

Personal data and the Library's collections

User guidance

22 October 2018

I. About this document

I. About this document	2
II. Personal data and the Library's collections	3
III. About data protection	4
The legislation	4
Data protection principles.....	4
Lawfulness of processing.....	5
Special categories of personal data.....	5
IV. Using personal data from the collections.....	6
Personal use	6
Research use.....	6
Journalistic, academic, artistic and literary uses.....	7
Anonymisation and pseudonymisation.....	8
V. Glossary of terms.....	9
Data Controller.....	9
Data Processor.....	9
Data Subject.....	9
Personal Data	9
Processing.....	9
Special Categories of Personal Data.....	9
VI. Links to further information.....	10
VII. Contact	10

Data protection and privacy are complex, detailed, and sensitive areas of law and practice. This document is not comprehensive and focuses on data protection and the use of collections held by the National Library of Scotland. If you require more information see Section VI 'Links to further information', speak with a member of staff, or use the contact details in Section VII 'Contact'.

Information provided by the National Library of Scotland is not intended as, and should not be construed as, legal advice. If you need legal advice please consult a legal professional.

II. Personal data and the Library's collections

The National Library of Scotland collects, preserves and provides access to a range of published and unpublished works. We undertake these activities in the course of our public functions.

Works in our collections may contain personal data. We collect, store and process personal data in accordance with data protection legislation and our published privacy information, which is available from www.nls.uk/privacy or a member of staff.

The Library is normally the data controller of personal data held in our collections. Sometimes, we may be a data processor (for example, when material is owned by a third party) or a joint data controller (for example, when we own material jointly with a third party).

We often provide access to personal data held in our collections to our users and members of the public in the course of our public functions.

You will become the data controller in respect of any personal data you use or otherwise process from materials held in the Library's collections.

This means you, and not the Library, will be responsible for ensuring that your use of personal data is lawful.

See Section IV 'Using personal data from the collections' for more information.

III. About data protection

Data protection rules have wide application. This is because of the broad definitions of two key terms – personal data and processing.

When personal data is processed, data protection rules normally apply.

The legislation

Data protection legislation relates to the protection of living individuals with regard to the processing of their personal data. Core legislation includes the General Data Protection Regulation (GDPR) and the Data Protection Act 2018. These pieces of legislation, as well as supplementary legislation, case law, guidance, and best practice, work together and are addressed collectively in this document.

General Data Protection Regulation

The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a piece of European Union legislation with direct effect in the UK. The GDPR provides much of the UK's core data protection law and sets out, for example, the data protection principles, the lawful bases for processing personal data, and definitions for personal data, special categories of personal data, and Pseudonymisation.

Data Protection Act 2018

The Data Protection Act 2018 (DPA 2018) is a piece of UK legislation that supports and expands on the rules set out by the GDPR. The DPA 2018 does not replace the GDPR. This is a lengthy piece of legislation, covering a wide range of topics. In particular, the DPA 2018 provides certain specific exemptions to data protection law, such as for archiving, research, and freedom of expression, that are addressed in this guidance document.

Data protection principles

Personal data must be processed in accordance with the six data protection principles in Article 5 of the GDPR.

The data protection principles are:

personal data must be:

1. processed lawfully, fairly and in a transparent manner;
2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (further processing for scientific or historical research purposes or statistical purposes may be compatible – see the “Research use” section);
3. adequate, relevant and limited to what is necessary (‘data minimisation’);
4. accurate and, where relevant, kept up to date;
5. 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 (longer retention for scientific or historical research purposes or statistical purposes may be permissible – see the “Research use” section); and
6. processed in a manner that ensures appropriate security of the personal data.

The data controller must be able to demonstrate compliance with the principles.

Lawfulness of processing

To comply with the first data protection principle, personal data may only be processed if there is a lawful basis for doing so. There are six lawful bases, set out in Article 6 of the GDPR. In rare cases there may be an exemption that means a lawful basis is not always required (see the “Journalistic, academic, artistic and literary uses” section).

The lawful bases are:

1. the data subject has given consent to the processing;
2. the processing is necessary for the performance of a contract (or entering into a contract) with the data subject;
3. the processing is necessary for compliance with a legal obligation;
4. the processing is necessary for protecting the vital interests of an individual;
5. the processing is necessary for the performance of a task carried out in the public interest; or
6. the processing is necessary for the purposes of the legitimate interests pursued by the data controller or another party.

There are detailed rules on the use of these lawful bases. In particular, there is further regulation around the ‘consent’ and ‘legitimate interests’ bases. Guidance is available from the ICO. Links to guidance are available in the “Links to further information” section at the end of this document.

Special categories of personal data

Additional restrictions apply to the processing of special categories of personal data.

special categories of personal data are:

- personal data revealing:
 - a. racial or ethnic origin
 - b. political opinions
 - c. religious or philosophical beliefs
 - d. trade union membership
- genetic data
- biometric data processed for the purposes of uniquely identifying an individual
- data concerning health
- data concerning an individual’s sex life or sexual orientation.

processing of personal data related to criminal convictions and offences is restricted in a manner largely equivalent to the special categories of personal data.

The Library may restrict access to materials that contain special categories of personal data. However, such information may not always be identified or identifiable in advance, or the Library may at times deem it fair and lawful to permit access to material containing special categories of personal data.

Therefore, it is possible material accessed through the Library’s collections contains special categories of personal data, in particular if the material has not previously been published or made widely available to the public (for example, if the material is archival in nature).

Guidance is available from the ICO. Links to the guidance are available in the “Links to further information” section at the end of this document.

IV. Using personal data from the collections

If you choose to copy, reproduce, manipulate, publish or otherwise use (process) material held in the Library's collections, you are responsible for ensuring the safe and lawful processing of any personal data in that material.

You will become the data controller in respect of any personal data you use or otherwise process from materials held in the Library's collections.

This means you will be responsible for ensuring your use of information is legal, and in particular that it is compliant with data protection laws.

As a user of the Library you have agreed to abide by the Library's terms and conditions. Our terms and conditions specify that you are responsible for compliance with data protection laws whenever you use personal information obtained from materials held in our collections.

If you intend to process personal data:

- for purely personal or household activities you **may** be able to do so without further restrictions (see the "Personal use" section);
- for scientific or historical research purposes or statistical purposes you must ensure specific safeguards are in place (see the "Research use" section); or
- with a view to publication for journalistic, academic, artistic or literary purposes there are specific exemptions in data protection law you may wish to consider (see the "Journalistic, academic, artistic and literary uses" section).

You should consult the legislation or external guidance before you use personal data from material in the Library's collections.

You may wish to seek advice from the ICO or a legal professional if you have questions or concerns about processing personal data.

Personal use

Processing of personal data by individuals in the course of purely personal or household activities is outside of the scope of the GDPR.

Therefore, it **may** be possible to make use of personal data for purely personal or household activities without additional requirements. However, it remains important to exercise significant care for all personal data and to ensure that data is not used or accessed for other purposes that do not comply with the legislation.

Research use

The second and fifth data protection principles permit further use and retention of personal data for the purposes of scientific or historical research or statistical purposes, provided specific safeguards are in place.

The safeguards are:

1. the processing must not be likely to cause substantial damage or substantial distress to a data subject; and
2. the processing must not be carried out for the purposes of measures or decisions with respect to a particular individual (except in certain cases in relation to certain forms of medical research).

Processing of personal data for these purposes in accordance with the safeguards must still comply with the other data protection principles. For example, a legal basis is still required to ensure compliance with the first data protection principle.

When personal data is processed for these purposes in accordance with the safeguards, the following provisions of the GDPR will not apply:

The right of access by the data subject, but only if the results of the research or any resulting statistics are not made available in a form which identifies a data subject (GDPR Article 15(1)-(3))

The right to restriction of processing (GDPR Article 18(1))

The right to object to processing (GDPR Article 21(1))

Journalistic, academic, artistic and literary uses

Subject to the listed requirements, various provisions of the GDPR do not apply to personal data that is processed for the listed special purposes, to the extent that the data controller reasonably believes that the application of those provisions would be incompatible with the special purposes.

The special purposes are:

- a. The purposes of journalism;
- b. Academic purposes;
- c. Artistic purposes;
- d. Literary purposes.

The requirements are:

- a. the processing is being carried out with a view to the publication by a person of journalistic, academic, artistic or literary material; and
- b. the data controller reasonably believes that the publication of the material would be in the public interest, taking into account the special importance of the public interest in the freedom of expression and information and having regard to any of the following codes of practice or guidelines that is relevant to the publication in question:
 - i. BBC Editorial guidelines;
 - ii. Ofcom Broadcasting Code;
 - iii. Editors' Code of Practice.

The provisions are listed in the DPA 2018 (at Schedule 2, Part 5, Paragraph 26(9)) and include:

Data protection principles 1 to 5 (GDPR Article 5(1)(a)-(e))

Requirement to have a lawful basis (GDPR Article 6)

Restrictions on processing special categories of personal data and criminal convictions data (GDPR Articles 9 and 10)

Requirements to provide information to data subjects (GDPR Articles 13(1)-(3) and 14(1)-(3))

The right of access by the data subject (GDPR Article 15(1)-(3))

The right of rectification	(GDPR Article 16)
The right of erasure	(GDPR Article 17(1) and (2))
The right to restriction of processing	(GDPR Article 18(1)(a), (b) and (d))
The right of data portability	(GDPR Article 20(1) and (2))
The right to object to processing	(GDPR Article 21(1))

Anonymisation and pseudonymisation

Anonymisation and pseudonymisation of personal data are valuable and helpful techniques to support compliance with the data protection legislation and to protect peoples' personal data. These practices may enable safer use of information. However, it is important to ensure data are properly and effectively anonymised or pseudonymised.

Anonymous information is information that does not relate to an identified or identifiable natural person, or is personal data that has been rendered anonymous in such a manner that the data subject is not or no longer identifiable.

Because it is not personal data, anonymous information is outside the scope of the GDPR.

However, it is important to ensure that data is truly anonymous. In particular, it may not be sufficient to remove names or other identifiers from a set of information if it would be reasonably practicable for a person to identify specific individuals, for example by looking at the context of the data or by combining the data with other data to which they may have access.

Pseudonymisation is the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to a data subject.

Unlike anonymous data, pseudonymous data **is** personal data and so within scope of the GDPR. However, the legislation encourages the use of pseudonymisation as a means of reducing risks to data subjects and of helping data controllers meet their data protection requirements. Pseudonymisation may in particular support compliance with the sixth data protection principle (integrity and confidentiality of the data).

External advice is available on anonymisation and pseudonymisation, which you are encouraged to consult. The ICO has previously published an Anonymisation Code of Practice. To date, this has not been updated to account for changes to data protection law in 2018. However, the principles and recommendations in the Code are likely to remain highly applicable.

V. Glossary of terms

- Data Controller** The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data
- Data Processor** A natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller
- Data Subject** An identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
- Personal Data** Any information relating to a data subject
- Processing** Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction
- Special Categories of Personal Data**
- personal data revealing:
 - racial or ethnic origin
 - political opinions
 - religious or philosophical beliefs
 - trade union membership
 - genetic data
 - biometric data processed for the purposes of uniquely identifying an individual
 - data concerning health
 - data concerning an individual's sex life or sexual orientation.

VI. Links to further information

General Data Protection Regulation (GDPR)	bit.ly/2knMlxY
Data Protection Act 2018	www.legislation.gov.uk/ukpga/2018/12/contents/enacted
Information Commissioner's Office	ico.org.uk
Information Commissioner's Office Anonymisation Code of Practice (archived)	bit.ly/2NDSGHx
National Library of Scotland Data Protection Policy	www.nls.uk/media/1632540/2018-data-protection-policy.pdf
National Library of Scotland privacy notices	www.nls.uk/privacy

VII. Contact

Web: www.nls.uk/privacy
Email: privacy@nls.uk
Phone: +44 (0)131 623 3700