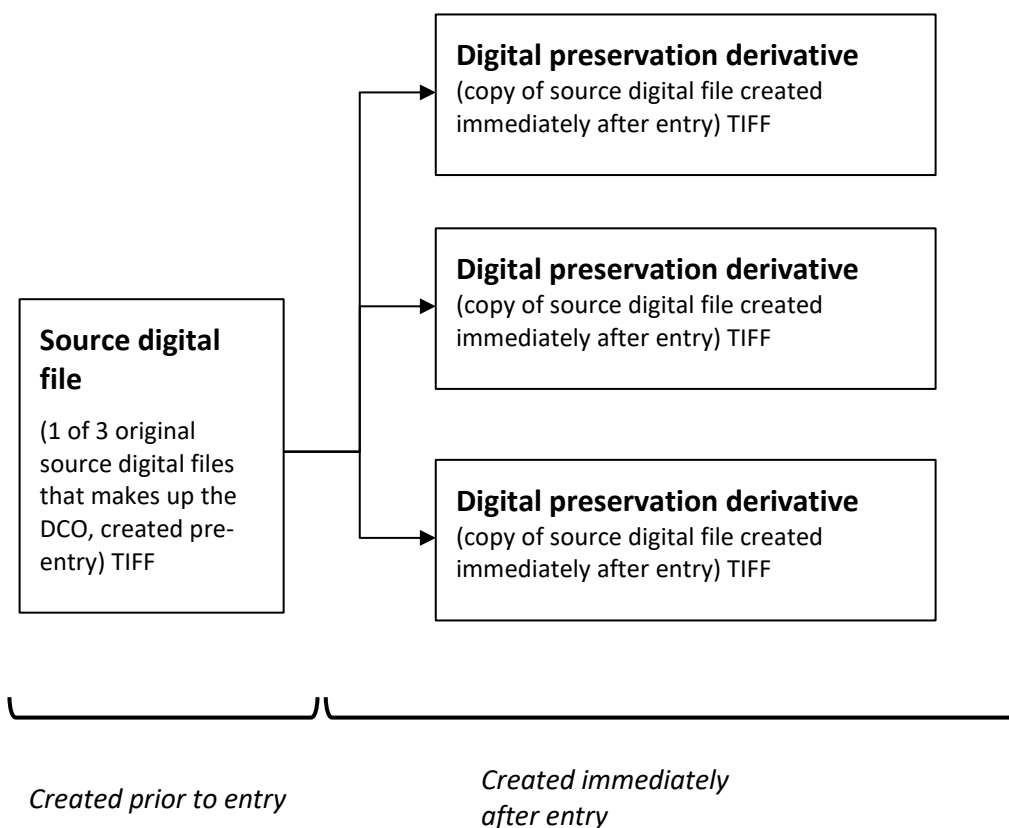
<i>Current location</i>	Only record the current location at this level when the DCO relates to one physical digital thing, e.g. iPhone 1. If the DCO is made up of multiple digital files, record the location in the part records. For further information, see Section 5.3.1.2. Location control process by storage medium in the <i>Location and Movement</i> chapter for further information.	Spectrum core inventory: <i>Current location</i>	Yes (if applicable).	Physical location: Room 3/Bay 3/Rack 5/Shelf 5 Digital location: Permanent archive storage (for organisation with a digital preservation system)
Digital dependencies	Record any metadata , hardware (auxiliary object) or software essential to render or make the DCO accessible and understandable.	N/A	Yes.	• Encryption keys for encrypted files. • XML files with metadata explaining how the digital files are put together to form the whole. • The make and model of hardware used to access digital files.
<i>Date</i>	Record the date that the creator originally produced or created the DCO, rather than the date the digital files were created. If there are versions or releases of software, record the date the first version was released to the public.	Spectrum other important information: <i>Content – date</i>	No.	2015-05-30
<i>Date Type</i>	Record the type of date described above, e.g. release, production, copyright etc.	N/A	No	Date released
<i>Preservation notes</i>	As part of workshops carried out by the Towards A National Collections funded project “Preserving and sharing born-digital and hybrid objects from and across the National Collection”, the project report notes that as some complex digital objects cannot be preserved long term in the manner in which the artist or producer intended, documentation will take on an important aspect of the object’s “preservation strategy” and a “source of authenticity”. The report later recommends that sometimes it’s important to “document a loss” - in other words, record what the museum cannot currently preserve in the long term. In this field	N/A	No.	“The video walk-through version of “In the Eyes of the Animal” has been preserved. The artistic collective first performed the work in Grizedale Forest as part of the “Abandon Normal Devices” festival, where visitors were invited to experience the immersive experience with an Oculus headset and haptic backpack. Through the headset, visitors were able to

	describe exactly what parts of the digital heritage will be preserved in the museum and what will not be preserved. This field is not for describing the detailed logistics of the preservation strategy for this object.			view augmented reality and sound layered on top of real time images of the forest. The oculus headset and haptic backpack have not been acquired.”
<i>Recorder and Recording date</i>	Same principles apply.	Spectrum core inventory: ● <i>Recorder</i> ● <i>Recording date</i>	Yes.	walkers; 2020-05-23

7.2.1.4. Object identification Information | Source digital and physical components (part record/s)

The digital components in this category are the accessioned [source digital files](#) or hardware components received at the point of object entry that, put together, render the Digital Collection Object (DCO). The units of information recorded at this level, relate to digital and technical characteristics of the digital file or hardware considered either essential or very useful to ensure the efficient management of the DCO now and in the long term. [Digital preservation actions](#) like [fixity checks](#), [virus scanning](#) and [file format migration](#), carried out on the source digital files could be recorded at this level too.

Information about [digital preservation derivatives](#) should be kept separate from the source digital files and should have separate records. See the diagram below, which illustrates how new digital files should be created to ensure the DCO remains accessible over time, in accordance with digital preservation best practice.



If your CMS has an import function, much of the information listed here is [technical metadata](#) or [descriptive metadata](#) that can be extracted from the digital file using [open source software](#) into a [XML](#) or [CSV file](#), and imported into the database to create a basic catalogue record. Where information is available in the metadata, this is flagged below. For more information on extracting metadata and importing into your CMS, see [Section 6.4.5. Extracting metadata for use in documentation](#).

As the information properties required to document a piece of hardware are so different from the information required to document a digital file, the object types are described in separate sections below.

7.2.1.4.1. Object identification Information | Source digital components (part record)

The information below is all the information required to effectively document a source digital component, e.g. a [source digital file](#). For information about how to catalogue a source physical component, see [Section 7.2.1.4.2. Object identification information | Source physical components \(part record\)](#). If your organisation has a CMS and a DAMs, the units of information below may be split between the catalogue record in the CMS to accession it as part of the permanent collection and a media record in the DAMs to manage and retrieve the digital file. In the column “Which record?”, a suggestion is made as to where the information unit should be recorded - in the CMS record, the DAMs record or both.

Unit of Information	Description	Referenced in Spectrum or PREMIS?	Min Req? Yes/No	Which record?	Example
Object number	Unique number assigned by the museum and used to track the component in the museum.	<i>Object number</i>	Yes	CMS and DAMs record	C-25315.1
Original filename/folder name	This is the filename for the source digital file that was created pre-entry by the creator, donor or lender. It is also referenced in the original filelist included in the object entry documentation. Many organisations leave the original filename of the source digital file, as acquired, as this is an integral part of the authentic digital object. The filename is sometimes referenced in the metadata or source code and re-naming the file may prevent the DCO from working correctly. For further information about managing file and folder names see Section 7.4. File and folder names .	Spectrum other important information: • <i>Technical attribute</i>	Yes	CMS and DAMs record	In_the_Eyes_of_the_Animal_1_of_8.WAV
Folder name assigned by the museum	This is the unique new folder name for the folder holding all source digital files relating to the DCO together. It is the equivalent to an object label for physical objects and can be used to identify and track a group of digital files. For further information about managing file and folder names see Section 7.4. File and folder names .	Spectrum other important information: • <i>Technical attribute</i>	Yes	CMS and DAMs record	C_25315.In_the_Eyes_of_the_Animal

Current location	Record the current location of the digital component. See Chapter 5. Location and movement control for information on recording current location for all types of DCO.	Spectrum core inventory: <i>Current location</i> <i>PREMIS: 1.7. Storage</i>	Yes	CMS record	Permanent digital archive
Checksum	Record the first checksum, generated by the donor or lender pre entry. If the donor or lender did not provide a checksum, record the checksum generated in-house, post entry. For further information about fixity checking and generating checksums, see Section 12.2.2. Fixity checking .	<i>PREMIS:1.5.2. Fixity</i>	Yes	CMS record	CE114E4501D2F4E2DCEA3E17B546F339
Checksum type	Record the Checksum Type (e.g. MD5), the algorithm used to generate the checksum code.	N/A	Yes	CMS record	MD5
Checksum date	Record the date the checksum was generated. If the checksum was generated pre-entry and the date of generation is not known, record the date before the date the digital component arrived at the museum.	N/A	Yes	CMS record	2015-05-16
File Format	Describe the file format of the digital file in its current digital state. This is a primary unit of information that ensures the DCOs are managed in accordance with digital preservation best practice. This information will be extracted when a file format profiling tool is used to identify the specific digital formats and version used. For further information about file format profiling, see Section 12.2.3. File format validation .	<i>PREMIS: 1.5.4. Format</i>	No	CMS and DAMs record	TIFF
File format profiling tool (digital only)	The name of the file format profiling tool used to recognise the file format.	N/A	Yes	CMS record	DROID
Is the file format recognised? (digital only)	Using a file format profiling tool, such as DROID, to scan and identify the file format. If the file format is not recognised, this gives the museum important information about the viability of preserving this	N/A	Yes	CMS record	Yes

	format, if the format is not known by the digital preservation community.				
File size	Describes the total size of the source digital file at the point of entry. This is the number of bytes of storage space the digital file takes up.	Spectrum other important info: • <i>Dimension value</i> • <i>Dimension measurement unit</i> <i>PREMIS: 1.5.3. Size</i>	No	CMS and DAMs record	30.5 MB
Legal Status	Record the legal status of the digital file. As the digital and physical components at this level are part of the accessioned collection the legal status would be “permanent collection” or the equivalent status used by your museum.	N/A	Yes	CMS record only	Permanent collection
Creating Application	For source digital files only. Record details of the application that created the digital file.	<i>PREMIS: 1.5.5. Creating Application</i>	No	CMS record	LiDAR scanner
Date created	This is the date when the digital component was created by the application.	<i>PREMIS: 1.5.5.3. Date Created by application</i>	No	CMS and DAMs record	2015-03-25
Authenticity	Record the private key or pin required to gain access to a digital file with a digital signature. This system is used to prove the authenticity of the digital file.	<i>PREMIS: 1.8. Signature information</i>	No	CMS record	Pin: 053546
original/ derivative	Record if the digital file is the original source digital file that was originally acquired or if the digital file is a copy of the “original” made post entry for the purposes of digital preservation.	N/A	Yes	CMS record	Original
[Link to derivative/s]	Record the digital file number of all digital preservation derivatives created from the source digital file to ensure the long term digital preservation of the DCO. This is all digital files created from the copying,	N/A	No	CMS record	[Link to derivative/s]

	migration, emulation etc. of the source digital file.				
Source/ derivative relationship	Describe the relationship between the source digital files and the digital preservation derivatives described, e.g. “ bits migrated to”; “bits copied to”; “file emulated to” etc.	N/A	No	CMS record	“Bits copied to”
Physical or digital?	Record if the component is in a physical or digital state. Describe the state of that version or copy. If the digital file is held on a physical digital device , record that the element is digital as the acquired DCO element is digital, only the container or device is physical.	N/A	No	CMS record	Digital
<i>Recorder and Recording date</i>	Same principles apply.	Spectrum core inventory: • <i>Recorder</i> • <i>Recording date</i>	Yes	CMS and DAMs record	Walkers; 2020-05-23

The following units of information relating to other Spectrum procedures should be recorded in the record for the source digital items.

Unit of Information	Why is this important for digital collections?
<i>Acquisition information</i>	See Chapter 4. Acquisition and accessioning .
Restrictions of Use	See Chapter 4. Acquisition and accessioning .
Conservation and preservation information	See Chapter 13. Collections care and conservation .

7.2.1.4.2. Object identification Information | Source physical components (part record)

Unit of Information	Description	Referenced in Spectrum or PREMIS?	Min Req? Yes/No	Example
Object number	Each physical component should be assigned a unique object number. This number should only be assigned to the accessioned physical components, not components that are not an intrinsic part of the DCO. It is recommended that the same numbering system is applied to that of physical movable parts.	<i>Object number</i>	Yes	DZ023.3
Make and model	Describe the make and model of the hardware.	N/A	Yes	• Apple iPhone 8 • Macintosh LC II • Oculus Rift
Operating system	Describe the operating system the hardware is running on.	N/A	No	• IOS
Processor	Describe the name and version of the processor.	N/A	No	• Motorola, 68030
RAM	Describe make, type and capacity of the RAM.	N/A	No	• Samsung, DDR4, 128GB
Connector type	Type of connection used on the device/hardware.	N/A	No	• USB • FireWire • SCSI
File system (physical digital device)	File system used on a physical digital device .	N/A	No	• Ex-FAT • NTFS
<i>Current location</i>	See Chapter 5. Location and movement control for information on recording a current location for all types of DCO.	Spectrum core inventory: • <i>Current location</i>	Yes	Store 5; Bay 2; Rack 3; Shelf 1

		<i>PREMIS: 1.7. Storage</i>		
Legal Status	Record the legal status of the digital file. If the digital file is the acquired source digital file , the status would be “permanent collection” or the equivalent status used by your museum to describe the accessioned collection. If the digital file is an exact copy of the source digital file, using the same format, the status would also be “ digital preservation derivatives ”. If the source digital file becomes obsolete and the bits from the source digital file are transferred to a new preservation format, the status of the new file would also be “preservation digital derivative”.	Spectrum other important info: <i>Current owner</i>	Yes	Permanent collection
original/ digital preservation derivatives	Record if the digital file is the original source digital file that was originally acquired or if the digital file is a copy of the “original” made post entry for the purposes of digital preservation.	N/A	Yes	Original
[Link to derivative/s]	Record the digital file number of all digital derivatives created from the source digital file to ensure the long term digital preservation of the DCO. This is all digital files created from the copying, file format migration , emulation etc. of the source digital file.	N/A	No	[Link to derivative/s]
Source/ derivative relationship	Describe the relationship between the source digital files and the derivative described, e.g. “bits migrated to”; “bits copied to”	N/A	No	“bits migrated to”
Physical or digital?	Record if the component is in a physical or digital state. Describe the state of that version or copy. If the digital file is held on a physical digital device , record that the element is digital as the acquired DCO element is digital, only the container or device is physical.	N/A	Yes	Physical
<i>Recorder and Recording date</i>	Same principles apply.	Spectrum core inventory: • <i>Recorder</i> • <i>Recording date</i>	Yes	walkers;2021-05-23

7.2.1.5. Object identification Information | Physical component parts - non-digital

The DCO may be made up of physical non-digital components. These physical parts are to be accessioned into the museum collection. These components should be documented in the same way as the museum would document other physical component parts of an object.

7.2.1.6. Object identification Information | digital preservation derivatives

The [digital preservation derivatives](#) files are copy digital files created from the [source digital files](#), after the DCO has entered the museum, to ensure the DCO is digitally preserved in the short and long term. This information about the digital derivative files has been separated out from information about source digital files as it is recommended that separate media records are created and linked to the records for the source digital files.

If your CMS has an import function, much of the information listed here is technical or [descriptive metadata](#) that can be extracted from the digital file using open source software into [XML](#) or [CSV file](#), and imported into the database to create a basic catalogue record. Where information is available in the metadata embedded in the digital, this is flagged below.

Unit of Information	Why is this important for digital collections?	Referenced in Spectrum or PREMIS?	Minimum Req? Yes/No	Example
ID number	A unique number assigned to each digital preservation derivative created. If using a DAMs system, this is the automatically generated number, sometimes called the media ID.	N/A	Yes.	456411
Filename	This is the unique new filename assigned to the digital file, created in-house. This should reference the ID number of the digital file and the object number of the digital or physical component part of the DCO which this digital file has been copied from. It should comply with the museum's in-house filename conventions. For further information see Section 7.4. File and folder names .	N/A	Yes	456411_C-25315.1_1_of_3.TIF
<i>Current location</i>	See Chapter 5. Location and movement control for information and recommendations.	Spectrum: • <i>Current location</i> <i>PREMIS: 1.7. Storage</i>	Yes.	Permanent digital archive

File Format	Describe the file format of the digital file in its current digital state. This is a primary unit of information that ensures the DCOs are managed in accordance with digital preservation best practice.	<i>PREMIS: 1.5.4. Format</i>	Yes.	TIFF
File Size	Describe the total number of bits that make up the digital file.	Spectrum other important info: • <i>Dimension value</i> • <i>Dimension measurement unit</i> <i>PREMIS: 1.5.3. Size</i>	Yes	353 MG
Date created	This is the date that the digital file was created by the application.	<i>PREMIS: 1.5.5.3. Date Created by application</i>	Yes	2020-06-23
[Link to derivative/s]	Record the digital file number of all digital preservation derivatives created from the source digital file to ensure the long term digital preservation of the DCO. This is all digital files created from the copying, format migration , emulation etc. of the source digital file.	N/A	No	[Link to derivative/s]
Source/ derivative relationship	Describe the relationship between the source digital files and the derivative described, e.g. “bits migrated to ”; “bits copied to”	N/A	No	bits migrated to”
<i>Recorder and Recording date</i>	Same principles apply.	Yes.	Yes.	Walkers; 2021-05-23

7.3. Recommended data structure for digital collections

7.3.1. Cataloguing recommendations for museums with a CMS and DAMS

It is recommended that museums with a dedicated CMS and DAMs create the following records to manage the digital files related to a DCO:

- One CMS catalogue record should be created for each DCO.
- One CMS catalogue record should be created for each component or digital file that makes/made up the DCO at the point of entry. This record should be linked, ideally as a child of the record for the DCO.
- One DAM media record should be created for every digital file representing the DCO, including the source digital files and [digital preservation derivatives](#) (copies). The information about the source digital file should be split between the CMS and the DAMs. The acquisition information should be recorded in the CMS and the more technical information in the DAMs. Ideally the DAM media record should be linked to the CMS record for the source digital file from which the derivative was created.

7.3.2. Cataloguing recommendations for museums with a CMS but no DAMS

- One CMS catalogue record should be created for each DCO.
- One CMS catalogue record should be created for each source digital file that makes up the DCO only and linked as a “child” of the DCO. These records should hold the specific technical information for the digital file at the point of entry, e.g. the format, size, and fixity information.
- One CMS media record should be created for second, third, fourth etc. generation digital derivatives that have been created from digital information in the source digital files. The record should ideally be linked to the CMS record for the source digital component it has been copied from.

7.4. File and folder names

In a similar way to an object label, the filename or folder name acts as a unique identifier for any digital files that make up the DCO or the folder containing the digital files.

You may have an existing organisational policy which requires you to rename individual files with the object number. Careful consideration should be made before following this decision as there are some significant risks attached to renaming the original filename/folder name.

For [source digital files](#), it is recommended that the original filename or folder name, inherited from the previous owner, stays the same, unless the filename is illegal and cannot be read or managed by a computer. The reason for keeping the original filename is to:

- Maintain the authenticity of the original digital object.
- Ensure the DCO remains accessible. Sometimes the source digital files are referenced in the source code or [metadata](#) used to structure the DCO. If the filename were to change, it could break the source code or prevent the DCO from being accessed correctly.

When the source digital files arrive at the museum, it is best practice to create a folder for each DCO and to store all source digital files and supporting files used to render and provide information about the DCO in this folder. This folder should follow the museum's in-house folder name convention.

Any digital preservation copies of the source digital file/s made after entry into the museum, should also follow the museum's in-house file/folder name convention.

For further information on file naming, see the Digital Preservation Coalition's guide on the subject.⁵²

The museum should have a filename convention in place before re-naming digital files or folders.

7.4.1. Rules for file/folder names

If multiple files require re-naming, there are bulk renaming tools widely available free online that could help with this task. These tools will ensure far fewer errors and no inconsistencies are made in the filename.

The following rules are recommended for managing existing file names created by the donor pre-entry or creating or renaming files and folders created in house. These rules can be used to create your museum's file/folder name convention.

All folder and Filenames (including original file and folder names) must:

- Be machine readable. If the original file name has any of the following illegal characters, the file name must be carefully altered, but ensure the original file name is recorded in the CMS for reference. For example remove any special characters, perhaps replacing a pipe with an underscore.
- Use underscores or another legal character to separate units of information.
- Exclude any illegal characters or symbols, see below:
 - # pound
 - % percent
 - & ampersand
 - { left curly bracket
 - } right curly bracket
 - < left angle bracket
 - > right angle bracket
 - * asterisk
 - ? question mark
 - \$ dollar sign
 - ! exclamation point
 - ' single quotes
 - " double quotes
 - + plus sign
 - ` backtick
 - | pipe
 - = equal sign

⁵² Digital Preservation Coalition. [Filenaming and formats](#). Accessed on 20 March 2023.

All folder names created in-house must:

- Be consistent.
- Be agreed in advance.
- Reference the unique identifier for the DCO.
- Reference the title or object name of the DCO.

All filenames created in-house must:

- Be consistent.
- Be agreed in advance.
- Reference the following units of information:
 - The unique identifier for the digital file, such as the media ID generated by the DAMs system.
 - The object number or temporary number for part of the DCO that the file relates to.
 - Sequence number of the digital file, relating to the order in which the digital files should be put together to make up the whole DCO.
 - Total number of digital files that make up the whole DCO.
 - File extension.

8. Object exit

Spectrum definition - recording when objects leave the buildings you are responsible for and pass out of your direct care.

For digital collections, the methods used to move the DCOs will be very different to physical objects.

8.1. Spectrum suggested procedure⁵³

Spectrum suggested procedure workflow	Is the step in the workflow different for digital collections?
Authorise the exit according to your policy and the linked procedure.	No.
If the objects are being transported, go to <i>Location and movement control</i> .	No.
Schedule collection of the objects.	No.
Arrange for the objects to be at the agreed pick-up point at the agreed time.	Yes. See Section 8.2.
Update location records.	Yes. See Section 8.3.
Record information about the exit.	Yes. See Section 8.4.
Update insurance and indemnity records as needed.	No.
Return to whichever linked procedure triggered the object exit.	No.

8.2. Arrange for the objects to be at the agreed pick-up point at the agreed time

The *Object exit* procedure relates to DCOs being transferred outside the museum as part of an authorised loan out, disposal or transfer back to the owner.

8.2.1. Different methods of digital and physical exit

⁵³ Collections Trust. [Spectrum, Object exit - suggested procedure](#). Accessed 2023.

The details of object exit are not explicitly described in Spectrum, as this level of detail is not required for managing physical objects. However, it is necessary to describe them for digital collections, as there are a variety of ways in which the [source digital files](#) and any supporting files that make up the Digital Collection Object (DCO) may exit the museum. The list below outlines common methods of digital and physical/digital exit:

- **Virtual exit - unmanaged:** Digital files are transferred out of the museum using an unmanaged virtual method i.e. uploaded to an online source or attached to an email. It is recommended that only trusted secure digital sources are used for transferring DCOs.
- **Virtual exit - file transfer platform:** Digital files are uploaded and transferred onto a dedicated file transfer platform which manages and organises the stages of transfer, fixity, file validation, and receipt of files from the museum to the recipient.
- **Physical exit - digital storage:** Digital files are transferred to a [physical digital device](#) e.g. hard drive or USB stick and transported to the recipient in an agreed way.
- **Physical entry:** The DCO has physical components e.g. a computer terminal or a video games console.

8.2.2. Digital exit process

Prior to any DCOs being transferred outside the museum or disposed, the following process should be carried out on all DCOs made up (in whole or part) of digital files:

Order of Priority	Activity	Risk to digital collection if not actioned
1	Ensure an inventory of each digital file to be transferred has been carried out. As part of the inventory: 1.1. Check that all the corresponding supporting files and metadata required for preserving the DCO is together in the same folder, including a checksum for each digital file. 1.2. Check that up-to-date basic inventory information has been recorded in the catalogue record for the DCO and the digital files being transferred. For further information on carrying out an inventory, see Section 6.4. Producing an inventory in the <i>Inventory</i> chapter.	For disposed digital files: There is not sufficient information about the disposed digital files. For transferred digital files: The recipient of the digital files cannot carry out basic digital preservation actions on the digital files, cannot identify the digital files, does not know about any copyright restrictions placed on the DCO or has lost information about the owner.
2	If any digital files do not have a checksum, generate one. For further information, go to Section 12.2.3. Fixity checking.	There is no evidence that the digital files that will be copied from a digital preservation derivative are exactly the same as the source file. Therefore, if an error occurred when copying the digital file, it wouldn't be picked up.

3	3.1. Use a dedicated workstation, not connected to the museum IT network. You will need to temporarily connect the computer to the internet to send the outgoing digital files. 3.3. Create a separate folder in the digital quarantine environment to temporarily hold the outgoing digital files. 3.4. If the digital files have their own folder structure, this should be maintained. For further information, see Section 2.3.2. Setting up a digital quarantine environment.	If files are not saved into a digital quarantine environment before they have been identified, scanned or fixity checked, the digital files could corrupt the IT network or other digital files saved in the same location.
4	4.1. If the digital files are being transferred, locate the DCO to be transferred and create an exact copy of all digital files and supporting files used to render the DCO. 4.2. Transfer the digital files to the dedicated folder in the digital quarantine environment. For further information on safely transferring digital files without losing data or damaging the digital file, go to Section 5.4.4.1. File copying software in the <i>Location movement and control</i> chapter.	If the source digital file or another copy created for digital preservation is sent out, there is a significant risk that the digital file could be corrupted, deleted or essential metadata could be altered, interfering with the integrity of the source digital file.
5	If the digital files are being disposed of, follow the protocol described in Chapter 18. Deaccessioning and disposal .	N/A
6	Carry out a fixity check to confirm the copied digital files are identical to their source digital files. For further information see Section 12.2.2. Fixity checking .	There is no evidence that the digital files, that will be copied from a digital preservation derivative ready for transfer, are exactly the same as the source digital preservation derivative. Therefore, if an error occurred when copying the digital file, it wouldn't be picked up.
7	Using the correct hardware or software, access each DCO to be transferred and check that the content of each digital file is as expected. For further information on carrying out an inventory, see Section 6.4. Producing an inventory in the <i>Inventory</i> chapter.	We cannot guarantee that we have sent or disposed of the correct digital files.
8	If the digital files are being transferred, create a separate record for the digital file to be transferred. Record the date the copy was created and other basic inventory information.	If a separate record is not created, object exit information and other essential collections management information such as the lender's name and future digital preservation actions relating to this particular digital file, cannot be correctly recorded.
9	If the digital files are being transferred, update the metadata embedded in each digital file to ensure all important information, such as object number, legal owner, copyright restrictions and digital signature stays with the digital files at all times. For a full list of information requirements, see Section 8.2.2.1. Metadata to accompany externally transferred digital files.	Metadata describes and keeps safe fundamental information about the digital files and the DCO. Without this information, the museum may not be able to identify, access, preserve or carry out any other essential preservation, documentation or collections management activity.

10	10.1. Produce a filelist of all the digital files to be transferred held in the dedicated folder in the digital quarantine environment. For more information, see Section 6.2.5. Extracting metadata for use in documentation. 10.2. Send the file list to the recipient.	There is no record of what digital files were sent to the recipient.
11	Transfer all the digital files that make up the DCO using the agreed transfer method.	N/A
12	Receive confirmation that all the digital files that make up the DCO have been transferred correctly. You may ask for confirmation that the digital files have been virus scanned and fixity checked .	There is no record that the digital files were received by the recipient.
13	Update the catalogue record to amend the legal status of the DCO if required and any digital preservation actions carried out on the digital files, e.g. deletion or copying.	Core inventory information is incorrect.

8.2.2.1. Metadata to accompany externally transferred digital files

The information outlined in the table below is required to ensure the digital components of the DCO can be accessed, stored, managed, and digitally preserved now and in the future. The information is separated into two categories: [technical metadata](#) and [descriptive metadata](#).

Information Type	Description	Example	Metadata Type	Essential/ Very useful?
Object number	Unique number assigned to the digital file and the DCO.	N-0521	Descriptive metadata	Essential
Object name	Name or title of DCO.	Flappy Bird mobile application	Descriptive metadata	Essential
Number of digital files	Number of digital files (if a group) that are used to render the DCO (excluding supporting digital files)	5	Descriptive metadata	Essential
Current Owner	Record the legal owner of the digital file.	Royal Museums Greenwich	Descriptive metadata	Essential
Rights holder/s	Record the rights holders to be credited if the DCO is displayed.	Microsoft	Descriptive metadata	Essential
Filename and folder names	The current filenames and folder names.	N_0521_1_of_3.mov	Technical metadata	Essential
File size	The size of each digital file for each DCO in megabytes (MB), gigabytes, terabytes (TB) or petabytes (PB).	3 TB 304 GB	Technical metadata	Very useful
File format	The file extension of each digital file. This information is required to inform future digital preservation actions .	- TIFF - REP - PDF - X3D	Technical metadata	Essential
Checksum	A checksum for each digital file.	120EA8A25E5D487BF687096440019	Technical metadata	Essential
Checksum type	The algorithm used to generate the checksum. The museum needs to know this so it can run another checksum on entry using the same algorithm.	MD5	Technical metadata	Essential

Terms and conditions	Record any terms and conditions describing how the organisation must document, store, preserve, display, and otherwise use or re-use the DCO.	"The DCO must be exhibited using x hardware in accordance with the setup guide accompanying the work."	Descriptive metadata	Essential
Digital dependencies	Describe any technology (software or hardware), information or other factors that are required to ensure the DCO can be accessed, preserved, stored and experienced in the way the creator intended. It is a dependency if the DCO cannot be accessed, used, preserved or shared without it. This is sometimes described as the auxiliary object .	Technology dependencies example: a virtual reality game requires a virtual reality headset. Information dependency example: Metadata recording the encryption key to access the source digital files. Other examples: Some DCOs are constantly changing and evolving and need to be connected to the internet or an online social network.	Descriptive/technical metadata	Essential (if exists)
Authenticity	Proof that the digital files that make up the DCO are authentic. This may be particularly important for digital artwork.	A digital signature	Descriptive metadata	Very useful

8.3 Update location records

Update the catalogue record with the new location of the copy of the digital file/s and the date it was transferred.

8.4. Record information about the exit

Create an *Object exit* receipt for the copy of the digital file/s being transferred. Record the filename and object number of each digital file and the object name or title of the DCO.

9. Loans in (borrowing objects)

Spectrum definition - managing objects you borrow for a fixed period of time and for a specific purpose.

Typically, this might include objects borrowed for an exhibition or another extended activity such as a research project.

For digital collections, there are some additional aspects to consider especially around agreements, receiving the loan, monitoring and returning.

For digital collections, it should be confirmed from the outset if a loan or a license agreement is required. As with physical objects, if the object will be displayed and interpreted as an object, then a loan from the object owner is required; if a copy of the object, whether a still or a video, gif or similar, will be used as part of the interpretation in a display or exhibition then a license agreement is required from the rights holder.

9.1. Spectrum suggested procedure workflow⁵⁴

Spectrum Procedure	Is the step in the workflow different for digital collections?
Loan research	
Make the case for borrowing the objects and obtain authorisation.	Yes. See Section 9.2.1.
Send a loan request to the lender.	No.
Record details of request.	No.
Maintain an up-to-date record of the status of the loan throughout the process.	No.
Exchanging further information	
Complete and send a facilities report to the lender.	Yes. See Section 9.3.1.
Obtain further information for each object from the lender, and update loan file.	No.
Agreeing the loan	

⁵⁴ Collections Trust. [Spectrum, Loans in \(borrowing objects\) - suggested procedure](#). Accessed 2023.

Create and sign the loan agreement.	Yes. See Section 9.4.1.
Record loan information.	No.
Preparing to receive the loan	
Schedule and prepare for the arrival of loaned objects.	Yes. See Section 9.5.1.
On arrival send a receipt and condition update to the lender.	No.
If conservation work is needed, agree this with the lender.	No.
Monitoring the loan	
Monitor and report the condition of the objects during the loan.	Yes. See Section 9.6.1.
Extending the loan	
Do you want to extend the loan?	No.
Return and closure	
Contact the lender to arrange for the return of objects.	No.
Carry out a final condition report on the objects.	Yes. See Section 9.7.1.
Return the objects to the lender.	Yes. See Section 9.7.2.
Confirm all loan conditions have been met and close the loan file.	No.

9.2. Loan research

9.2.1. Make the case for borrowing the objects and obtain authorisation

The loan proposal should be made in writing following the requirements for Digital Collections Objects (DCOs) outlined in your Loans Policy. Do not under-estimate the time required to organise the loan of a DCO, the time required will be the same as that of a physical object or longer if equipment has to be procured to display or manage the object.

Resource and planning factors normally recorded in the proposal for the loan will have variations for DCOs and will include the following considerations:

- Provenance and ownership of each element of the digital object.
- Ensure the objects being requested can be supported by the museum.
- If any specific hardware or software is required to manage or display the object it should be budgeted for appropriately.
- Proposal for managing the display, storage and security of the object.
- Rights clearances.
- Arrangements for the return of the object at the end of the loan period.

9.3. Exchanging further information

9.3.1. Complete and send a facilities report to the lender

Ensure that the museum has the capacity and resources to receive, store and display the objects being requested. The current UKRG facilities report does not address the needs of digital collections, so the lender may request supplementary information about the digital preservation and IT capabilities, cyber security and infrastructure of the museum. A full list of digital formats which can be supported should be sent to the prospective lender along with details of security provision for digital files.

For detailed information on what should be included, see [Chapter 3. Object entry](#) in particular section 3.2.1.1 for questions to ask the lender.

9.4. Agreeing the loan

9.4.1. Create and sign the loan agreement

The loan agreement will include the terms and conditions of the loan. For detailed information on what should be included, see [Chapter 3. Object entry](#). In most cases the lender's loan agreement should be used.

Agree if the loan will include the original copy of any digital file, or if a copy will be created for the purpose of the loan (See [Section 20.2.1 Access and re-use copies](#)). Specify the format, [file size](#) and file type required, and ensure the loan agreement includes what hardware and/or extra software will be provided by the lender or is to be provided by the borrower. For DCOs the loan agreement should include permission from the lender to use the DCO for the duration of the loan period only.

The loan agreement must also include information on the return of the digital object to the lender, or how the file will be securely removed from the museum's servers or other digital storage at the end of the loan period.

In the loan schedule, ensure the following information for each object being supplied is noted:

- DCO title(s).
- Format.
- Valuation for insurance/indemnity purposes.
- Lender Name and credit line for captions.
- IP information.
- Territory.
- Method of delivery.
- Dates the license is granted for.

Contact the insurance company, or the Arts Council for GIS, for advice on insuring the DCO for the duration of the loan.

9.5. Preparing to receive the loan

9.5.1. Schedule and prepare for the arrival of loaned objects

Planning for the arrival of digital loans should be consistent with planning for the arrival of digital objects for other purposes. For more detailed information on these processes, see [Chapter 3. Object entry](#).

9.6. Monitoring the loan

9.6.1. Monitor and report the condition of the objects during the loan

See [Chapter 12. Condition checking and technical assessment](#).

9.7. Return and closure

9.7.1. Carry out a final condition report on the objects

If the DCO is to be returned to the lender, a final condition report should be carried out. See [Chapter 12. Condition checking and technical assessment](#).

9.7.2. Return the objects to the lender

Arrangements for return of the objects should be agreed as part of the loan agreement. In some instances for digital-only objects where a copy has been provided to the borrower it will be appropriate for the DCO to be removed from the borrower's server and confirmation of this secure deletion sent to the lender.

If the DCO is to be returned to the lender, follow the guidance in [Chapter 8. Object exit](#).

10. Loans out (lending objects)

Loans out (lending objects) involves assessing requests for you to lend your objects and managing the lending process until loans are returned to you.

For digital collections, there are some additional aspects to consider including preparing the loan and sending the loan.

10.1. Spectrum suggested procedure⁵⁵

Spectrum suggested procedure workflow	Is the step in the workflow different for digital collections?
Assessing the request	
Open a file for the loan.	No.
Record details of request.	No.
Consider the request.	Yes. See Section 10.2.1.
Acknowledge the request.	No.
Reserve the objects for the loan.	No.
Requesting further information	
Request further information from the borrower.	Yes. See Section 10.3.1.
Consider the request.	Yes. See Section 10.3.2.
Agreeing the loan	
Record the final conditions of the loan and create the loan agreement.	Yes. See Section 10.4.1.
Both parties sign loan agreement.	No.
Preparing for the loan	
Check and record, with images, the condition of objects for loan.	Yes. See Section 10.5.1.

⁵⁵ Collections Trust. [Spectrum, Loans out \(lending objects\) - suggested procedure](#). Accessed 2023.

Carry out any necessary conservation work, including bespoke mounts and frames.	Yes. See Section 10.5.2.
Confirm that all security conditions have been met.	Yes. See Section 10.5.3.
Obtain evidence of insurance or indemnity arrangements and update records.	No.
Sending the objects	
Make arrangements for sending the objects and confirm their safe arrival.	Yes. See Section 10.6.1.
Monitoring the loan	
Monitor the condition and location of the objects during the loan.	Yes. See Section 10.7.1.
Extending the loan	
Does the borrower want to extend the loan?	No.
Arranging for return	
Confirm the arrangements for the return of the objects, and plan their return to you.	Yes. See Section 10.8.1.
Closing the loan	
Invoice the borrower for any remaining costs.	No.
Acknowledge safe receipt of the objects and confirm that all loan conditions have been met.	.
Add relevant information about the loan to the objects' catalogue records.	No.
Close the loan file.	No.

10.2. Assessing the request

10.2.1. Consider the request

The loan proposal from the borrower should be made in writing following the requirements outlined in your Loans Out Policy. Consider whether the loan request meets the criteria for lending digital objects. Some digital objects may not be suitable for loan, for example due to rights agreements or their current [file format](#) or

preservation medium. Consider whether the borrower is requesting the original object or if a copy of the digital object can be provided for the duration of the loan for digital only objects.

For digital collections, it should be confirmed from the outset if a loan or a license agreement is required. As with physical objects, if the object will be displayed and interpreted as an object, then a loan is being requested; if a copy of the object, whether a still or a video, gif or similar, will be used as part of the interpretation in a display or exhibition then a license agreement is required and this should be dealt with in the same way as license requests for images of physical collection objects.

10.3. Requesting further information

10.3.1. Request further information from the borrower

If you are considering lending a Digital Collection Object (DCO), further information will be required. As well as the information requested for all loans including a facilities report, specific information is required for digital objects. This will include the following considerations:

- How the borrower expects to receive the object, including method of [file transfer](#)
- The format, [file size](#) and file type required
- Proposal for digital storage and security of the object during the loan
- If the borrower has the facilities and expertise to maintain and display the digital object in the appropriate manner, such as access to the correct operating systems and software.

If the loan is being requested as part of a touring exhibition, ensure all venues have the capability and expertise to receive and display the DCO, and that the method of transfer of the loan between tour venues has been considered.

10.3.2. Consider the request

In light of the further information, consider whether you want to go ahead with the loan of the proposed digital objects. Factors may include:

- Whether the borrower has the appropriate experience with, or can access expertise in, receiving, managing and displaying digital objects. Refer to [Section 1.3.1. Managing digital collection objects](#) to help make this decision
- The costs of preparing the digital object for loan
- Security considerations around digital storage, and whether the borrower has appropriate cyber security measures in place
- How the digital object will be stored and displayed (e.g. via a dedicated terminal, via networked access)

10.4 Agreeing the loan

10.4.1 Record the final conditions of the loan and create the loan agreement

The loan agreement should include the terms and conditions of the loan. In most cases the lender's loan agreement should be used and sent to borrowing institutions.

For DCOs, specific clauses may be required including:

- The format, file size and file type being provided as part of the loan, and whether it is the original or a copy supplied for the duration of the loan
- The responsibility for provision of hardware and software to support the DCO, and, if the lender is providing it, a schedule of the equipment provided
- Specific cyber security requirements related to the DCOs, including prohibitions around making copies or sharing the object
- How the object will be returned and/or deleted from the borrower's systems at the end of the loan as appropriate
- Whether any digital storage media supplied with the object is for transit only, or is an integral part of the object

In the loan schedule, include the following information for each object:

- DCO title(s).
- Format.
- Valuation for insurance/indemnity purposes.
- Lender Name and credit line for captions.
- IP information.
- Territory.
- Method of delivery.
- Dates the license is granted for.

Note that there is currently little advice available to value DCOs. Advice from other organisations and experts such as the Digital Preservation Coalition may be sought if there is no current market valuation available for the object.

10.5. Preparing for the loan

10.5.1. Check and record, with images, the condition of objects for loan

See [Chapter 12. Condition checking and technical assessment](#).

Note that for some digital objects such as digital-only files it may not be possible to have images of objects.

10.5.2. Carry out any necessary conservation work, including bespoke mounts and frames

See [Chapter 13. Collections care and conservation](#) for how to proceed with any required conservation work on the digital objects before they are lent. Follow normal procedures for any conservation or mounting work required to physical aspects of the digital object (e.g. terminals, USB sticks).

Where possible, information indicating the ownership of the DCO and the dates of the loan should be embedded in the metadata of the DCO before the loan.

10.5.3. Confirm that all security conditions have been met

If specific security conditions are required, such as secure servers or a secure stand-alone terminal to host the digital object during the loan, confirm these are in place before the loan is sent. If possible, create a tamper-proof copy of the object to be sent on the loan.

10.6. Sending the objects

10.6.1. Make arrangements for sending the objects and confirm their safe arrival

For detailed information on this process see [Chapter 8. Object exit](#) and [Chapter 5. Location and movement control](#).

10.7. Monitoring the loan

10.7.1. Monitor the condition and location of the objects during the loan

Monitor loans at least annually as laid out in the Loan Agreement. See [Chapter 12. Condition checking and technical assessment](#) for guidance on monitoring the condition.

10.8. Arranging for return

10.8.1. Confirm the arrangements for the return of the objects, and plan their return to you

Arrangements for return of the objects should be agreed as part of the loan agreement. If the digital object is to be returned to the lender, follow the guidance in [Chapter 3. Object entry](#) to receive the object.

In some instances for digital-only objects where a copy has been provided to the borrower it will be appropriate for the digital object to be removed from the borrower's server and confirmation of this secure deletion sent to the lender. This process, and the method of confirmation, should be agreed in advance of the loan and noted in the signed loan agreement.

11. Documentation planning

Spectrum definition - making your documentation systems better and enhancing the information they contain as an ongoing process of continual improvement.

For digital collections, this should include creating a [digital assets](#) register.

11.1. Spectrum suggested procedure⁵⁶

Spectrum suggested procedure workflow	Is the step in the workflow different for digital collections?
Reviewing your existing collections information	
Review whether your existing collections information meets your needs.	No.
Writing your documentation plan	
Create your documentation plan.	Yes. see Section 11.2.1.
Putting your documentation plan into practice	
Get the plan approved.	No.
Put the plan into action.	No.
Regularly review your progress, based on the milestones in the plan.	No.
Complete the work and evaluate the plan.	No.
Continual improvement	
Repeat the procedure.	No.

⁵⁶ Collections Trust. [Spectrum, Documentation planning - suggested procedure](#). Accessed 2023.

11.2. Writing your documentation plan

11.2.1. Create your documentation plan

Use the instructions below to expand the museum's existing documentation plan to include digital collections that have not yet been fully accessioned. The DPC Digital Preservation Handbook has created a useful guide on creating a basic digital assets register.⁵⁷ The Government of Canada have also created a digital preservation inventory template for museums⁵⁸.

The scope of the plan should include:

- All DCOs made up entirely or partly of digital files, hardware, software or other technology.
- DCOs stored 'virtually' on digital environments like servers and stored on [physical digital devices](#) such as hard drives.
- DCOs that have a permanent physical form such as a computer.
- All supporting [metadata](#), files, hardware and information used to ensure that the DCO can be accessed, identified and preserved.
- Any exact copies or copies on new digital formats made to preserve or access the DCO.

Order of Priority	Activity	Risk to digital collection if not actioned
1	It is recommended that the following process is carried out without digitally or physically accessing the digital collection.	The digital collections are exposed to corruption.
2	2.1. Consult museum staff and documentation to map out the extent, type and location of all digital collections considered to be part of the accessioned collection. 2.2. Larger organisations may wish to create a survey that is sent out and followed up with face-to-face consultations to check details.	Some digital collections are not included in the documentation plan and are not accessioned.
3	3.1. Update the documentation plan with the results of consultation with staff. 3.2. In the documentation plan ensure the following is recorded for digital collections: • Actions - List other actions required to document these collections	The museum cannot account for its digital collections, understand the risks or plan for the resource required to fully preserve and manage the digital collections in scope.

⁵⁷ [Digital Preservation Coalition. *Getting Started*. Digital Preservation Handbook.](#)

[Digital Preservation Coalition. *Creating a Digital Asset Register*.](#) Accessed 2023.

⁵⁸ [Government of Canada. *Digital preservation inventory template for cultural heritage institutions*.](#) Accessed 2023.

	and measures to mitigate against short and long term risks. ● Risks - Prioritise in accordance with risk to collection if not documented. ● Location - Record the physical or digital location of each digital collection. ● Formats - Without accessing the file, briefly overview the file type or formats if known, represented in the collection. ● Resources - estimate the time, expertise and resources required to document these collections.	
--	--	--

12. Condition checking and technical assessment

Spectrum definition - documenting the make-up and condition of objects, and noting any resulting recommendations.

For digital collections, this will be very different to physical objects, but it is an essential procedure. It includes virus scanning, [fixity checks](#), [file format validation](#), monitoring storage, and monitoring [file formats](#). The results of these checks should inform any [digital preservation actions](#). Further information see [Chapter 13. Collections care and conservation](#)).

12.1. Spectrum suggested procedure⁵⁹

Spectrum suggested procedure workflow	Is the step in the workflow different for digital collections?
Requesting a check/assessment	
Do the objects need to be moved to be checked?	No.
Carrying out a check/assessment	
Carry out the check or assessment.	Yes. See Section 12.2.
Where possible take photographs.	No.
Record information about the check or assessment.	No.
Record information about the result of the check or assessment.	No.
Responding to a check/assessment	
Update object records with any recommendations on storage, handling, etc.	No.
Does the check cause concern?	No.

⁵⁹ Collections Trust. [Spectrum, Condition checking and technical assessment - suggested procedure](#). Accessed 2023.

12.2. Carrying out a check/assessment

12.2.1. Virus scanning

The following protocol must be integrated into the workflow of any procedure when the digital file is accessed for the first time or when it has been accessed externally. These steps also apply to legacy digital files where there is no evidence that virus software has been used to protect the digital files from viruses and other malware.

For any digital files held on “virtual” digital locations, e.g. a server or the local drive on a museum’s computer, go to [Section 12.2.1.1](#). For any digital files held on [physical digital devices](#), e.g. floppy disks, hard drives or USB sticks, go to [Section 12.2.1.2](#).

12.2.1.1. Digital files held on “virtual” digital locations

<i>Order of Priority</i>	<i>Activity</i>	<i>Risk to digital collection if not actioned</i>
1	1.1. Using a standard networked workstation, download trusted virus scanning software. The National Archives provides some recommendations⁶⁰ in its digital preservation online resource. 1.2. Without transferring or accessing any digital files, open the virus scanning software. Point the application to the folder or other digital location where the digital files are currently held. The application will scan all the folders and files within the digital location. For example, you may have some digital files on one server and some saved to the hard drive of the computer.	Digital files making up a DCO are at risk of corruption or viruses. The latter can easily compromise a museum's IT network.
2	2.1. When the scanning is complete, the anti-virus software will run a report, flagging any digital files with “errors”. These files should not be transferred, accessed or touched in any way until step 4. has been actioned.	Opening files with an error could compromise the IT network.
3	3.1. Document what anti-virus software was used and the date the virus scanning was carried out. 3.2. Document any filenames or folder names with an error, or export the technical metadata from the virus-scan report into a CSV file and save somewhere safe. 3.3. Export any other report the software generates and save in a “metadata” folder with the “safe” digital files.	Documenting digital preservation actions is a vital part of digital preservation best practice and will help provide documentation required as part of the <i>Deaccessioning and disposal</i> procedure.
4	See chapter on <i>Deaccessioning and disposal</i> for recommendations on seeking authorisation for, deleting and documenting digital files where some/all bits are damaged, corrupted or missing.	Seeking appropriate authorisation for deleting or transferring corrupted digital files is an important part of the <i>Deaccessioning and disposal</i> procedure.

⁶⁰ [Digital Preservation Workflows - 1. Select and transfer](#). The National Archives. Accessed 2023.

5	Digital files with no errors are ready to be fixity checked. See Section 12.2.2. Fixity checking below.	N/A
---	---	-----

12.2.1.2. Digital files held on physical digital devices

<i>Order of Priority</i>	<i>Activity</i>	<i>Risk to digital collection if not actioned</i>
1	1.1. Use a workstation that ideally has not been connected to the main IT network, to ensure the network and digital files contained there are not corrupted or compromised. 1.2. If using Write-Blocker⁶¹ software, ensure this is installed on your workstation before you proceed. 1.3. Download a trusted virus scanning software. The National Archives provides some recommendations⁶² in its digital preservation online resource. Your institution may already have virus scanning software installed on workstations. For further information see Section 12.2.1. Virus scanning.	The digital files making up the DCO or the IT network are at risk of deletion, alteration or corruption.
2	2.1. Place the physical digital device into the appropriate reader or port on your workstation. 2.2. Without transferring or accessing any digital files, open the virus scanning software. Point the application to the digital device and scan all the folders and files contained within. The application will scan all the folders and files contained within the device.	The digital files making up the DCO or the IT network are at risk of deletion, alteration or corruption.
3	3.1. When the scanning is complete, the anti-virus software will run a report, flagging any digital files with “errors”. These files should not be transferred, accessed or touched in any way until step 4. has been actioned. The digital device is an effective digital quarantine environment, so the files are safe to leave here until further action is taken.	Opening files with an error could compromise the IT network.
4	4.1. Document what anti-virus software was used and the date the virus scanning was carried out. 4.2. Document any filenames or folder names with an error, or export the technical metadata from the virus-scan report into a CSV and save somewhere safe.	Documenting digital preservation actions is a vital part of digital preservation best practice and will help provide documentation required as part of the <i>Deaccessioning and disposal</i> procedure.

⁶¹ [Example of open source Write Blocker software for USB](#). Accessed 2023.

⁶² [Digital Preservation Workflows - 1. Select and transfer](#). The National Archives. Accessed 2023.

5	See Chapter 18. Deaccessioning and disposal for recommendations on seeking authorisation for, deleting and documenting digital files where some/all bits are damaged, corrupted or missing.	Seeking appropriate authorisation for deleting or transferring corrupted digital files is an important part of the <i>Deaccessioning and disposal</i> procedure.
6	Digital files with no errors are ready to be fixity checked. See Section 12.2.2. Fixity checking below.	N/A

12.2.2. Fixity checking

Fixity checking is a fundamental component of digital “condition checking”, as it provides evidence of missing or corrupted data that can occur during transfer or other actions. A fixity check involves generating a [checksum](#) post file transfer, and comparing it with a checksum generated pre-transfer. A checksum is a unique digital code derived from the file that would change if the number of [bits](#) in the file changed through loss of information or corruption when the file is transferred, [migrated](#), compressed or encrypted. Although checksums can be used to detect if the contents of a file have changed, they cannot identify for you where in the file that the change has occurred, or indeed what the change is.

Ideally a checksum should be generated by the previous owner or custodian and provided for each digital file as part of core [metadata](#) provided about the DCO pre-entry. Similarly, digital files that are exiting the museum as part of the object exit procedure, for example as part of a loan to another institution, should be fixity checked prior to transfer and the checksum should be sent to the recipient as part of core metadata about the DCO.

If the checksum was not provided at entry, or cannot be found, a checksum should be generated as soon as it is safe to do so post entry. There are plenty of tools available online to facilitate this. This checksum and the date it was carried out, should be recorded in the catalogue record for the DCO and used as a control from which future checksums are compared.

Post entry, a fixity check should also be carried out to check that the integrity of the digital file has been maintained since the last fixity check. It should also be carried out after a digital file is transferred between digital locations, migrated or is subjected to any other [digital preservation action](#). In the same way that physical objects are subjected to scheduled condition checks, regular fixity checks should be implemented for the digital collection.

For further information on Fixity Checking, see the Library of Congress blog *Protect your data: File Fixity and Data Integrity*⁶³ and the *Fixity and checksums* chapter of the DPC’s *Digital Preservation Handbook*⁶⁴

⁶³ [Library of Congress. Protect your data: File Fixity and Data Integrity](#). Accessed 2023.

⁶⁴ [Digital Preservation Coalition. Fixity and checksums. Digital Preservation Handbook](#). Accessed 2023.

Order of Priority	Activity	Risk to digital collection if not actioned
1	Check the file metadata and other documentation for a checksum for each digital file. Ideally, this should have been provided by the previous recipient prior to or at the point of entry. If this has not been provided, go to step 2. If it has been provided, go straight to step 3.	If no checksum was provided, there is a risk that the digital file was corrupted during transfer, but there is no evidence that this occurred.
2	If no checksum can be found, generate a checksum on each digital file. Make a note of the checksum code. Open source tools like will do this for you ⁶⁵ .	N/A
3	Carry out the digital preservation action, such as file transfer to a different digital location, migration or normalisation . For further information, see Section 13.3. Carrying out conservation .	N/A
4	Run a fixity check, comparing the original checksum to the checksum generated immediately after the digital preservation action has been carried out. Make a note of any mis-matching checksums.	No evidence that the digital file before the digital preservation action took place is the same or different to the same digital file after the digital preservation action took place.

12.2.3. File format validation

Validation checks whether the content conforms to their [file format](#) specification. In some cases it can also fix issues. It is not always seen as an essential step but can help flag issues. For example, if the content does not conform to this specification then it may be more difficult to read or manage in the future.

For further information on validation and validation software see Section 2.2 of the National Archives' *Digital Preservation Workflows*⁶⁶.

12.2.4. Monitoring formats

As part of the Inventory procedure you will have captured information about the [file formats](#) in the DCOs (see [Section 6.4](#)). You should monitor your content to understand if any of the file formats you hold, or the software/technology needed to access them, are at risk of becoming obsolete (outdated or no longer used). For more information see Section 3.5 of The National Archives' *Digital Preservation Workflows*⁶⁷.

If you are concerned about [obsolescence](#) then please see [Section 13.3 Carrying out conservation work](#).

⁶⁵ [Hash Generator](#). Accessed 2023.

⁶⁶ [Digital Preservation Workflows](#). The National Archives. Accessed 2023.

⁶⁷ [Digital preservation workflows. 3. Preserve](#). The National Archives. Accessed 2023.

12.2.5. Monitoring storage

The lifetime of storage can be short – it can fail or corrupt the content. You will need to review your storage every 3-5 years and may need to move content onto new storage. For more information see Section 3.4 of The National Archives' *Digital Preservation Workflows*⁶⁸.

⁶⁸ [Digital preservation workflows. 3. Preserve.](#) The National Archives. Accessed 2023.

13. Collections care and conservation

Spectrum definition - managing and documenting any conservation work on particular objects, such as treatments to slow decay, repair damage or improve appearance.

For digital collections, this will be very different for physical objects, but it can include [normalisation](#), [format migration] or [emulation](#). These [digital preservation actions](#) should be informed by the results of the technical assessment. For further information, see [Chapter 12. Condition checking and technical assessment](#).

13.1. Spectrum suggested procedure⁶⁹

Spectrum suggested procedure workflow	Is the step in the workflow different for digital collections?
Agreeing conservation work	
Scope the work to be carried out.	Yes. See Section 13.2.1.
Reach agreement on the work to be carried out.	Yes. See Section 13.2.2.
Provide the conservator with information about each object.	No.
Record information about the conservation work before it is carried out.	No.
Carrying out conservation work	
Move the objects.	No. Only applicable for DCOs with physical components or carriers.
Carry out the agreed conservation work.	Yes. See Section 13.3.1.
Recording conservation work	
At the time, or as soon as possible, record details of the job and the work on each object.	Yes. See Section 13.4.1.
Add relevant information from the conservation record to your documentation system.	Yes. See Section 13.4.2.

⁶⁹ Collections Trust. [Spectrum, Collections care and conservation - suggested procedure](#). Accessed 2023.

Check the objects on the agreed recall dates.

No.

13.2. Agreeing conservation work

13.2.1. Scope of the work to be carried out

The condition checks carried out as described in [Chapter 12. Condition checking and technical assessment](#) will help identify potential need for [digital preservation actions](#). Understanding what you have will help you plan for any future work.

Whilst standard Spectrum procedures often involve a conservator, this may require input from IT professionals and other specialists.

Before agreeing on a preservation approach for one DCO or a group of DCOs, it is useful to consider a number of factors that may inform the approach.

- What version, parts, aspects of the digital object or eco-system have been acquired?
- What was the reason for acquiring the DCO and why is it significant to the museum?
- Were any agreements made with the donor and rights holders on the digital preservation approach or the NSDA level of preservation to be achieved?
- What skills, knowledge and infrastructure can be utilised in-house to preserve and store the DCO now and in the future?
- What skills, knowledge and infrastructure will need to be out-sourced?
- Is it possible to contact the artist/creator/producer to discuss if the preservation approach aligns with their intention for the digital object?

For some complex digital objects, it has been recommended that a partnership approach may be more suitable where organisations pool resources to acquire and preserve a DCO. Annet Dekker⁷⁰ proposes the concept of ‘networks of care’, where professionals and amateurs from the digital preservation community work together to endeavour to reproduce the work as close as possible to its original intention, rather than a static copy. Although museums have rightly taken a very cautious approach to conservation for physical objects, an iterative, experimental approach is recommended for preserving some digital heritage, as in some cases there are no precedents for preserving this material. If we don’t try to preserve this heritage, there is a very real risk that no one else will.

13.2.2. Reach agreement on the work to be carried out

Refer for example to available guidance on appropriate [file migrations](#). See suggested preservation actions in [Section 13.3. Carrying out conservation work](#).

⁷⁰ Dekker, A. *Collecting and conserving net art: moving beyond conventional methods*. London: Routledge. 2018.

Consider who will be involved in agreeing any proposed [digital preservation actions](#), where required. Ensure this is recorded in your organisation's digital preservation policy.

Check the terms and conditions of the acquisition and any rights restrictions to check what can be preserved and if permission should be granted before proceeding. If the DCO is a loan, seek permission from the lender in the usual way.

13.3. Carrying out conservation work

13.3.1. Carry out the agreed conservation work.

The following are examples of [digital preservation actions](#) that can be carried out on digital files, particularly if you are concerned the [file formats](#) you hold, or the software/technology needed to access them, are at risk of becoming [obsolete](#) (outdated or no longer used):

- [Format migration](#) - involves migrating digital files from old file formats to a new format when they are at risk of becoming obsolete.
- [Normalisation](#) - is similar to format migration, but usually happens during the acquisition procedure. You may choose to convert particular types of digital files into a preferred file format when you first receive the DCO. This ensures that the DCO is easier to manage as it's in a format familiar to the museum.
- [Emulation](#) - is an alternative to format migration and attempts to recreate the functionality of the original software or technology.
- Hardware preservation - This involves the keeping of computers and their systems software as well as the data and applications programmes. This approach is particularly important for digital artworks if the artist specifies the particular device or machine in which the DCO should be displayed.

Please note that some of the preservation actions above such as format migration and normalisation may not be suitable for some DCOs such as digital artworks, especially where the action could change the original intention of the artwork.

For further information on these see the Digital Preservation Coalition Handbook⁷¹.

⁷¹ Digital Preservation Coalition. [Preservation action - Digital Preservation Handbook](#). Accessed 2023.

13.4. Recording conservation work

13.4.1. At the time, or as soon as possible, record details of the job and the work on each object

At the time, or as soon as possible, record details of the digital preservation action carried out. Record the date and the individual who carried out the action.

13.4.2. Add relevant information from the conservation record to your documentation system

Check the DCOs on the agreed recall dates. For further information, see [Chapter 12. Condition checking and technical assessment](#).

14. Valuation

Spectrum definition - documenting the financial value of objects, whether your own or borrowed.

This procedure is no different for digital collections – refer to the Spectrum suggested procedure⁷²

15. Insurance and indemnity

Spectrum definition - ensuring your own objects, loans and other objects left in your care have appropriate cover against damage or loss.

This procedure is no different for digital collections – refer to the Spectrum suggested procedure⁷³

⁷² Collections Trust. [Spectrum, Valuation - suggested procedure](#). Accessed 2023.

⁷³ Collections Trust. [Spectrum, Insurance and indemnity - suggested procedure](#). Accessed 2023.

16. Emergency planning for collections

Spectrum definition - managing information about potential risks to all the objects in your care, and the action to be taken in emergency situations.

For digital collections, it is important to ensure that Digital Collections Objects (DCOs) are included in the plan and there are some specific aspects to consider.

16.1. Spectrum suggested procedure⁷⁴

Spectrum suggested procedure workflow	Is the step in the workflow different for digital collections?
Assessing risk	No.
Assess the risks to objects in your care.	No.
Create plan for minimising the risks, with recommendations.	No.
Put the recommendations into action.	No.
Review risk assessment regularly.	No.
Creating an emergency plan	Yes. See Section 16.2.
List key people and their emergency contact details.	No.
List the locations to be used in the case of evacuation.	No.
Record priority codes for removing objects from an emergency area.	No.
Draw up site plans.	No.
Identify and list equipment you might need in an emergency.	No.
Note immediate steps to care for objects after an emergency.	No.

⁷⁴ Collections Trust. [Spectrum, Emergency planning for collections](#). Accessed 2023.

Note first aid steps for damaged objects, by material.	No.
Note the backup location of core inventory information.	No.
Compile this information into an easy-to-follow emergency plan.	No.
Staying prepared	No.
Train all staff and volunteers in how to put the emergency plan into action, and practise regularly.	No.
Review the emergency plan regularly.	No.

16.2. Creating an emergency plan

When creating an emergency plan for collections ensure that Digital Collections Objects (DCOs) are included in the plan. The plan will be a mix of risk assessment and mitigation. There is a need to separate out prevention and response. If you have a separate IT department they should provide input to the creation of the plan, and help manage the response to emergencies.

In particular consider:

- What can be put in place to safeguard DCOs?
- How will at least one copy of every [source digital file](#), [digital preservation derivative](#), [supporting file](#) and any unique hardware and software required to render the DCO, be recovered in the event of an emergency?
- How each copy of the digital files, in various formats, are stored and backed up (who has access to masters and copies, who has control?). It is recommended that exact copies of a digital file are stored on geographically separate digital environments. It is likely you will require multiple copies of each DCO on multiple formats in multiple, geographically separate locations.
- How can DCOs be protected from accidental or intentional deletion, either by a member of staff or a hacker. With prevention of hacking it might be necessary to have input from a cyber security expert.
- How to protect your DCOs from malware, particularly when acquiring or transferring files externally.
- How to protect sensitive and personal data or content from being published or hacked.

17. Damage and loss

Spectrum definition - responding to the damage or loss of objects in your care. In particular, documenting the incident and recording decisions made and actions taken.

This procedure is no different for digital collections – refer to the Spectrum suggested procedure⁷⁵

⁷⁵ Collections Trust. [Spectrum, Damage and loss - suggested procedure](#). Accessed 2023.

18. Deaccessioning and disposal

Deaccessioning and disposal involves the formal decision by a governing body to take objects out of its accessioned collection ('deaccessioning'), and managing the disposal of those objects through an agreed method.

For digital collections, there are some needs that are different to physical objects including destroying/deleting and transfer.

18.1. Spectrum suggested procedure⁷⁶

Spectrum suggested procedure workflow	Is the step in the workflow different for digital collections?
Deaccessioning objects	Yes. Section 18.2.
Check possible sources of information about the objects.	No.
If in doubt, seek advice.	Yes. Section 18.2.1.
Select the method of disposal and seek authorisation.	No.
Does your governing body approve the disposal?	No.
Disposing of objects	
Are the objects to be destroyed?	Yes. See Section 18.3.1.
Approach potential recipients directly or advertise the disposal appropriately.	Yes. See Section 18.3.2.
Do you have a suitable recipient?	No.
Agree terms with the new owner and transfer legal title to them.	Yes. See Section 18.3.3.
Arrange for the objects to be collected or delivered, along with relevant original documents.	No.
Recording the disposal	
Record information about the disposal process.	No.

⁷⁶ Collections Trust. [Spectrum, Deaccessioning and disposal - suggested procedure](#). Accessed 2023.

Update your accession register, if applicable.	No.
Update catalogue records if not done already.	No.
Update your list or file of disposed objects, if applicable.	No.
Guidance Notes	
Note 1: Destroying objects	No.

18.2 Deaccessioning objects

Deaccessioning a DCO involves the complete removal of all physical and digital components and digital copies from the registered collection.

For DCOs, the reason for deaccessioning and disposal might include one of the following:

- The museum does not have the capacity, storage space, resource or in-house expertise to manage and/or digitally preserve the DCO either now or in the long term.
- The museum does not have the capacity, resource or in-house expertise to manage and/or digitally preserve or maintain software or hardware to enable the ongoing preservation or access of the DCO.
- The museum does not have the rights to carry out actions on the DCO considered fundamental to its preservation, use, or access.
- There is another exact copy of the DCO with the same digital provenance, [metadata](#) and [checksums](#).
- Any/all metadata, hardware or software used to describe or provide access to the DCO has been lost, meaning that the DCO cannot be accessed and/or understood, e.g. encryption keys.
- The [source digital files](#) that make up the DCO are corrupted beyond repair, the data completely destroyed and no copies were made.
- The museum is rationalising its collections and the DCO no longer fits within the museum's collecting policy.

18.2.1. If in doubt, seek advice

Refer to Spectrum procedure and then note the following recommendations for DCOs:

- Seek legal advice before proceeding with deaccessioning a DCO, particularly DCOs under copyright, licence or other legal contract.
- Seek advice from the digital preservation and GLAM community as there is currently no precedent or ethical guidance on deaccessioning and disposing of DCOs within museums.

18.3. Disposing of objects

18.3.1. Are the objects to be destroyed?

A Digital Collection Object (DCO) should only be destroyed once all opportunities for transfer have been explored, and advice has been sought from the digital preservation community, or if the object has become corrupt or [obsolete](#) with no possibility of backup, [format migration](#) or [emulation](#) that would enable access in the future.

If the decision to destroy a DCO is made, a robust deletion process must be followed. When deleting the DCO consider the following:

- Are there [digital preservation derivatives](#) or other copies of the DCO stored in different locations? They will need to be deleted too.
- Are there backups of your [digital collections storage](#)? How will you manage copies of the DCO in any storage backups?

18.3.2. Approach potential recipients directly or advertise the disposal appropriately

Information provided to potential recipients should include:

- Resources and expertise required to digital preserve the DCO now and in the long term.
- The level of digital preservation recommended for the long term access of the DCO.
- Costs involved in digital preserving the DCO in the long term.

18.3.3. Agree terms with the new owner and transfer legal title to them

The museum should agree to the conditions of transfer, including the minimum digital preservation level that the organisation should aim to achieve. Only organisations with appropriate expertise and resources to manage and digitally preserve the DCO in the long term should be considered.⁷⁷

⁷⁷ [Digital Preservation Coalition Handbook. Retention and review](#). Accessed 2023.

19. Rights management

Spectrum definition - managing the intellectual property rights and data protection rights associated with objects, reproductions and information.

This is an important procedure for digital collections since they are potentially subject to a wider range of rights than physical objects. There are some specific aspects that need considering including researching the rights and getting permissions.

19.1. Spectrum suggested procedure⁷⁸

Spectrum suggested procedure workflow	Is the step in the workflow different for digital collections?
Researching rights associated with your collections	
Research the rights associated with objects, reproductions and information in your collection.	Yes, see Section 19.2.1.
For each right, record information about the right and its holder.	No.
If the rights holder is not known, record them as 'unknown' and keep a due diligence file of your research.	No.
Maintain your rights records.	No.
Getting permission from other rights holders (Rights in)	
Ask the rights holder, or their agent, for permission to use their material in the way you want.	Yes. See Section 19.3.1.
Record information about the permission (which might be a formal licence).	Yes. See Section 19.3.2.
Licensing your rights to others (Rights out).	No.
Do you agree to the proposed use?	No.
Propose the terms of the licence you offer.	No.
Record information about the licence.	No.

⁷⁸ Collections Trust. [Spectrum, Rights management - suggested procedure](#). Accessed 2023.

19.2 Researching rights associated with your collection

19.2.1 Research the rights associated with objects, reproductions and information in your collection

Digital Collection Objects (DCOs) are potentially subject to a wider range of rights than physical objects. For a complex digital object you may need to allocate a greater amount of time to researching the rights which exist within the object. The rights you may encounter for objects produced under UK legislation are:

- **Intellectual Property rights:** IPR or specifically copyright, will exist in all categories of DCO. Aspects that may be copyrighted are artworks, photographic images, design documents and source code. See [Section 19.2.1.1. Intellectual property rights](#) for further details.
- **Design rights:** Registered designs may exist in commercially produced DCOs. Aspects that may be registered designs are icons, fonts and graphic symbols.
- **Database rights:** Database rights exist in the structured compilation of data. This includes database structures and websites, but also the layout of a user interface in a software based object. Unlike copyright, which expires, these rights may be renewed indefinitely by the rights holder so will need to be monitored.
- **Trademarks:** Trademarks may exist for commercially produced objects. These include company logos. These rights may be renewed indefinitely by the rights holder so will need to be monitored.
- **Patents:** In rare circumstances, patents may exist in the technical function of a DCO. An example would be phone or computing technology which the collection has acquired as a working object. If you wish to emulate a patented experience within the period of the patent, you will need to negotiate the right to do this.
- **Data protection:** In some cases, where personal data is contained in the DCO, specific permissions may need to be sought. See [Section 19.2.1.2. Data protection](#) for further details.

The Collections Trust holds a detailed set of resources which provide support for researching rights in collections.⁷⁹

19.2.1.1. Intellectual property rights

As part of the project 'Preserving and sharing born-digital and hybrid objects from and across the National Collection', a IPR decision model⁸⁰ has been produced, to be used by curators, registrars and other colleagues involved in acquiring DCOs. The full decision model can be accessed in the footnotes, but here is a summary of the key questions:

- Are relevant rights to elements of the DCO held by the creator or donor?
- Is it possible to work with the donor/creator to secure these rights?

⁷⁹ Collections Trust. [Spectrum Related Resources - Rights management](#). Accessed 2023.

⁸⁰ [Preserving and sharing born-digital and hybrid objects from and across the National Collection. Decision Models Report](#). Gabi Arrigoni, Victoria and Albert Museum, Natalie Kane, Victoria and Albert Museum, Stephen McConnachie, British Film Institute, Joel McKim, Birkbeck University. January 2022. p.17. Accessed 2023.

- Are all rights required for preservation and access being transferred at the point of acquisition?
- If not all rights have been transferred, can a licence or other agreement be used to permit the organisation to carry out the required preservation and allow the required access or use?
- Consult with a rights lawyer for advice on how to proceed.

19.2.1.2. Data protection

As part of the project “Preserving and sharing born-digital and hybrid objects from and across the National Collection”, a Data protection decision model⁸¹ has been produced, to be used by curators, registrars and other colleagues involved in acquiring DCOs. The full decision model can be accessed in the footnotes, but here is a summary of the key questions:

- Does the personal data come with formal waivers or permissions for reuse outside the original context and if not can they be sought?
- Is it possible to anonymise the data to the extent required under law, without compromising the object’s value?

19.3. Getting permission from other rights holders (Rights in)

19.3.1. Ask the rights holder, or their agent, for permission to use their material in the way you want

You do not need to seek permission to copy the Digital Collection Object (DCO) for preservation. Legislation has been passed in the UK which allows museums, libraries, and archives the right to make copies of ‘works’ in their collection for the purposes of archiving and preservation if it is not reasonably practicable to purchase a replacement. For further information see *Exceptions to copyright: Libraries, archives and museums*, issued by the Intellectual Property Office⁸².

In advance of negotiation of usage rights, you should identify how you wish to use the DCO, how you wish to preserve the DCO and how you wish to license the object to third parties. This information should be recorded in the object documentation.

You may need to approach the same rights holder for several categories of rights. You should be explicit about each type of right you wish to seek permission for.

⁸¹ [Preserving and sharing born-digital and hybrid objects from and across the National Collection. Decision Models Report](#). Gabi Arrigoni, Victoria and Albert Museum, Natalie Kane, Victoria and Albert Museum, Stephen McConnachie, British Film Institute, Joel McKim, Birkbeck University. January 2022. p.18. Accessed 2023.

⁸² Intellectual Property Office. [Exceptions to copyright: Libraries, archives and museums](#). Accessed 2023.

19.3.2. Record information about the permission (which might be a formal licence)

As rights in digital collections may encompass a range of rights, which each have different terms, it is vital that the recording of rights should document the element of the object covered by the right, the type of intellectual property right which applies, and the expected expiry or renewal date for that right.

You will need to revisit any trademark or database rights when the expected expiration date approaches to document any renewals.

If the DCO has been acquired from an established company (e.g. a software provider), the permissions you have may be documented in their own standard usage agreement. In these circumstances, this should be attached to the object documentation in addition to recording the rights in the object record.

20. Reproduction

Spectrum procedure - managing and recording the creation of images and other kinds of reproduction of objects, including digital copies.

For digital collections, this involves making access copies of [source digital files](#).

20.1. Spectrum suggested procedure⁸³

Spectrum suggested procedure workflow	Is the step in the workflow different for digital collections?
Requesting reproduction	
Clarify the main purpose of the request.	No.
Check that the request is in line with your rights management policy.	No.
Send whoever is carrying out the reproduction the information they need.	
Do the objects need to be moved?	No.
Make the reproduction.	Yes. See Section 20.2 .
Documenting the resulting reproduction	
Record information about the reproduction.	

20.2. Make the reproduction

20.2.1 Access and re-use copies

You may wish to create access or re-use copies of the digital files. For example, providing access to a researcher or re-using it in an exhibition. This can include converting the files to a different [file format](#) to reduce their size (e.g. MP3 for audio content, JPG for images) and/or to make the content more accessible because free viewers are available (e.g. PDF). This can be undertaken when you acquire the content or you may decide to only create

⁸³ Collections Trust. [Spectrum, Reproduction - suggested procedure](#). Accessed 2023.

access copies when someone requests access. If you are using a CMS or DAMS then it may automatically create access copies for certain file formats.

For more information see Section 4.3 of The National Archives' *Digital preservation workflows*⁸⁴.

⁸⁴ [Digital Preservation workflows. 4. Access. The National Archive.](#) Accessed 2023.

21. Use of collections

Spectrum definition - managing and recording how your collections, including images and other reproductions of them, are used, whether by you or anyone else.

This procedure is no different for digital collections – refer to the Spectrum suggested procedure⁸⁵

22. Collections review

Spectrum definition - managing and documenting any formal assessment of your collections that follows a stated methodology.

This procedure is no different for digital collections – refer to the Spectrum suggested procedure⁸⁶

⁸⁵ Collections Trust. [Spectrum, Use of Collections - suggested procedure](#). Accessed 2023.

⁸⁶ Collections Trust. [Spectrum, Collections review - suggested procedure](#). Accessed 2023.

23. Audit

Spectrum definition - systematically checking the accuracy and completeness of the information you have about your collections.

For digital collections, this includes some additional needs such as having the correct information to open and access digital files and checking digital files' content.

23.1. Spectrum suggested procedure⁸⁷

Spectrum suggested procedure workflow	Is the step in the workflow different for digital collections?
Identifying the scope of an audit	
Agree the aims and scope of the audit and create a written brief.	No.
Auditing objects	
Decide the group of objects to be audited and generate a list from your core inventory information.	No.
Verify the physical presence of each object and the accuracy of associated core inventory information.	Yes. See Section 23.2.1.
Record information about the audit process.	No.
Record the result for each object, or group of objects, being audited.	No.
Auditing object information	
Check that the information being audited is present and accurate.	No.
Record information about the audit process.	No.
Record the result for each object record being audited.	No.

⁸⁷ Collections Trust. [Spectrum, Audit - suggested procedure](#). Accessed 2023.

Post-audit action	
Report the results of the audit in line with your policy.	No.
Agree any action needed.	No.
Go to the appropriate procedure for further action.	No.

23.2. Auditing objects

23.2.1. Verify the physical presence of each object and the accuracy of associated core inventory information

- Check that all digital and physical components, supporting metadata files, hardware and software and preservation copies are in the digital or physical location they are expected to be in.
- Check that all encryption keys, [metadata](#) and other information such as copyright permissions are available so that the files can be opened, content accessed and verified.
- Open files and check files' content as expected.

A.1. Glossary

Glossary term	Definition
Authenticity	Proof that the digital files that make up the DCO are authentic. This may be particularly important for digital artwork.
Auxiliary object	Hardware that has not been acquired but required to provide access or long term digital preservation to the DCO.
Bit	‘Binary digit’ – the smallest unit of data held in a digital file or computer The digital file or computer renders the bits into information and content.
Bit rot	Describes the decay of software over time.
Bit-level preservation	A term used to denote a very basic level of preservation of the DCO, ensuring that the source digital files are safe and backed up. Bit-level preservation is not digital preservation but it does provide the foundations for best practice digital preservation that ensure the survival of the DCO in the long term.
Checksum	A unique digital code or fingerprint generated from the digital file that would change if the number of bits in the file changed through loss of information or corruption when the file is accessed, transferred, migrated , compressed or encrypted. A checksum is used to validate and authenticate a file. The process of comparing a checksum is called a fixity check .
Checksum type	The algorithm used to generate the checksum. The museum needs to know this so it can run another checksum on entry using the same algorithm.
CSV file	A comma-separated values (CSV) file is a delimited text file that uses a comma to separate values. Each line of the file is a data record. Each record consists of one or more fields, separated by commas. The use of the comma as a field separator is the source of the name for this file format. Excel spreadsheets can be easily converted into a CSV file and used to import data into databases.
Data tape storage	A system for storing digital information on magnetic tape. Data tape storage is considered to be one feasible option for backing up and storing digital files safely in the long term.
Descriptive metadata	Descriptive metadata is a subcategory of metadata and is normally recorded either in the digital file itself or in a dedicated metadata file that should be kept with the Digital Collection Object (DCO). Unlike technical metadata, it is recorded by a human, and normally describes meaningful attributes of the digital file or DCO not recorded in the technical metadata such as title, creator, object name, copyright holder and owner. If the digital file is shared or loaned, the metadata recorded in the digital file is an essential means of identifying and documenting core information. This information can also be used to aid discovery if shared online.
Digital dependency	Any technology (software or hardware), information or other factors that are required to ensure the DCO can be accessed, preserved, stored and experienced in the way the creator intended. It is a dependency if the DCO cannot be used without it.
Digital art installation	An artistic work or practice that uses digital technology as part of the creative or presentation process.

Digital asset	Anything that exists in a digital format and comes with the right to use. Data that does not possess that right is not considered an asset. Examples include digital images held in Picture Libraries, supporting documentation in electronic form or audio-visual files that are held in the museum to document events, objects and aid interpretation and access of the physical collection and other museum activities. Digital assets are a corporate asset of the museum, and are not normally acquired into the accessioned collection.
Digital collection storage environment	The set of software and hardware elements which together are used to store, manage and preserve a digital collection.
Digital forensic tool	Digital forensics was originally developed to provide evidence in digital materials that could be used to solve criminal investigations. For example, it is used to prove that an internet video is a “Deep fake” that has been created to slander someone’s reputation or could be used to provide evidence that phone data has been deleted. Digital forensic technology is now used in a number of open source applications that are widely used in digital preservation to help us scan, analyse and review digital files and physical digital devices without opening and accessing them, which would expose the digital files to corruption, deletion, or other changes. It ensures the technical metadata in the original digital object is not changed or updated and is the same DCO that was received at the point of entry into the museum. If we were to open the digital file, before it had been fixity checked, virus scanned and copied, this action would change the technical metadata in the file and would affect the integrity of the Digital Collection Object (DCO).
Digital quarantine environment	Used to temporarily store digital files that have not yet been virus scanned and could corrupt or damage other digital files or the IT network. The storage solution should sit outside the museum’s IT network.
Digital preservation action	An action that can be taken to help mitigate the technical challenges of preserving DCOS over time. Includes normalisation , format migration and emulation .
Digital preservation derivative	A digital derivative is a digital file, that is an exact copy, derived from the source digital file, that is created for digital preservation purposes.
Digital preservation strategy	The strategy, based on policy, which leads to actions that ensure access to digital assets , regardless of the challenges of media failure and technological change.
Emulation	The imitation of the behaviour of a computer, or other electronic system, with the help of another type of computer or system. Especially old systems that are no longer being used.
Executable format	The executable format is the form in which the software is run or executed. This is typically the primary form in which software is distributed and accessed. Examples include Windows .exe files and Java .jar files.
File format	The file format for each digital file. This information is required to inform future digital preservation actions.
File header metadata	Metadata held in the file header contains information that will not be accessible to the user but useful for administrative purposes, such as title and links to style sheets. For example in image files the header stores metadata about an image’s size, resolution, number of colours, and so on.
File manifest	A file containing metadata for a group of accompanying files that are part of a set or coherent unit.

File packaging	File packaging is the process used to keep the metadata and digital files used for a complex digital object together and in order. This is useful when the files are being transferred internally or externally. <i>BagIt</i> File Packaging Format is a file packaging specification that enables you to keep together digital files in their original formats, within “bags”, meaning that all digital files part of the same DCO will be kept together at transfer. Bagger is the corresponding open source application that packages data files according to the BagIt specification.
File path	The form of the name of a file or directory, specifies a unique location in a computer file system.
File size	The size of each digital file for each Digital Collection Object (DCO) in megabytes (MB), gigabytes, terabytes (TB) or petabytes (PB). This information is very useful during resource planning to calculate the total size of the deposit and the digital storage capacity required.
File transfer	The process of digitally transferring a digital file from an external or internal digital location to a new digital location.
File transfer platform	A digital object 'virtual' entry method involving file transfer of digital files from an external source with no physical digital device. This entry method is managed and controlled. Digital files are uploaded and transferred onto a dedicated file transfer platform which manages and organises the stages of transfer, validation and receipt of files from the depositor to the museum.
File format validation	The process of checking whether the digital files conforms to their file format specification. For further information see Section 12.2.3. File format validation .
Filelist	The set of files associated with each other in some way.
Fixity check	A fixity check is the process of checking and comparing the checksums for a digital file before transfer and after transfer to ensure that the digital file in location ‘x’ is an exact copy of the received digital file in location ‘y’. It is the process of checking the integrity of a file and verifying it has not been altered or corrupted. For a fixity check to work, a checksum should be provided by the lender, creator of acquisition prior to entry. The museum can then generate their own checksum immediately after object entry and compare the code. The original checksum provided at entry can be used again and again to confirm that the digital file is still the same after the digital file has been copied, transferred and other digital preservation actions are carried out to it throughout its life at the museum. If the codes are identical this is proof that the file received is exactly the same as the file transferred by the sender with exactly the same number of bits. For further information see Section 12.2.2 Fixity check .
Metadata	The data which provides information about one or more aspects of another entity, such as an image, text, audio-visual file, object, person, organisation, place or event.
Metadata standard	A requirement which is intended to establish a common understanding of the meaning or semantics of the data, to ensure correct and proper use and interpretation of the data by its owners and users.
File format migration	The process of migrating digital files from old file formats to a new format when they are at risk of becoming obsolete.
Normalisation	Normalisation is the process of converting a digital object from its original format to an accepted format in order to make it easier to manage the collections.
OAIS	Open Archival Information System (OAIS) is an international standard widely used by the archive sector to ensure that digital files are described consistently and information shared to ensure long term preservation and access.

Obsolescence	A state of being which occurs when an object, service, or practice is no longer maintained, required, or degraded even though it may still be in good working order.
Open file format	A file format for storing digital data, defined by a published specification usually maintained by a standards organisation, and which can be used and implemented by anyone.
Open source software	A type of computer software in which source code is released under a license in which the copyright holder grants users the rights to use, study, change, and distribute the software to anyone and for any purpose.
Original filename/foldername	The unique name assigned to the digital files and the folder the files are supplied in. It is the name assigned by the creator of the file, prior to entry and not to be confused with any in-house file/folder name assigned after entry. For further information about managing and renaming (or not) file and folder names, see Section 7.4. File and folder names .
Physical digital container	The bits are organised and stored on a piece of hardware or a physical digital storage device.
Physical digital device	Some digital files are stored temporarily or longer term, on physical digital devices, such as hard drives, USB sticks. They are physical, portable devices and can be stored in a physical location.
Proprietary software	Computer software where preservation, access, use or other activities are restricted by copyright, contract or patent law. Most proprietary software is covered by copyright and an end-user licence agreement, some of which stipulate that the licensor can be held liable for damage that arises through ‘improper use of the software’. Software patents are commonly granted to protect exclusive rights to algorithms and unique software functionality. The source code for a piece of software is routinely handled as a trade secret, a form of intellectual property rights that protect formula, design and processes.
Sidecar file	A computer file that stores data (often metadata) which is not supported by the format of a source file.
Standard physical entry	Physical object entry as described in Spectrum <i>Object entry</i> procedure.
Source code	Source code is the form in which the software is authored. It describes what the software does and is written in a programming language. Source code acts as both a form of documentation and as the basis for future preservation strategies such as code migration.
Source digital file	The source digital file is the “original” digital file received at the point of entry into the museum. They should not be used for access. These digital files render the DCO at the point of entry and should be accessioned into the museum’s registered collection. Sometimes referred to as the “master preservation copy”. This term has not been used due to its associations with slavery.
Supporting digital file	Supporting digital files are digital files that provide metadata and other information such as source code that ensure the source digital files are rendered, preserved and interpreted in the correct way.
Technical metadata	Information on the technical properties of a digital file or the particular hardware and software environments required in order to render or process digital information.

Unmanaged virtual entry	A digital object entry method involving file transfer of digital files from an external source with no physical digital device . This entry method is unmanaged. It includes: download from an online source, an email attachment or an encrypted URL link e.g. Vimeo. It is recommended that only trusted secure digital sources are used.
Virus scanning	The process, using software of examining digital files to prevent, detect, and remove malware. For further information see Section 12.2.1. Virus scanning .
Write blocker	Software or hardware that permits read-only access to data storage devices without compromising the integrity of the data. A write blocker, when used properly, can guarantee the protection of the data chain of custody and integrity of the digital file. It is advisable to use a Write blocker when accessing a physical digital device on a workstation. Write-blockers prevent any data from being written to or deleted from the physical digital device, and therefore safeguard it from the accidental deletion of files and any changes to the files introduced by accessing them. There are both software and hardware Write-blocker options available.⁸⁸ For further information about Write-Blockers software, see Technical solutions and tools⁸⁹, a resource produced by the Digital Preservation Coalition.
Workflow	An orchestrated and repeatable pattern of activity that delivers an expected result.
XML file	Extensible Markup Language (XML) is a markup language and file format for storing, transmitting, and reconstructing arbitrary data. It defines a set of rules for encoding documents in a format that is both human-readable and machine-readable. Like CSV, XML is commonly used to export metadata from a digital file.

A.2. Other Glossaries

URL	Description
https://dptp.london.ac.uk/mod/glossary/view.php?id=2323&mode=letter&hook=A&sortkey=&sortorder=	<i>OAIS Glossary</i> 2018.
https://www.dpconline.org/handbook/glossary	<i>Digital Preservation Coalition Handbook. Glossary.</i>
https://nationalarchives.gov.uk/archives-sector/projects-and-programmes/plugged-in-powered-up/digital-preservation-workflows/glossary/	<i>The National Archives Digital preservation workflow.</i>

⁸⁸ [Comparison between Hardware and software Write Blockers. Write Blockers – Hardware vs Software](#). Accessed 2023.

⁸⁹ [Technical solutions and tools. Digital Preservation Coalition](#). Accessed 2023.

A.3. Bibliography

Subject	Description	Author	Title
Collections management guidance	A guide to rights management.	Collections Trust	Rights management
Collections management guidance	A guide to copyright exceptions for the GLAM sector.	Intellectual Property Office	Exceptions to copyright: Libraries, archives and museums
Collections management and digital preservation guidance	A guide and researching findings, written by museum sector experts on managing complex digital and hybrid physical/digital objects.	Gabi Arrigoni, Natalie Kane, Stephen McConnachie, Joel McKim	Preserving and sharing born-digital and hybrid objects from and across the National Collection
Collections management and digital preservation guidance	Practical guidance on creating an inventory of digital assets within a cultural organisation.	Government of Canada	Digital preservation inventory template for cultural heritage institutions
Collections management and digital preservation guidance	A toolkit on contemporary collecting, including a chapter on digital preservation.	Ellie Miles, Susanna Cordner, Jen Kavanagh	Contemporary Collecting: An ethical toolkit for museum practitioners
Digital preservation guidance	BitCurator collates resources, webinars and tools useful for digital preservation.	BitCurator Consortium	BitCurator
Digital preservation guidance	An introduction to digital forensics.	Bodleian Libraries, Oxford University	Introduction to Digital Preservation: Digital forensics
Digital preservation guidance	Introduction to digital preservation best practice and concepts.	Digital Preservation Coalition	Digital Preservation Handbook
Digital preservation guidance	List of digital formats and devices that are at risk of obsolescence .	Digital Preservation Coalition	The “Bit List” of Digitally Endangered Species
Digital preservation guidance	Overview of the risks of not carrying out digital preservation and the benefits of implementing digital preservation best practice.	Digital Preservation Coalition	What are the risks of not preserving digital material?
Digital preservation guidance	A quick introduction to some basic digital preservation concepts.	Digital Preservation Coalition	Just Keep the Bits: An introduction to digital preservation
Digital preservation guidance	Practical guide of how to implement digital preservation workflow in your organisation.	Kevin Bolton, Jan Whalen and Rachel Bolton	Guidance for Digital Preservation Workflows

Digital preservation guidance	Introduction to digital preservation best practice and concepts.	Library of Congress	Digital Preservation
Digital preservation guidance	An introduction to fixity checking and data integrity.	Library of Congress	Protect your data: File Fixity and Data Integrity
Digital preservation guidance	Introduction to digital preservation best practice and concepts.	The National Archive	Preserving Digital Records
Digital preservation guidance	Very useful practical step-by-step instructions or workflows to be used by archives to transfer digital collections into the archive, access the content and preserving it for the long term. Some of the procedures will be different in museums.	The National Archive	Digital Preservation Workflows
Digital preservation tools	Example of an open source tool that generates a checksum on your digital files.	Hash Generator	Hash Generator
Digital preservation tools	An introduction to digital asset management systems.	Collections Trust	Digital Asset Management
Digital preservation tools	BagIt is a technical specification that describes how digital files and accompanying metadata and other files, together in a "Bag", so the digital files can be more easily moved together and the relevant checks are carried out to ensure the digital files in the bag have moved correctly.	Library of Congress	BagIt File Packaging Format
Digital preservation tools	Bagger is an application that puts digital files and accompanying metadata and other files, together in a "Bag", so the digital files can be more easily moved together and the relevant checks are carried out to ensure the digital files in the bag have moved correctly. It follows the BagIt specification.	Library of Congress	Bagger
Digital preservation tools	An introduction to digital preservation systems.	The National Archives	Digital Preservation tools and systems
Digital preservation tools	DROID File format profiling tool produced by TNA.	The National Archives	File Profiling Tool (DROID)
Metadata	Introduction to metadata standards .	Collections Trust	What information should I record?
Metadata	Introduction to metadata.	Getty Research Institute, 2016	Introduction to Metadata

Models and standards	Metadata standard, focussing on the information required to manage and preserve digital objects so they are identifiable, retrievable, understandable and viable.	Library of Congress	<i>PREMIS. Data Dictionary for Preservation Metadata v 3</i>
Models and standards	Model used to assess your organisation's readiness for managing digital collections.	National Digital Stewardship Alliance	<i>2019 Levels of Digital Preservation</i>
Models and standards	OAIS is a model for describing the processes of a digital archive. The terms AIP (Archival Information Package) and SIP (Submission Information Package) are particularly useful concepts for keeping digital files together during Object entry and moving the DCO within the museum's digital locations.	The Consultative Committee for Space Data Systems	<i>The Open Archival Information System (OAIS)</i>
Models and standards	Model used to assess your organisation's readiness for managing digital collections.	The Digital Preservation Coalition	<i>Rapid Assessment Model (RAM)</i>
Models and standards	PRONOM is a register of recognised file formats produced by TNA and works with DROID.	The National Archives	<i>The Technical Registry PRONOM</i>
Policy	Template for collections development policy.	Collections Trust	<i>Collections Development Policy Template</i>
Policy	Guidance on developing a digital preservation strategy and policy.	The National Archives	<i>Developing a digital preservation strategy and policy</i>
Policy	White paper on digital preservation and why it is needed in museums.	United Nations Educational, Scientific and Cultural Organization (UNESCO)	<i>Charter on the Preservation of Digital Heritage</i>
Training	Free online training run by the Digital Preservation Coalition, available free for anyone working in the GLAM sector.	Digital Preservation Coalition	<i>Novice to Know How - Digital preservation training</i>