Data Protection for Community Archives

2026

Community Archives and Heritage Group

Data Protection Handbook

Introduction

All groups that are collecting information about members, volunteers, donors to their collection and those that may have items in their collection that contain personal information about an individual who may still be alive will need to consider data protection.

It is important to understand what you should and should not be doing when managing personal data your group is responsible for.

Data Protection law in the UK

The **Data Protection Act 2018** with its associated secondary legislation and the **General Data Protection Regulation (GDPR)**, together referred to in this handbook as Data Protection law, came into force from May 2018. Since leaving the EU the UK Government has transposed the provisions of the EU GDPR into the UK GDPR. The UK GDPR has been amended further by the **Data (Use and Access) Act 2025**.

Data Protection law applies to personal information held about living, or potentially living, individuals. Your group may well be deemed a Data Controller under the law for information you collect and hold about people – either in your administrative records or in your collections themselves.

Key terms in Data Protection

- **Personal Data**: any information relating to an identified or identifiable living individual.

- **Data Controller**: the person/organisation/body who determines the purposes for which and the way in which any personal data are processed.

- **Data Subject**: the individual the personal data is about.

- **Processing**: Collecting, recording, organising, structuring, storing, adapting, altering, retrieving, consulting, using, disclosing by transmission, dissemination or making available, combining, restricting, erasing or destroying.

- **Data Processor**: any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

- **Special Category (formerly 'Sensitive') Personal Data**: Information about someone's race or ethnic origin, political opinions, religious/philosophical beliefs, physical or mental health, sexual life, membership of a Trade Union, alleged criminal offences and, under GDPR, biometric and genetic data.

THE WEBSITE OF THE INFORMATION COMMISSIONER'S OFFICE (ICO) IS A KEY SOURCE OF GUIDANCE FOR UNDERSTANDING RESPONSIBILITIES UNDER DATA PROTECTION LAW
https://ico.org.uk/for-organisations/advice-for-small-organisations/

Unstructured manual records

Data protection law only applies to personal data found in unstructured manual records if it is being processed by a public authority that is subject to the Freedom of Information Act 2000. It is possible, therefore, that paper or analogue records held by a community archive group that are not indexed or part of a filing system may not be subject to data protection law.

However, if collections containing unstructured manual records are processed by digitisation or by indexing or cataloguing them, it may bring them in scope of the law[1].

[1] See the National Archives' Guide to Archiving Personal Data, section 32-33: https://cdn.nationalarchives.gov.uk/documents/information-management/guide-to-archiving-personal-data.pdf

The Data Protection Principles

The previous Data Protection Act 1998 was underpinned by 8 Data Protection principles. Under GDPR there are now 7 Data Protection Principles BUT nothing has disappeared or been taken out – in fact some areas have been strengthened, and a new principle of Accountability has been added.

The table below compares the old and new principles side by side. In GDPR the principles are laid out in Article 5(1) (a-f) and Article 5(2). Data Subject Rights and International Transfers of data have been given separate chapters under GDPR, so even though they aren't covered in a list of the principles, they are still part of managing personal data lawfully.

The principles lie at the heart of data protection law. They are set out right at the start of the legislation and inform everything that follows. They don't give hard and fast rules but rather embody the spirit of the general data protection regime - and as such there are very limited exceptions.

Compliance with the spirit of these key principles is therefore a fundamental building block for good data protection practice. It is also key to your compliance with the detailed provisions UK data protection law.

Failure to comply with the principles may leave you open to substantial fines. Article 83(5)(a) states that infringements of the basic principles for processing personal data are subject to the highest tier of administrative fines. This could mean a considerable fine, especially for larger organisations.

	Data Protection Act, 1998 Principles	**General Data Protection Regulation Principles**
Lawfulness	1 Personal data shall be processed fairly and lawfully and according to conditions (described in Schedules 2 & 3 of the Act)	a) Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject. *(lawfulness, fairness & transparency)*
Purpose	2 Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.	b) Personal data shall be collected (whether from the data subject or otherwise) for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. *(purpose limitation)*

Data Minimisation	3 Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.	c) Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. *(data minimisation)*
Accuracy	4 Personal data shall be accurate and, where necessary, kept up to date.	d) Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay. *(accuracy)*
Storage	5 Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes	e) Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. *(storage limitation)*
Access	6 Personal data shall be processed in accordance with the rights of data subjects.	The GDPR does not have an equivalent principle. Instead access rights are found separately in Chapter III of UK GDPR and in Part 3, Chapter 3 of the DP Act 2018. Subject rights have been strengthened.

Security	7 Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data	f) Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. *(integrity and security)*
Overseas transfer	8 Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data	The GDPR does not have an equivalent principle. Instead, overseas transfers of personal data are addressed separately in Chapter V, but there should still be no transfers outside of the EEA unless that 'third country' has been deemed to have adequacy in relation to data protection. Similar provisions now apply in the UK – which currently has been deemed to have adequacy.
Accountability	The 1998 Act does not have an equivalent principle.	Art 5 (2) The controller shall be responsible for, and be able to demonstrate, compliance with the principles. *(accountability)*

Special Category Personal Data

Data Protection legislation particularly serves to protect the disclosure of very sensitive personal information. Under GDPR this is now called 'special category' personal data and new types of personal data have been included. This includes data that gives the following details about a person:

- Their racial or ethnic origin
- Their political opinions
- Their religious (or similar) beliefs
- Their physical or mental health
- Their sexual life
- Their membership of a Trade Union
- Their alleged criminal offences and the court proceedings for any (alleged) offences
- Their genetic or biometric data (new under GDPR)

This means that records containing sensitive personal information **must not** be made available to the general public during a period of time that would allow for an individual mentioned in them to still be alive. It is usual to assume a 100-year lifespan. It is possible that records containing other sorts of personal data should also be restricted from public access.

Guidance from the ICO

Make sure that you have read the guidance from the ICO about your responsibilities under Data Protection law. You will find it on their website at

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

The detailed advice covers the principles and what's expected, along with a checklist for you to follow at

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/

They have also recently added pages specifically aimed at smaller organisations, which contain simplified guidance that will help you with compliance:

https://ico.org.uk/for-organisations/advice-for-small-organisations/

Lawful basis

The detailed guidance explains the different types of lawful basis for processing. It's important to remember that 'consent' is only one of the types of lawful basis. There are six available lawful bases for processing[2]:

- **Consent** – this must be clear, specific, explicit and opt-in if you choose to use it.
- **Contract** – you can use this if you need to process someone's personal data to deliver a contractual service to them or because they have asked you to do something for them before entering into a contract (like provide a quote).
- **Legal Obligation** – you can use this if you need to process someone's personal data to comply with a common law or statutory obligation.
- **Vital Interests** – you are likely to be able to rely on vital interests as your lawful basis if you need to process the personal data to protect someone's life.
- **Public Task** – you can rely on this lawful basis if you need to process personal data: 'in the exercise of official authority' or to perform a specific task in the public interest that is set out in law.
- **Legitimate Interests** – this can be the most flexible lawful basis, but you cannot assume it will always be the most appropriate. You have to show that the processing is necessary to achieve the legitimate interest AND that you have balanced it against the individual's interests, rights and freedoms.

The Rights of Data Subjects

The GDPR provides the following rights for individuals:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

You will find detailed guidance on these rights on the ICO website at

https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/

Some of the guidance is in the process of being updated following the passing of the Data (Use and Access) Act 2025.

[2] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/

It is possible that any personal data in your archive collections may be partially exempt from these rights where you are carrying out processing for **Archiving Purposes In The Public Interest**, providing you have appropriate safeguards in place.

Individuals' Right of Access

Individuals **do** have a right of access to personal information about themselves that you may hold as an organisation. Under current legislation you have 1 month to respond the Subject Access Requests and can no longer charge a fee for carrying them out.

Where personal data is being held for archiving purposes in the public interest it may be exempt from the right of access (but it is good practice to support people in accessing their own information where you can).

Your search for personal data for a data subject need only be reasonable and proportionate, so you may need to ask them for further information to help guide or limit the search for their information.

To determine whether searches may be unreasonable or disproportionate, you **should** consider:

- the circumstances of the request;
- the volume of information you may need to search in order to respond;
- any difficulties involved in finding the information; and
- the fundamental nature of the right of access.

You **must** be able to show why a search is unreasonable or disproportionate.

Accountability and Governance

The principle of accountability makes you not only responsible for complying with data protection law but ensuring you are able to demonstrate your compliance.

You will need to make sure you have policies and procedures in place to describe how you are managing personal data properly and you will need to make sure everyone in your group is aware of them and follows them.

Make sure you read the guidance on the ICO website and consider what documentation you need to have in your group. This might include a Data Protection Policy, Privacy Notices that explain what you do with particular types of personal data and information on how you manage requests for access. You will also need to have clear procedures for what to do if something goes wrong.

Make sure you produce a list of documents your group needs and keep them up to date.

Article 84 – processing for Archiving Purposes in the Public Interest

- The UK GDPR has specific reference to processing personal data for historical/scientific research, for archiving purposes in the public interest (APIPI), or for statistical purposes (together these are known as RAS purposes).

- This modifies the limitation principles that would otherwise have prevented the continued processing of personal data that wasn't original created and collected 'to be an archive' and is no longer required for its original purpose.

- You still need to 'safeguard the rights and freedoms of individuals' – this may include restricting items in your collections from open public access during the data subject's potential lifetime.

- Where you are processing personal data for APIPI you may be exempt from some GDPR provisions (including some of those data subject rights).

The exemption can apply if you process personal data for archiving purposes in the public interest.

It exempts you from the GDPR's provisions on:

- the right of access;
- the right to rectification;
- the right to restrict processing;
- the obligation to notify others regarding rectification, erasure or restriction;
- the right to data portability; and
- the right to object.

The GDPR also provides exceptions from its provisions on the right to be informed (for indirectly collected data) and the right to erasure.

But the exemption and the exceptions only apply if the processing is subject to appropriate safeguards for individuals' rights and freedoms, which are now laid out in Article 84c of the UK GDPR.

The requirements for RAS processing (including APIPI) are not met

- if the processing is likely to cause substantial damage or substantial distress to a living individual; and

- if the processing is used for measures or decisions about particular individuals, except for approved medical research.

- In addition, safeguards must include technical and organisational measures to respect the principle of data minimisation.

Data protection law applies to the personal data of living (or potentially living) individuals, so you may need to make some assumptions when considering the age of the records you are caring for and the possible age of people mentioned in them. We generally **assume a possible lifespan of 100 years** when we have no other information available.

If there is no information in the records about the age of an adult mentioned in them – **assume an age of 16 at the time the record was created.**

If there is no mention of the age of a child in the records made about them **assume they were less than 1 year old** at the time the record was created.

If you know for certain that an individual is more than 100 years old and still alive then you will need to comply with data protection law if you hold information about them.

Guidance is available

The National Archives has produced a detailed guide on Archiving Personal Data in line with the new legislation. It is important that you read it and understand how it affects records in your collections[3].
https://www.nationalarchives.gov.uk/documents/information-management/guide-to-archiving-personal-data.pdf
This gives guidance on approaches to managing the collection, cataloguing, making accessible and possibly restricting access to archival material that holds personal data.

The Archives & Records Association (ARA) have recently published new guidance on Generally Recognised Standards for Archiving in the Public Interest

ARA+Generally+Recognised+Standards+25.3.26+FINAL.pdf

This is intended to help archives of all sizes and types to demonstrate that the work they are doing meets the standards for APIPI. It provides detailed guidance on meeting the standards and a checklist for compliance to help archives decide what policies, procedures and documentation they need to have in place. It is particularly useful for community archive groups, charities, business or school archives who may not be able to rely on public task (like a council or national archive service).

Data Protection Toolkit
The National Archives have also developed a Data Protection Toolkit to help archives dealing with data protection requests and issues arising from their collections. Anyone can request access to the Toolkit, which is designed as a self-directed training tool that presents scenarios and helps you work out the answer to questions you may have to consider in relation to data protection.

The toolkit presents a simplified overview of the statutory, regulatory, ethical and policy essentials in the context of access to information in archives. It then explores how these might apply in a series of 10 case studies. There are 4 sections in total which build on each other, allowing the user to move through each stage, gaining in understanding and confidence. It is also possible to use the toolkit as a quick reference resource. Throughout the toolkit, you will be able to direct your own learning, take quizzes and reflect on what you have learned.

You can sign up for a new account on Moodle to access the Toolkit here:

https://elearning.nationalarchives.gov.uk/login/signup.php

Following the link provided above, please fill out the New Account form with your details. Please enter your email address as your username and use the enrolment key: 'Data Protection Toolkit'. Once you have registered, you will receive an automatic confirmation email from Moodle.
It is very much recommended.

[3] NB – This guidance predates the changes made to UK GDPR following the enactment of provisions in the Data (Use & Access) Act 2025, so some references to parts of legislation may need updating.

Useful Further Reading

Legislation

Current UK Legislation can be viewed online in full at http://www.legislation.gov.uk

The Data Protection Act, 2018 –
https://www.legislation.gov.uk/ukpga/2018/12/contents

You can find the text of the EU GDPR with UK amendments here:
https://www.legislation.gov.uk/eur/2016/679/contents

The Data (Use and Access) Act 2025 can be found here –
https://www.legislation.gov.uk/ukpga/2025/18/contents?section-77-2-a-ii

Data protection resources

One of the most useful resources for information on Data Protection legislation is the website of the Information Commissioner's Office. They are the Regulator responsible for enforcing it.

Here you will find their Plain English Guide to the (current) Data Protection Act for organisations:
https://ico.org.uk/for-organisations/

They have also created new, simplified, guidance aimed specifically at smaller organisations:
https://ico.org.uk/for-organisations/advice-for-small-organisations/

Their detailed guidance to the GDPR can be found here:
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/

The ICO's guidance on 'Information in the Public Domain'. While this guidance is aimed at organisations answering enquiries under the Freedom of Information Act 2000, it does give some good examples of when personal data might, or might not, be considered to already be in the public domain. –
https://ico.org.uk/for-organisations/foi/freedom-of-information-and-environmental-information-regulations/information-in-the-public-domain/

The ICO is currently updating its guidance on RAS (Research, Archiving and Statistics provisions):
https://ico.org.uk/for-organisations/research-archiving-and-statistics-provisions/

The National Archives guidance on archives and data protection law in the UK can be found here:
https://www.nationalarchives.gov.uk/archives-sector/legislation/archives-data-protection-law-uk/

Their Guide to Archiving Personal Data can be found here:
https://cdn.nationalarchives.gov.uk/documents/information-management/guide-to-archiving-personal-data.pdf

The new ARA guidelines on generally recognised standards for Archiving in the Public Interest can be found at
https://www.archives.org.uk/generally-recognised-standards

The link to request access to the TNA e-learning platform and Data Protection Toolkit can be found here:
https://elearning.nationalarchives.gov.uk/login/signup.php

You sign up using enrolment key 'Data Protection Toolkit' and then you can log in through the TNA e-learning site at https://elearning.nationalarchives.gov.uk/login/index.php

The Community Archives and Heritage Group (CAHG) has a resource page on Community Archives and GDPR:
https://www.communityarchives.org.uk/content/resource/community-archives-gdpr

Miss IG Geek's blog post about what GDPR says about 'consent' for data processing
http://missinfogeek.net/gdpr-consent/

Some Data Protection case studies to look at

Samaritans' Radar app –
Note: Just because personal data *appears* to be 'in the public domain' it does NOT mean you can *process* it. Do the wrong thing and you can lose trust, face the regulator and place your organisation at risk.
https://en.wikipedia.org/wiki/Samaritans_Radar

The Consulting Association case –
Where information about Trade Union activities and membership was used to harm people working in the construction industry.
https://en.wikipedia.org/wiki/Consulting_Association

A case study – Ethics, the historian and digitisation –
https://medium.com/on-archivy/on-april-at-the-organization-of-american-historians-i-participated-in-a-roundtable-discussion-563213dc94a
Digitisation – Just because you can, doesn't mean you should – Reveal Digital and On Our Backs
http://tararobertson.ca/2016/oob/

An example of an Access Policy from an archive service describing where access may currently be restricted for various reasons (including data protection – FOIA s.40)
https://www.wyjs.org.uk/media/197087/access_to_records_policy_2023_v17.pdf

ICO Decision Notices relating to archives

A West Yorkshire Archive Service ICO decision notice – where it was decided NOT to provide access to a record because of Data Protection –
https://ico.org.uk/media2/migrated/decision-notices/684728/fs_50416747.pdf

The Powys Archives ICO decision notice – which gives the ICOs opinion on (not!) providing access to school admission registers and confirms that the information in them is covered by data protection law –
https://ico.org.uk/media2/migrated/decision-notices/607040/fs_50314844.pdf

FS50536204 – East Riding of Yorkshire Council
https://ico.org.uk/media2/migrated/decision-notices/1023986/fs_50536204.pdf
This Decision Notice is important because it upholds the Powys Archives DN restricting access to school admission registers for 100 years. It also makes it clear that, as far as the ICO are concerned, it would be unreasonable to expect an archive service to carry out lots of research to establish definitively whether people mentioned in records less than 100 years old and restricted under the s.40 exemption (data protection) are either living or dead. It's enough for us to restrict access on the assumption that they could be still living.

You can search the ICO Decision Notices database for archive and data protection related decisions here:
https://ico.org.uk/action-weve-taken/decision-notices/

You can put 'archive' in as a keyword search term to find archive services and narrow the search to the topic of data protection by selecting the right section of the act the DN relates to.
The section of the Freedom of Information Act that exempts information because of data protection is s.40.