Creating digital resources: GDPR, copyright and using open licences

18/01/2023

See all updates

A new toolkit to help heritage projects openly licence digital materials, in line with copyright and privacy rules.

Attachment	Size
PDF View Digital Guide Creative Commons licences A guide to data protection and copyright as PDF(1.95 MB)	1.95 MB
PDF View Trwyddedau Creative Commons: Canllaw i Ddiogelu Data a Hawlfraint as PDF(1.98 MB)	1.98 MB

We are committed to making sure that the work we fund benefits as many people as possible.

It's crucial that our audiences can access and use the digital resources we fund. That's why we ask projects to make sure the images, documents, web pages, code and other digital resources they create are accessible, available and open.

Download the new toolkit, Creative Commons Licences: A Guide to Data Protection and Copyright, from this page under the contents section.

Digital in the heritage sector

Digital is an increasingly essential part of how we preserve, learn about and connect to heritage.

Understanding how copyright and data management rules apply to the resources we put online is especially important. Heritage projects often deal with materials that are still in copyright and involve living people who have legal rights.

We understand that producing some digital resources can be difficult – particularly where resources are created by contractors, volunteers or the public, or feature information about living people.

How we can help

Licensing requirements – which have been in place for over 12 years – were reviewed and updated in 2020. In 2021, we created introductory guidance to help projects better understand copyright rules and how open licences work.

We now have our new practical toolkit, Creative Commons Licences: A Guide to Data Protection and Copyright, available to download from this page, which provides step-by-step support to the sector for open licencing.

Who is this guide for?

This digital guide includes information on data protection and copyright, along with a range of tools, templates, checklists and frequently asked questions to help you take the right steps in open licencing and meeting GDPR

requirements.

It is aimed at The National Lottery Heritage Fund applicants and grantees and provides guidance on the default CC BY 4.0 licence requirements for your project outputs.

Authors

The toolkit has been produced for the Heritage Fund by Naomi Korn Associates as part of the Digital Skills for Heritage initiative.

Expand All accordions

Digital project outputs

Digital heritage outputs created with grants from the Heritage Fund need to be available online and openly licensed under the terms of a Creative Commons Attribution 4.0 International (CC BY 4.0) licence.

Data protection rules mean that digital outputs that include information about living people require specific permissions or approaches before these materials can be shared online or an open licence applied. Copyright necessitates that all rights need to be cleared before content is published online.

This guide provides a summary of the data protection and copyright requirements associated with different types of digital outputs and how these relate to the default CC BY 4.0 licence, to help you better plan your project.

Expand All accordions

Data protection considerations

If you are planning an application to the Heritage Fund to carry out a project, the planned outputs of your project may include images, audio or other information relating to living individuals. Where this material could identity a living individual, then this is 'personal data' and you have several obligations you must fulfil around data protection law.

If you are going to be using personal information in your digital outputs, for example, images, film, audio or written text, you will have to comply with data protection laws.

This guide provides a range of tools, templates and guidance to consider the issues and help you take the right steps. In line with data protection rules, you will need to document your approach and any permissions you collect.

About data protection

Data Protection is an important legal requirement. Getting it wrong could lead to risks to individuals' privacy or safety, your organisation's reputation and can lead to financial penalties (including fines). We live in a data-driven world.

Sharing data can make life easier, more convenient and connected for us all. Data protection law sets out what should be done to make sure everyone's data is used properly and fairly.

Generally speaking, data protection law applies to all workplaces, business ventures, societies, groups, clubs and enterprises of any type. That includes you if you're a sole trader or self-employed, if you work for yourself or if you're an owner or director. It also applies if you only employ a handful of staff or even if you don't employ any staff at all.

Definitions

- **Data Protection Law**: data protection law covers the General Data Protection Regulations (UK GDPR) and Data Protection Act 2018.
- **Data Controller**: an organisation that collects and makes decisions about how personal data will be processed.
- **Data Subject**: the subject of the personal data/the individual which the personal data relates to.
- **Digital Outputs**: content created during the course of the project and arising as a result of funding from the Heritage Fund.
- **Information Commissioners Office (ICO)**: the UK's regulator on data protection law.
- **Explicit Consent**: a very clear and specific statement of consent. Explicit consent must be expressly confirmed in words, rather than by any other positive action.
- **Personal Data**: personal data is information that relates to an identified or identifiable individual. What identifies an individual could be as simple as a name or a number or could include an IP address or other factors.
- **Special Category Data**: in all cases, extra consideration is required for this type of information in data protection law. As greater risk to individuals is involved, so must the technical measures to protect the data against unauthorised access or loss be more robust. Covers data relating to:
    - racial or ethnic origin
    - political opinions
    - religious or philosophical beliefs
    - trade union membership
    - data concerning health
    - data concerning a person's sex life or sexual orientation
    - genetic data or biometric data
- **Criminal Convictions Data**: data about an individual's criminal convictions also requires an additional legal condition to use and these are set out in the Data Protection Act 2018.

All digital outputs created with grant funding to help people access, engage with and learn about heritage need to be available online for at least five years after the end of the project. This includes images, films, audio, documents and data.

Conditions of our grants are given on the basis that digital outputs created with grant funding are made available online, and shared under an open licence, unless specific exceptions apply.

These digital outputs also need to be shared openly with a CC BY 4.0 licence. This means the outputs will be available for others to re-use, re-publish and adapt, as long as they give the correct acknowledgement of the source. The CC BY 4.0 licence does not apply to any personal data included in the output.

Special category personal data

If your outputs include ‘special category’ personal data, the Heritage Fund will provide an exception, which means that you do not have to share these outputs under CC BY 4.0 licence. In the first instance, you should contact your Engagement Manager at the Heritage Fund to discuss this. Typically, this is the case where there is personal information about health, belief or ethnicity.

Personal data classed in the GDPR as ‘special category’ or relating to criminal convictions will require an additional legal basis or condition for processing personal data. Projects which involve this type of data are subject to an exception to the requirement to apply a CC BY 4.0 licence for re-use. If your outputs depict under 18-year-olds, or relate to vulnerable adults, you should also seek an exception from the open licence requirement.

If you believe there are good ethical reasons for not sharing your funded outputs online or under an open licence, you should contact the Heritage Fund.

You will need to ensure that you get data protection ‘right’ in your project by:

- making sure the use of personal information in outputs is fair and lawful
- making sure the people whose personal information is included in the outputs fully understand how their contribution will be used
- present the outputs, if possible, in ways that do not identify individuals
- allowing participants to request a takedown of the information

Further information

- For more details, see the 'Guide 2: special category and criminal convictions data' section on this page.
- A data protection law checklist is also available to download in the toolkit.

Expand All accordions

Copyright considerations

If you are creating content for a Heritage Fund project, one of the conditions is that the outputs will be given a Creative Commons CC BY 4.0 licence. This means that they will be available for others to re-use, re-publish and adapt as long as they give the correct acknowledgement of the source.

At the planning stage of your project, you should assess whether the content you are creating may not be suitable for the licence or other types of sharing. You will need to inform and agree this assessment with the Heritage Fund at the earliest opportunity.

At the beginning of a project, it is crucial that any copyright is identified as early as possible to reduce the risks of infringing any third-party copyright and to ensure that the work can be reused under the terms of a CC BY 4.0 licence.

The steps that you take will depend on:

- **Who is contributing or creating the content**. This might include employees, volunteers, contractors, and members of the public. If content is created by anyone other than employees, then the appropriate steps will be

required to ensure that you have the necessary copyright permissions from them.
- **Whether there is any other content which might be in copyright** and require the necessary permissions to use. There may be possible fees associated with reuse, and these fees should also be identified as early as possible. There may also be copyright exceptions which might apply depending upon your use.

CC BY 4.0 definition

This licence enables the reuse, adaptation and sharing of content for all purposes as long as attribution is provided.

When your project formally begins, you need to ensure that you consider how your copyright obligations will be met and what products or tools you will need to ensure this. Your copyright obligations will depend on who is contributing to your project.

It will be crucial to ensure that you secure copyright permissions that enable you to make content available online and to apply a CC BY 4.0 licence from anyone contributing to the project who is not one of your employees.

Data protection and copyright templates

We have created a range of model templates for collecting the permission you will need from members of the public or other third parties. These are available for you to download from the toolkit and include:

- template permissions forms
- template deed of copyright assignment/licence (for volunteers contributing to your project)
- template separate supplier guide (for when working with contractors)

What do I need to do?

The next steps you need to take are:

- understand your role in the project (see Roles and responsibilities section in this guide)
- use the decision matrix to help you understand which of the templates you will need
- read the relevant Guides to Data Protection and Copyright
- identify which templates your project requires and customise them to your project
- read the FAQ section or seek additional support

Expand All accordions

Does CC BY 4.0 apply to my outputs?

This table summarises what you need to know regarding the sharing of digital outputs.

	Your outputs do not contain any personal data or fully anonymise the data	Your outputs contain data relating to living individuals	Your outputs contain sensitive personal data relating to matters such ethnicity, health, sexuality or relate to children or vulnerable individuals	Your outputs contain data concerning the criminal convictions, allegations or proceedings relating to living individuals
Will be able to give the outputs a CC BY 4.0 copyright licence or apply an exception?	**Yes**, the CC BY 4.0 licence can be added to these outputs	**Yes**, the CC BY 4.0 licence can be added to these outputs	**No**. The Heritage Fund allows an exception from the requirement for outputs with this type of data	**No**. The Heritage Fund allows an exception from the requirement for outputs with this type of data

Expand All accordions

Roles and responsibilities

A project supported by the Heritage Fund may engage a range of participants throughout its lifecycle. This section sets out the data protection responsibilities of each participant and the fundholder/ creator's obligations to them.

It also covers any organisation re-using material available under a CC BY 4.0 licence. There may be some overlap in participants, and they may have a number of data protection responsibilities.

Project role:

Grantee/project lead, or the projects nominated Data controller

Data Protection responsibilities:

- Data Controller for any personal data collected
- ensures all relevant data protection issues have been covered and documentation generated

Fundholder/fund grantee's obligations:

- adequate resources in project plan to protect and manage personal data (Privacy Notice, data minimisation, data security, contractual protections with third parties)

Obligations of organisation re-using materials under a CC BY 4.0 licence:

- correct referencing and attribution
- contact for any data protection queries

Project role:

Member of staff – Senior responsible officer (SRO)

Data Protection responsibilities:

- undertakes available data protection training
- handles personal data in accordance with the law and organisational policy

Fundholder/fund grantee's obligations:

- managing staff data in accordance with the law and organisational policy
- provide a privacy notice, explaining how their data is collected and managed
- see 'Template: Project privacy notice'

Obligations of organisation re-using materials under a CC BY 4.0 licence:

- N/A

Project role:

Contractor

Data Protection responsibilities:

- accepts data protection obligations by signing agreed contractual terms

Fundholder/fund grantee's obligations:

- ensuring formal contracts with data protection clauses are in place

Obligations of organisation re-using materials under a CC BY 4.0 licence:

- permission
- correct referencing and attribution

Project role:

Volunteer

Data Protection responsibilities:

- undertakes available data protection training appropriate to their access to data
- handles personal data in accordance with the law and organisational policy

Fundholder/fund grantee's obligations:

- provide a privacy notice, explaining how their data is collected and managed
- ensures appropriate guidance is given
- manages volunteer personal data in accordance with the law and organisational policy
- see 'Template: Project privacy notice'

Obligations of organisation re-using materials under a CC BY 4.0 licence:

- permission
- correct referencing and attribution

Project role:

Participant (interviewee, subject of an image, appears in a video)

Data Protection responsibilities:

- understands what data is being collected and for what purpose, including copyright and re-use
- signs relevant documentation

Fundholder/fund grantee's obligations:

- privacy Notice
- takedown policy
- manages data in the project in accordance with data protection principles and under a relevant legal basis
- see 'Template: Project privacy notice'

Obligations of organisation re-using materials under a CC BY 4.0 licence:

- permission
- attribution/referencing
- data controller responsibilities: specifically that they manage any personal data in the project in accordance with t he data protection principles and under a relevant legal basis
- organisation may need to provide privacy notice unless exemption applies

Expand All accordions

Guide 1: legal basis

If you are processing any personal data, you need to have a good reason, referred to as lawful basis.

Data protection definition: lawful basis

In data protection law there are six legal bases for processing:

- the individual has consented to the processing
- the processing is necessary for a contract to which the individual is a party
- your organisation has a legal obligation to process the data, perhaps under charity law or the National Heritage Act 1983
- your organisation needs to process data to protect the vital interests of an individual
- if your organisation is a public authority, they need to process data as part of their powers established in law
- your organisation has a legitimate interest in processing the data, balanced against the rights and freedoms of the individual

Key point: The legal basis under which you process personal data should be set out in your organisation's overarching privacy notice.

In the context of making content available online under a CC BY 4.0 licence, the following legal bases are the most suitable.

Consent

The ICO states that "genuine consent should put individuals in charge, build trust and engagement, and enhance your reputation." To make sure that consent is valid, it needs to be:

- **a clear affirmative action**: an "opt-in" rather than "opt-out"
- **fully informed**: people need to know what they are opting into, who will be storing their data and how
- **freely given**: there should be no power imbalance or implied pressure to provide the consent. The consent should be as easy to retract as it is to provide
- **must be recorded**: the organisation should retain a record of the consent

Legal basis for personal data subject to CC BY 4.0

UK GDPR Article 6 (1) (a) Consent is the most appropriate legal basis in our scenario but it will still be challenging to use. You can brief participants fully on the copyright arrangements and many will be 'on board' with the objectives of your project and the principles of open access to collections.

However, you must ensure that individuals understand how their data might be re-used beyond the boundaries of the current project. Additionally, individuals might feel compelled or obliged to give their consent to the project, which would undermine the validity of consent.

A template project consent form is available in the toolkit to download.

Necessary for a task in the public interest

If the fundholder is a public authority under Schedule 1 of the Freedom of Information Act, they can rely on UK GDPR Article 6 (1) (e), where 'processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller'.

For galleries, libraries and museums that are public authorities, creating, maintaining and providing access to the cultural resources in its collections will be fundamental to their public mission.

Legal basis for personal data subject to the terms of a CC BY 4.0 licence

Where the cultural objectives of your organisation and the Heritage Fund are met by making the material available, and obtaining valid consent is not possible, the legal basis of task in the public interest could be used.

As with legitimate interests – explained below, this is a flexible legal basis but still requires fair and lawful use of personal data. The public task need to be valid for the authority and the 'necessity' must be demonstrable.

Legitimate interests

One of the available legal bases for processing personal data in this scenario, where obtaining valid consent is not possible, is UK GDPR Article 6 (1) (f). This is where 'processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data'.

The legitimate interests of your organisation, such as promoting its collections or encouraging donations, always needs to be balanced against the rights and freedoms of the individuals. The less privacy intrusive the photo or video, the more the balance favours the legitimate interest.

Legitimate Interests as a legal basis for personal data subject to CC BY 4.0

This is a flexible legal basis but always relies on the balance between the interest and the rights and freedoms of the individuals whose data is at issue. As an organisation, you can work out and document the balance in a Legitimate Interests Assessment.

ICO Guidance

Safeguards around the use and presentation of data, allied with pro-active management of 'takedown requests' or GDPR rights requests are a key part of this legal basis.

For further information on legitimate interests as a lawful basis, visit the ICO website.

Expand All accordions

Guide 2: special category and criminal convictions data

Special category data definition

'Special category data' covers data relating to:

- racial or ethnic origin
- political opinions

- religious or philosophical beliefs
- trade union membership
- data concerning health
- data concerning a person’s sex life or sexual orientation
- genetic data or biometric data

In all cases, extra consideration is required for this type of information in data protection law. As greater risk to individuals is involved, so must the technical measures to protect the data against unauthorised access or loss be more robust.

Criminal convictions data definition

Data about an individual’s criminal convictions also requires an additional legal condition to use and these are set out in the Data
Protection Act 2018.

Additional legal bases

As befits data with a higher risk, an additional legal basis needs to be relied upon to justify the processing of ‘special category data’ and data relating to criminal convictions.

There are a range of options in the GDPR, but the following are most likely to arise for cultural and heritage organisations:

- the individual has provided explicit consent for what you will do with the data
- the use of the data is necessary for carrying out your statutory obligations (such as those under health and safety, equality or employment law)
- the data may have clearly already been made public by the individual (such as the political affiliation of an MP or the criminal record of a former prisoner turned public activist)
- the use of the data may have a statutory basis (for example, where a museum may be a public authority)
- the use of the data is necessary for archiving purposes, scientific or historical research purposes or statistical purposes, whilst safeguarding the rights of the individuals involved

Special category data, criminal convictions and copyright

Special category data will not be suitable for re-use under the CC BY 4.0 licence. A fund recipient should apply for an exception from the CC BY 4.0 licence requirement.

- For further information, see the 'Guide 5: securing an exception to the default licence requirement' section on this page.

Expand All accordions

Guide 3: keeping it minimal and relevant

This section provides an overview of how to collect personal data which is minimal and relevant. The third data protection principle is that personal data should be ‘adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. This is usually called the ‘data minimisation’ principle.

Adding personal data to project content needs careful consideration and organisations must avoid collecting or publishing more than is necessary, which could impact on the privacy of the individual.

Data protection example: data minimisation

The London Lute Museum is working on captions for its promotional photos for its latest funded project. The photographer initially writes: ‘One of our donors John with Seema (his wife) and Rachel from the collections team at the reception’ but redrafts as ‘Attendees at our reception’. Provision of the names would be excessive for the purpose of publishing the image.

The UK GDPR defines a number of specific approaches to protect privacy in the use of personal data. These can be adapted for project content in the following ways.

Pseudonymisation

‘Pseudonymisation’ in GDPR terms means presenting the personal data in such a manner that the personal data can no longer be linked to a specific person without the use of additional information. That additional information is kept separately and is subject to technical and organisational measures to ensure that the person is not identified. Pseudonymised data is still personal data and requires the data protection principles to be observed and a legal basis to process.

Data protection example: pseudonymisation

The London Lute Museum is publishing a range of written and audio feedback from its recent exhibition. The interviews are attributed to
coded identities, presented as “B, London” and “J, Manchester”. In its secure repository, the Museum holds the raw data with the full identity of “B, London” and other contributors, including the records of their involvement in the project, such as a signed release form and outtakes.

Anonymisation

‘Anonymisation’ in GDPR terms means managing the data in such a manner that it no longer becomes possible to link the data back to the individual and therefore ceases to be personal data and in the scope of GDPR.

Data protection example: anonymisation

The London Lute Museum has reached a year since it published the written and audio feedback from its recent exhibition. As agreed with the participants, the Museum deletes from its secure repository the raw data with the full identity of “B, London” and the records of their involvement in the project, such as a signed release form and outtakes. Any audio or written content that might contain information that would identify an individual (“I came to the exhibition because I work as a luthier at Joe’s Guitars on Denmark Street”) are edited or removed from the available content. The

Museum cannot now link the data back to any of the participants.

The benefits of anonymisation and pseudonymisation

The benefits or anonymisation and pseudonymisation for cultural content can be summarised as follows:

- reduces risk and impact in the event of a data breach or other unauthorised access
- mitigates reputational risk for organisations publishing content
- helps enable re-use of data for archiving and research

Expand All accordions

Guide 4: withdrawal of consent or participation

Engaging with project participants in a fair, transparent and lawful way is essential in complying with data protection law as well as ensuring an overall ethical approach. Dealing with the possibility of a participant wishing to remove data about them or retract their consent should be the part of any project from the planning stage onwards.

Data subject rights

Individuals have several rights under data protection law to address how their personal data is processed. These rights have specific relevance for personal information made available for public access and re-use and your organisation needs to be able to identify these rights requests and act on them, in most cases, within 30 days.

Data subject rights under data protection law include:

- **Right to be informed**. An individual should be provided a Privacy Notice informing them how data will be used.
- **Right of access** (or “Subject Access Request”, “SAR” or “DSAR”). An individual has the right to receive a copy of their personal information that your organisation holds about them and information about how you use it.
- **Right to rectification**. An individual has a right to ask your organisation to correct their personal information where it is incorrect or incomplete.
- **Right to erasure** (or “right to be forgotten”). An individual has the right to ask that their personal information be deleted in certain circumstances, such as where consent has been withdrawn, where it is no longer necessary to keep it or where it legally needs to be deleted.
- **Right to restrict processing**. An individual can restrict their data being used in certain circumstances.
- **Right to object**. An individual has the right to object to your organisation’s processing of their personal data unless you can prove legitimate interests.
- **Right to data portability**. An individual can request to transfer data to another organisation.
- **Rights in relation to automated decision making and profiling**.

Lawful bases

Whether these rights apply depends on the legal basis under which you are processing the data.

Legal or contractual obligation

In managing the project there will be a range of personal data where your organisation will have a legal or contractual obligation to retain
data and any requests for withdrawal can be refused.

Consent

If you are relying on consent as your legal basis for using data in your project, there are a few elements needed to make that consent valid. The consent needs to be:

- a clear affirmative action: an “opt-in” rather than “opt-out”
- fully informed: people need to know what they are opting into, who will be storing their data and how
- freely given: there should be no power imbalance or implied pressure to provide the consent
- must be recorded: the organisation should retain a record of the consent‘

A key element of valid consent is that the consent must be as easy to retract as it is to provide. The ICO states that “genuine consent should put individuals in charge, build trust and engagement, and enhance your reputation.”

Data protection example: invalid consent

A cathedral project staff member is approaching visitors to the cathedral on a Saturday to obtain their views on a religious figure. The member of staff conducting the survey says that everyone will be interviewed and that their name, where they travelled from and why they came will be added to the project content.

He states that if they don’t want to be included, they can opt-out at the front desk by asking to arrange a meeting for the manager who is only in on weekdays. Everyone who has been coming to the museum has been doing this, he says, as he completes the interviews and leaves, preparing to add them to the document repository.

Data protection example: valid consent

The cathedral promotes its project on its website and social media accounts asking prospective participants to attend on a particular
Saturday, where it will conduct interviews. It includes the consent form and privacy notice, explaining the project and how the data will be used, on its website.

The interviewer gives each attendee who turns up on the Saturday a fact sheet explaining how the data will be used and a form to sign consenting for the information to be used. They are also available to answer any questions from participants about the project. The fact sheet includes information on how to ask for the details to be removed, which can be done with an email to the Project Team or direct message to the cathedral’s Facebook page.

The Project Staff Member keeps the signed forms, and the museum stores them for the duration of the project, removing any entries from the page if the participants notify them in the interim.

Consent under data protection vs consent for participation

Obtaining consent from the participants or subjects of research is a long-established benchmark of ethical research practice. This type of
consent, whilst containing a few similar elements, does not necessarily translate into an equivalent for valid GDPR consent.

A consent form may still be a vital part of your project documentation, but it may have to reference a different legal basis for processing personal data.

Requesting removal under other legal bases

If you are processing personal data under a different legal basis, the withdrawal of agreement to involvement must be considered
differently.

Legitimate interest

There are rights in data protection law for individuals to ask for an organisation to stop processing data or ask for it to be removed. If you are relying on legitimate interests as a legal basis, you will have to balance those legitimate interests against the rights and freedoms of the individual concerned.

In a typical Heritage Fund project scenario, an opportunity to withdraw involvement whilst the project is in progress would be seen as a reasonable safeguard to balance the legal basis.

For guidance, visit the ICO website.

‘Public Task’

If your organisation is a heritage body which is also a public authority, and you are using ‘public task’ as your legal basis, then the individual’s right to erasure does not apply under data protection law. The right to object to the processing, however, does still apply. A heritage organisation would have difficulty demonstrating there were no other reasonable and less intrusive means to achieve their purpose if they could not facilitate a reasonable process to remove or withdraw content both during and after the duration of the project.

The British Library’s ‘takedown policy’ is a useful example of this.

Dealing with requests for removal

Removal during the project

A participant should, at any stage during the project, be given an opportunity to withdraw their involvement in any of the outputs. At this stage, the organisation should, in most cases, fulfil the participant’s request.

This is covered in the template project consent form provided as part of this resource.

Data protection example: take down during the project

After a painting workshop has been completed and interviews concluded, the project leader asks all the participants whether they are still happy to allow their contributions to be published as part of the project. One participant changes their mind, and their contribution is removed from the final collection.

After the project is completed

When the project is completed and the outputs have been produced and published, in either digital or hard copy, the withdrawal of consent or agreement and removal of content is, in practical terms, more difficult. An organisation should consider implementing a ‘takedown policy’ which considers these types of requests. These can be made available to participants at the start of the project to give a fuller understanding of what control they have over their data. An example is available on the British Library website.

Data protection example: take down after the project is completed

One of the participants of a project contacts the museum and asks for their interview clip and information to be removed from any available outputs of the project. The Museum agrees to take down the clip and content from the website but cannot remove the information from the initial run of published booklets that have already been published.

Archiving in the public interest

There is an exemption from the right to erasure, to object and to restrict processing where you need to retain personal data for the purposes of ‘archiving in the public interest’. This will be relevant to many Heritage Fund projects, where content may have been made permanently available. The exemption is qualified and only applies where:

- removing the information would ‘seriously impair’ the purposes, e.g., mean that the cultural resource was no longer accessible
- there are appropriate safeguards in regard to the data being archived, e.g., you have carried out data minimisation, any sensitive information has been redacted or subject to a Heritage Fund exception and you have a reasonable takedown policy or approach
- keeping the information available would cause damage and distress
- the content is not used in relation to specific decisions or interventions about the individual concerned

These safeguards should all be part of any plan to produce Heritage Fund project content.

Data protection example: archiving in the public interest

A participant in a live event has asked that all images and footage in which she is included are removed from the project outputs under the ‘right to erasure’. The museum argues that the content was designed not to be privacy intrusive (it is a group event and names or close up images of faces were not used) and that removing these photos would be detrimental to the quality of the project outputs and, therefore, the public interest of the archiving. The Museum considers that it is exempt from carrying out the right to erasure request.

Withdrawal requests when content is re-used

Where there is a CC BY 4.0 licence in place, content containing personal data could be re-used by a person or organisation unrelated to the original fundholder or the objectives of their project. The re-use of content does not exist outside of data protection law and those re-using content will have the obligations of other data controllers. They may

have to comply with rights requests under data protection law and may have to rely on exemptions available to re-use in research or artistic context. The original fundholder's responsibility is to inform participants at the start of a project about the implications of re-use. At the stage of re-use, they may be subject to a takedown or rights request to prevent any subsequent re-use.

Expand All accordions

Guide 5: securing an exception to the default licence requirement

If you are creating content for a Heritage Fund project, one of the conditions is that the outputs will be given a Creative Commons CC BY 4.0 licence, where they will available for others to re-use, re-publish and adapt as long as they give the correct acknowledgement of the source.

At the planning stage of your project, you should assess whether the content you are creating may not be suitable for the licence or other types of sharing. You will need to inform and agree this assessment with the Heritage Fund at the earliest opportunity.

What material should be subject to an exception?

Examples of materials that may not be appropriate for open licensing for ethical reasons include:

- material depicting children and young people under 18
- material depicting or created by vulnerable adults
- artefacts, knowledge or memories of cultural significance to the communities of origin
- ancestral remains, spiritual works or funerary objects

In some cases, research, data or other media produced around the above examples may also not be appropriate for open licensing.

Data protection example:

The Town Museum is creating a project where elderly residents who moved to the town from Ireland in the 1950s and 1960s talk about their experiences of work, leisure and prejudice. Because the personal data revealed in the content will reference the ethnicity of the participants, this output will be subject to a Heritage Fund exception from the CC BY 4.0 licence requirement.

Special category data qualifies for an exception to the CC BY 4.0 licence requirement, and covers:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- data concerning health
- data concerning a person's sex life or sexual orientation
- genetic data or biometric data

Criminal convictions

Where a project collects personal data relating to criminal convictions and offences or related security measures, then this data will also qualify for an exception to the copyright licence.

Example: criminal convictions data in a project

The City Art Gallery is scoping a project where prisoners and ex-prisoners are holding art workshops on the theme of rehabilitation. One of the planned outputs is interviews with the participants, which will include a range of biographical information about their convictions and personal lives. This output will be subject to a Heritage Fund exception from the CC BY 4.0 licence requirement. Other outputs may still be suitable.

Data minimisation

Even where an exception is agreed, an organisation needs to carefully assess what data is being collected as part of a project and must avoid collecting or publishing more than is necessary, which could impact on the privacy of the individual.

Data management in the case of an exception

If content in a project is still subject to an exception from a CC BY 4.0 licence, the organisation still has legal responsibilities around the data it is processing.

Data security

The organisation is required to have ‘appropriate technical measures’ in place to protect the personal data it processes from unauthorised access or loss. Websites should have robust security protections such as firewalls, penetration testing and up- to-date software. Staff who are accessing personal data should be trained in data protection and IT security principles. Data collected should be stored and transferred securely.

Example: secure transfer

The Forest Friends Association sends a transcript of its interviews to the participants for them to approve as an accurate record. The Association ensures that the transcripts are sent via email using password protection, with the password provided separately to the recipient.

Data Protection Impact Assessment (DPIA)

Where you are collecting high risk data, a ‘Data Protection Impact Assessment (DPIA)’ is a useful tool. A DPIA maps out the data processing in a project and identify risks that you can prepare for and manage. There is a range of guidance on the Information Commissioner’s website on undertaking a DPIA.

Long term storage

After the project is completed, you may wish to add your data to your permanent collection or deposit it in a formal archive. Some of the data may be subject to an embargo before it is made available to researchers.

Any third parties wishing to use the data for research purposes will be responsible for their processing of the data.

Expand All accordions

Templates and checklists

The full toolkit, which is available to download from this page under contents, contains a series of templates to help you get started on your project's data protection documentation:

- Template 1: Project privacy notice
- Template 2: Project content form
- Template 3: Notice for re-use under a CC BY 4.0 licence
- Template 4: Copyright permissions form
- Template 5: Copyright deed of assignment/licence (volunteers)

Seek support from your Data Protection Officer if you have one.

In addition to the templates, the resource includes checklists to help you meet the open licencing requirements in line with data protection:

- Checklist: Does data protection law apply to my project's digital outputs?
- Checklist: My Heritage Fund project data protection

Expand All accordions

Frequently asked questions

The toolkit includes frequently asked questions on how you can make sure your project complies with data protection law.

Each question's answer includes links to guides and templates in the toolkit to help you navigate to the relevant area of support.

To read all of the questions and answers and access the guides and templates, download the document from this page.