# National Library of Scotland Data Protection Policy

28 August 2018

## 1. Commencement

This policy commences on 25 May 2018, irrespective of whether it is approved prior to that date.

## 2. Scope

This policy applies to:

1. all personal data processing activities carried out by the National Library of Scotland or on behalf of the Library, as well as to the planning or consideration of future processing activities;
2. the exercise of the Library's legal obligations in respect of personal data, including the exercise of data subject rights;
3. all Library employees (temporary and permanent), volunteers, board members, and the Chair of the Board, as well as contractors, data processors, and suppliers in the course of their service for the Library; and
4. personal data processed or intended to be processed:
    a. wholly or partly by automated means,
    b. as part of a relevant filing system, or
    c. by means of manual unstructured processing of personal data.

## 3. Definitions

| | | |
|---|---|---|
| Article 29 Working Party | A29WP | The former EU-wide data protection advisory body and predecessor to the European Data Protection Board |
| 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 (GDPR Art.4(7)) |
| Data breach | | A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed (GDPR Art. 4(12)) |
| Data Protection Act 2018 | the Act | The Act that functions alongside and in addition to the GDPR in the UK, repealing the Data Protection Act 1998 |
| Data Protection Legislation | | The GDPR and the Act together, as well as any additional legislation that may be applicable to the processing or protection of personal data |
| Data protection review | | A review or appraisal of a new or revised activity, policy, system, or similar that may involve the processing of personal data |
| Data subject | | An identified or identifiable natural person (ie an individual); 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 (GDPR Art. 4(1)) |
| Direct marketing | | The communication (by whatever means) of advertising or marketing material which is directed to particular individuals (Act s.122(5)) |
| European Data | EDPB | The EU-wide data protection authority and advisory body |

| | | |
|---|---|---|
| Protection Board | | established under the GDPR |
| General Data Protection Regulation | GDPR | Regulation (EU) 2016/679 of The European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (the Data Protection Directive 1995) |
| Information Commissioner's Office | ICO | The UK data protection authority |
| Personal data | | Any information relating to an identified or identifiable natural person ('data subject') (GDPR Art. 4(1)) |
| Personal Data Register | the Register | A register of information about various personal data processing activities, arrangements, and requirements. |
| 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 (GDPR Art. 4(2)) |
| Processor | | A natural or legal person, public authority, agency or other body which processes personal data on behalf of a controller (GDPR Art. 4(8)) |
| Senior Responsible Officer | | Has the meaning given the Records Management Policy |
| Special Categories Data Processing Document | | A document to be completed in certain cases where special categories of personal data or personal data relating to criminal convictions and offences are to be processed, in accordance with Schedule 1 paragraph 39 of the Act. |
| Special categories of personal data | | Personal data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as genetic data, biometric data (when processed for the purpose of uniquely identifying an individual person), data concerning health or data concerning an individual person's sex life or sexual orientation (GDPR Art. 9(1)) |
| Third country | | A country that is not a European Union (EU) Member State |
| Unstructured personal data | | Means personal data held by a public authority (such as the Library) that is not processed automatically or by means of a relevant filing system |

## 4. Policy statement

The Library, its employees and agents shall not process personal data except in accordance with the principles relating to processing of personal data in Article 5 of the General Data Protection Regulation (GDPR) or as otherwise permitted in the Data Protection Legislation.

The processing of personal data by the Library and its agents, including as a data controller, joint data controller, or data processor, must be in compliance with the Data Protection Legislation, this policy, and the Library's other policies as may be in place and of relevance from time to time.

# 5. Tasks carried out in the public interest

For the purposes of s.7(2) of the Data Protection Act (the Act), the Library is only a 'public authority' or 'public body' when performing a task carried out in the public interest or exercising official authority vested in it.

# 6. Data Protection Officer

## 6.1. Appointment

The Library will appoint a Data Protection Officer in accordance with the requirements of the Data Protection Legislation. The individual fulfilling this role may undertake other tasks and duties. The Data Protection Officer role may not be undertaken by any individual with tasks or duties that would result in a conflict of interests. In determining if particular tasks or duties may present a conflict of interest, particular reference should be made Section 4 of the GDPR and to relevant guidelines and publications of the A29WP, EDPB, and ICO.

## 6.2. Role

The role, position, and functions of the Data Protection Officer will be set out in a relevant job description and will accord with the requirements and guidelines of the Data Protection Legislation and the supervisory authorities.

The Data Protection Officer's line manager is responsible for keeping the Data Protection Officer job description up to date in accordance with legislative and policy changes.

# 7. Documentation of processing activities

## 7.1. Recording activities in the Register

The Library will maintain and keep up to date a record of personal data processing activities by means of the Personal Data Register (the Register).

The Register will be used to record and keep up to date the information required by Article 30(1) of the GDPR and by Schedule 1 paragraph 41 of the Act.

## 7.2. Maintenance and reporting of the Register

All employees are responsible for adding information to the Register and keeping information up to date in respect of any relevant work for which they are responsible, such as the management of a contract with a data processor.

The Data Protection Officer is responsible for maintaining the Register with the support of Senior Responsible Officers and other employees involved in personal data processing activities.

At least once every three months the Library Leadership Team will review the Register with input as required from the Data Protection Officer.

# 8. Data protection by design and by default

## 8.1. Data protection principles

In respect of its processing activities, the Library will implement suitable technical and organisational measures to ensure the principles relating to processing of personal data are upheld and, where relevant, that exceptions to the principles are applied appropriately.

In particular, data protection reviews are to be conducted in relation to processing activities, as set out in section 8.2 and Special Categories Data Processing Documents are to be in place as required under section **Error! Reference source not found.**.

The principles relating to processing of personal data are outlined in Appendix I: Data protection principles.

## 8.2. Data protection reviews

The following, as a minimum, must be subject to a data protection review:

a. New policies
b. Revisions to existing policies
c. New collaborations likely to involve the processing or sharing of personal data
d. Existing collaborations likely to involve the processing or sharing of personal data when subject to revision, change, expansion, or extension
e. New procedures, workflows or similar that relate to activities likely to involve the processing of personal data
f. Revisions to existing procedures, workflows or similar that relate to activities likely to involve the processing of personal data
g. The procurement, purchase, or implementation of a new software, hardware, or system that is likely to involve the processing of personal data
h. Revisions or changes to existing software, hardware, or systems that are likely to involve the processing of personal data
i. Any planned or likely processing of special categories of personal data or personal data relating to criminal convictions and offences

Data protection reviews should be begun at the earliest possible opportunity and in any case should be complete, unless this would be impossible, at the latest:

- prior to a policy being submitted for approval,
- prior to the start of a collaboration,
- prior to a procedure or similar being put into place,
- prior to a software, hardware, system, or similar being procured, purchased or implemented, or
- upon revision to an existing policy, collaboration, system, or procedure.

The employee leading or otherwise in control of the relevant policy, collaboration, system, procedure, or similar for the Library is responsible for completing the data protection review with input and assistance as required from the Data Protection Officer.

Data protection reviews must consider and assess relevant data protection matters following the structure set out in Appendix II: Data protection reviews.

A record of the data protection review must be submitted to the Data Protection Officer and to any group or management structure tasked with overseeing or approving the relevant activity, for example the Library Leadership Team.

# 9. Transparency and information supplied to data subjects

## 9.1. Privacy notices

The Library will provide or make available privacy notices that contain relevant information for data subjects in relation to all personal data processing activities.

**Content**

Privacy notices will provide the information set out in Article 13 (where the personal data has been obtained directly from the data subject) or in Article 14 (where the personal data has not been obtained directly from the data subject) of the GDPR, as relevant to the processing activity.

**Publication**

All privacy notices currently in use by the Library should be accessible at www.nls.uk/privacy. Privacy notices may be made available to data subjects through links or by other suitable means, including in print.

**New and existing privacy notices**

All distinct processing activities must have an appropriate privacy notice, which must be prepared and made accessible to data subjects before personal data is obtained or at the first available opportunity after personal data has been obtained (and in any case within one month). Personal data processing activities may make use of an existing privacy notice published by the Library, if suitable, or may rely on a new privacy notice where required.

New privacy notices should be prepared using the template set out in Appendix III: Privacy notice template and should be approved by the Data Protection Officer before use.

**Responsibilities**

All employees are responsible for ensuring that activities, projects, systems, collaborations, or similar for which they are responsible have made suitable privacy notice information available.

The Data Protection Officer is responsible for maintaining existing privacy notices, publishing privacy notices to www.nls.uk/privacy, and providing advice and assistance to employees seeking to prepare or provide privacy information.

## 9.2. Exceptions

In accordance with the Data Protection Legislation there are limited situations in which privacy notices do not need to be made available to data subjects. In particular, privacy notices do not need to be made available to data subjects insofar as a data subject already has the information in respect of that particular processing activity.

Privacy notices do not need to be activity communicated to data subjects where the following points apply. However, in such cases privacy notices must still be prepared, maintained, and made available by means of the Library's website or other widely accessible means:

a. actively providing the privacy notice to data subjects would be impossible or would involve a disproportionate effort, in particular where the personal data are processed for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes; or
b. actively providing the privacy notice to data subjects would be likely to render impossible or seriously impair the achievement of the objectives of that processing;

AND

c. the data has not been obtained directly from the data subject; and
d. where the personal data are processed for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes the processing is subject to the safeguards set out in the Data Protection Legislation and summarised at section 21.1.

# 10. Data subject rights

All data subjects benefit from certain rights under the Data Protection Legislation. The data subject rights are listed in Appendix IV: Data subject rights.

## 10.1. Receiving and reporting requests

The Library will provide the means for data subjects to submit requests to enact one or more of the data subject rights. These means may include a dedicated email address, a named Data Protection Officer with a postal address, a paper form, and/or an online form.

Any employee may receive a request directly from a data subject by any means.

All requests should be passed immediately to the Data Protection Officer, preferably in writing by internal post or by email to privacy@nls.uk.

Employees should not seek to satisfy a request without consulting the Data Protection Officer.

Requests are confidential and should be treated as such. Details of requests made, in particular the identity or other personal data of the data subject making the request, must not be discussed or shared with others except for the direct purposes of reporting and handling the request as required under this policy.

### 10.2. Making requests

Employees and agents of the Library may, as data subjects, make requests of the Library in respect of their own personal data. Employees may use the same requests mechanisms that are available for all data subjects as set out in section 10.1.

### 10.3. Responding to requests

The Data Protection Officer will coordinate the Library's handling of and response to all requests related to data subject rights, except as set out in this section.

If the Data Protection Officer makes a request to the Library in relation to their own personal data, the Associate Director of Business Support, the Human Resources Manager, or, in the absence of both, a nominated deputy, will coordinate the Library's handling of and response to such a request.

### 10.4. Record keeping

The Library will maintain a record of requests received and handled in respect of data subject rights. As a minimum the Library will record:

a. personal details of data subjects sufficient to the extent that relevant data subject rights may be exercised
b. the dates on which requests have been received and responded to or otherwise addressed
c. any further details required for the effective implementation of relevant data subject rights

The Data Protection Officer will maintain and keep up to date the Library's records related to data subject rights.

## 11. Special categories of personal data

### 11.1. Conditions

The Library may not process special categories of personal data unless a valid exception under Article 9(2) of the GDPR applies and, when relevant, the processing is in accordance with a relevant condition under Schedule 1 of the Act, in compliance with s.10 of the Act.

S.10 of the Act is relevant when special categories of personal data are processed in accordance with the following exceptions under Article 9(2) of the GDPR:

a. Article 9(2)(b) (employment, social security and social protection);
b. Article 9(2)(g) (substantial public interest);
c. Article 9(2)(h) (health and social care);
d. Article 9(2)(i) (public health); or
e. Article 9(2)(j) (archiving, research and statistics).

The Library may not process personal data relating to criminal convictions and offences unless the processing is in accordance with a relevant condition under Schedule 1 of the Act, in compliance with s.10(5) of the Act.

### 11.2. Processing documents

Processing of special categories of personal data or personal data relating to criminal convictions and offences that is carried out in reliance on a condition under Schedule 1 of the Act that requires an 'appropriate policy document' must have a Special Categories Data Processing Document in place as outlined in Appendix V: Special Categories Data Processing Document.

The employee leading or otherwise in control of the relevant processing activity is responsible for completing the Special Categories Data Processing Document with input and assistance as required from the Data Protection Officer.

### 11.3. Recording activities in the Register

The Library will maintain and keep up to date a record of its processing of special categories of personal data and personal data relating to criminal convictions and offences, including information required under Schedule 1 paragraph 41 of the Act, by means of the Personal Data Register (the Register).

## 12. Use of data processors

### 12.1. Conditions

The Library may not permit or enable a third party to process personal data on its behalf (ie act as a data processor for the Library) except as set out in this policy.

The conditions for the use of a data processor are:

a. completion of a data protection review in accordance with section 8.2 and Appendix II: Data protection reviews (unless the use of a processor is necessary for the purposes of meeting a legal obligation); and
b. implementation or agreement of a written contract or other legal instrument that is binding on the processor with regard to the Library and the relevant processing activity and that sets out the relevant subject-matter as specified in the Data Protection Legislation (in particular Article 28 of the GDPR) as outlined in Appendix VI: Data processor requirements.

All employees are responsible for ensuring data processor conditions are met in respect of activities, projects, systems, collaborations, or similar for which they are responsible.

The Data Protection Officer is responsible for providing advice and assistance to all employees in respect of data processor arrangements.

### 12.2. Recording activities in the Register

The Library will maintain and keep up to date a record of its use of data processors by means of the Personal Data Register (the Register).

## 13. The Library as a data processor

### 13.1. Conditions

The Library may function as a data processor for a third party data controller in accordance with the requirements of this policy and the Data Protection Legislation.

The conditions for the Library to function as a data processor are:

a. completion of a data protection review in accordance with section 8.2 and Appendix II: Data protection reviews (unless the function of the Library as a processor is necessary for the purposes of meeting a legal obligation); and
b. implementation or agreement of a written contract or other legal instrument that is binding on the Library with regard to the data controller and the relevant processing activity and that sets out the relevant subject-matter as specified in the Data Protection Legislation (in particular Article 28 of the GDPR) as outlined in Appendix VI: Data processor requirements

All employees are responsible for ensuring data processor conditions are met in respect of activities, projects, systems, collaborations, or similar for which they are responsible.

The Data Protection Officer is responsible for providing advice and assistance to all employees in respect of data processor arrangements.

### 13.2. Recording activities in the Register

The Library will maintain and keep up to date a record of its functions as a data processor by means of the Personal Data Register (the Register).

The Register will be used to record and keep up to date the information required by Article 30(2) of the GDPR.

# 14. The Library as a joint data controller

## 14.1. Conditions

The Library may function as a joint data controller in relation to processing activities in which the Library together with one or more other data controllers jointly determines the purpose and means of processing.

The conditions for the Library functioning as a joint data controller are:

a. completion of a data protection review in accordance with section 8.2 and Appendix II: Data protection reviews (unless the function of the Library as a joint data controller is necessary for the purposes of meeting a legal obligation); and
b. establishment, in a transparent manner, with the other data controller(s) each controller's respective responsibilities for compliance with the Data Protection Legislation, in particular the requirements to provide privacy information (as set out in section 9)

All employees are responsible for ensuring joint controller conditions are met in respect of activities, projects, systems, collaborations, or similar for which they are responsible.

The Data Protection Officer is responsible for providing advice and assistance to all employees in respect of joint data controller arrangements.

## 14.2. Recording activities in the Register

The Library will maintain and keep up to date a record of its functions as a joint data controller by means of the Personal Data Register (the Register).

# 15. Security

## 15.1. Security of personal data

Personal data processed by the Library must be managed in accordance with the Information Security Policy, the Records Management Policy, and the Library's other information, data, and property security policies and procedures.

## 15.2. Disposal of records containing personal data

Personal data disposed of by the Library, whether destroyed or retained for permanent archiving, must be disposed of in accordance with the Records Management Policy, the Business Classification and Retention Scheme, and the Records Disposal Procedures. Personal data disposed of by means of destruction must be destroyed in a safe and secure manner in accordance with the Records Disposal Procedures.

## 15.3. Disposal and repurposing of IT Assets

IT Assets must be disposed of or repurposed in accordance with the Information Security Policy.

Personal data must be removed from IT Assets by the Library before disposal or repurposing, or an appropriately certified third party subject to relevant contractual obligations must remove and destroy all personal data from IT Assets on the Library's behalf before disposal or repurposing.

# 16. Data Breaches

## 16.1. Reporting

All employees and agents of the Library must report immediately any possible or suspected data breach to the Data Protection Officer, to their line manager, or to any manager.

Any employee or agent of the Library in receipt of a report of a potential data breach must report it immediately to the Data Protection Officer, preferably in writing to privacy@nls.uk.

The Library will provide the means for third parties to submit reports of suspected data breaches. These means may include a dedicated email address, a named Data Protection Officer with a postal address, a paper form, and/or an online form.

The Library must report all data breaches to the ICO unless a breach is unlikely to result in a risk to the rights and freedoms of individuals. Such reporting should be undertaken in accordance with the Data Protection Legislation, in particular Article 33 of the GDPR.

If a data breach is likely to result in a high risk to the rights and freedoms of individuals the Library may need to report the breach to the relevant data subject(s). Such reporting should be undertaken in accordance with the Data Protection Legislation, in particular Article 34 of the GDPR.

The Data Protection Officer is responsible for determining whether a data breach report should be made to the ICO and/or to data subjects and is responsible for coordinating such reporting for the Library.

### 16.2. Recording breaches in the Register

The Library will maintain and keep up to date a record of data breaches by means of the Personal Data Register (the Register).

The Register will be used to record and keep up to date the information required by Article 33(5) of the GDPR.

## 17. Data protection impact assessments and prior consultation

### 17.1. Conditions

The Library will conduct a data protection impact assessment prior to the processing of personal data in the unlikely case that such is required by the Data Protection Legislation and the ICO, in particular with reference to Article 35 of the GDPR and any list(s) published by the ICO under Article 35(4) of the GDPR.

In general, data protection impact assessments are only required where processing is likely to result in a high risk to the rights and freedoms of individuals.

All employees are responsible for establishing whether a data protection impact assessment is required prior to processing and, if required, that the conditions set out in this section are met in respect of activities, projects, systems, collaborations, or similar for which they are responsible.

The Data Protection Officer is responsible for providing advice and assistance to all employees in respect of data protection impact assessments.

### 17.2. Prior consultation with the ICO

If a data protection impact assessment concluded under section 17.1 indicates that processing will result in a high risk in the absence of measures taken by the Library to mitigate the risk the Library must consult the ICO prior to commencing the processing, in accordance with the requirements of Article 36 of the GDPR.

### 17.3. Conduct of impact assessments and prior consultation

If a planned processing activity requires the conduct of a data protection impact assessment, such processing may not commence until the impact assessment has been concluded in accordance with the requirements of this policy, the Data Protection Legislation, and the ICO.

## 18. Transfer of personal data outside the United Kingdom

### 18.1. Transfer to European Union Member States

Subject to the requirements of this policy, personal data may be transferred by the Library to European Union Member States.

### 18.2. Transfer to adequate countries and international organisations

Subject to the requirements of this policy, personal data may be transferred by the Library to a country or international organisation that is outside the European Union and that has been determined to provide an adequate level of protection by the European Commission.

The website of the European Commission or EDPB should be consulted for an up to date list of the countries and international organisations that have been determined to provide an adequate level of protection.

### 18.3. Transfer to third countries or international organisations

Personal data may not be transferred to a 'third' country or international organisation – that is, a country or international organisation that does not fall under sections 18.1 or 18.2 – unless the conditions of this section are satisfied.

**Conditions for transfer**

Transfer to a third country or international organisation may only take place if appropriate safeguards are in place in accordance with Articles 46-49 of the GDPR. In particular, such safeguards may be set out in a binding contract or through model contract clauses as adopted by a supervisory authority.

The Library may make use of the most appropriate mechanism for enabling safe transfer of personal data, provided that such meet the requirements of the Data Protection Legislation.

All employees are responsible for ensuring appropriate safeguards for data transfers to third countries and organisations are place in respect of activities, projects, systems, collaborations, or similar for which they are responsible.

The Data Protection Officer is responsible for providing advice and assistance to all employees in respect of safeguard arrangements for data transfers to third countries and organisations.

**Recording transfers in the Register**

The Library will maintain and keep up to date a record of data transfers to third countries and organisations by means of the Personal Data Register (the Register).

## 19. Direct marketing

### 19.1. Conditions

The Library may not undertake activities that constitute Direct Marketing unless the relevant requirements are met, in particular in relation to the Privacy and Electronic Communication Regulations (PECR) and the advice and codes or practices published by the ICO or other advisory authorities.

All employees are responsible for ensuring that activities, projects, systems, collaborations, or similar for which they are responsible and that may involve direct marketing are only conducted in accordance with the relevant requirements.

The Head of External Relations and Governance is responsible for providing advice and assistance to all employees in respect of direct marketing and for ensuring the Library's compliance with the rules and regulations for direct marketing.

### 19.2. Recording activities in the Register

The Library will maintain and keep up to date a record of its direct marketing activities by means of the Personal Data Register (the Register).

## 20. Closed Circuit Television (CCTV)

### 20.1. Conditions

The Library must only implement a CCTV system or make use of CCTV in compliance with relevant legislation, including the Data Protection Legislation, and relevant advice and codes of practices published by the ICO or other advisory authorities. In particular, the Library's use of CCTV should be

in accordance with the ICO's CCTV code of practice and the Scottish Government's national strategy for public space CCTV in Scotland.

The Library's use of CCTV must be limited to the purposes set out in its registration with the ICO and purposes that are otherwise legitimate or permissible in accordance with legislation or legal requirements.

The Security and Cleaning Services Manager is responsible for providing advice and assistance to all employees in respect of CCTV and for ensuring the Library's compliance with the rules and regulations for the use of CCTV.

### 20.2. CCTV use and users

Only employees of the Library with a specific operational requirement may access data captured or recorded by the Library's CCTV system(s). Staff with an operational requirement to access CCTV data, for example for the purposes of ensuring safety and security, may only do so in the course of such specific functions, should have such specific functions clearly set out in a job description, and must receive suitable training in the use of CCTV and the Library's systems, policies, and procedures.

On occasion, employees may process CCTV data beyond the scope of specific activities set out in a job description, for example in the course of an investigation. In such cases employees must be limited specifically to data relevant to the processing activity and must undertake access to and any further use of the CCTV data in conjunction with, and with the advice and assistance of, the Security and Cleaning Services Manager and/or the Data Protection Officer.

CCTV data may be accessible by means of screens at the time of capture (ie live) or at a later time (ie as recorded data). In all cases the display of CCTV data constitutes data processing. Screens must at all times be arranged and positioned in such a manner that other persons may not view or otherwise gain access to the data.

### 20.3. Recording activities in the Register

The Library will maintain and keep up to date a record of its use of CCTV by means of the Personal Data Register (the Register).

## 21. Freedom of expression, archiving, and research

### 21.1. Processes and procedures

The Library will prepare and maintain appropriate processes, procedures, and guidance in relation to processing of personal data for archiving, research, statistical, and freedom of expression purposes, noting that such have a particular pertinence to the Library's core aims and objectives.

Such will be prepared and kept up to date by the Data Protection Officer with support from the Head of Collections and Research, the Head of Access, and other roles as appropriate.

## 22. Roles and responsibilities

### 22.1. Employees, volunteers, board members, the Chair of the Board, contractors, processors, and suppliers

| Responsibility | | Section |
|---|---|---|
| Data subject rights | Forward requests to the Data Protection Officer | 10.1 |
| Data breaches | Report these to the Data Protection Officer | 16.1 |

## 22.2. Employees

| Responsibility | | Section |
|---|---|---|
| Privacy information | Prepare and make information available | 9.1 |
| Data protection reviews | Conduct reviews when required, including in relation to: | 8.2 |
| | The use of data processors | 12.1 |
| | The Library as a data processor | 13.1 |
| | The Library as a joint controller | 14.1 |
| Personal Data Register | Prepare and keep Register records up to date, including in relation to: | 7.2 |
| | Special categories of personal data | 11.3 |
| | The use of data processors | 12.2 |
| | The Library as a data processor | 13.2 |
| | The Library as a joint controller | 14.2 |
| | Transfer to third countries or international organisations | 18.3 |
| | Direct marketing | 19.2 |
| Special Categories Data Processing Document | Prepare document in advance when required | 11.2 |
| Data protection impact assessments | Conduct assessments in advance when required | 17.1 |
| Transfer to third countries or international organisations | Meet transfer conditions in advance when required | 18.3 |
| Direct marketing | Meet conditions in advance when required | 19.1 |
| Training and support | Consult guidance, policies, and procedures and seek advice and support | 23 |

## 22.3. Managers

| Responsibility | | Section |
|---|---|---|
| Data breaches | Forward reports of breaches to the Data Protection Officer | 16.1 |
| Training and support | Make training and support available and known to direct reports and new starts | 23 |

## 22.4. Senior Responsible Officers

| Responsibility | | Section |
|---|---|---|
| Personal Data Register | Monitor and ensure information is kept up to date | 7.2 |

## 22.5. Library Leadership Team

| Responsibility | | Section |
|---|---|---|
| Personal Data | Review and monitor the Register | 7.2 |
| Training and support | Help to determine frequency and scope of training and guidance | 23 |

## 22.6. Data Protection Officer

| Responsibility | | Section |
|---|---|---|
| Provide advice and assistance, including in relation to: | Privacy notices | 9.1 |
| | Data protection reviews | 8.2 |
| | Special Categories Data Processing Document | 11.2 |
| | The use of data processors | 12.1 |
| | The Library as a data processor | 13.1 |
| | The Library as a joint controller | 14.1 |
| | The Personal Data Register | 7.2 |
| | Data protection impact assessments | 17.1 |
| | Transfer to third countries or international organisations | 18.3 |
| Privacy notices | Maintain existing notices and support preparation and publication of new notices | 9.1 |
| Data subject rights | Coordinate handling and response to subject rights requests | 10.3 |
| | Maintain records of requests | 10.4 |
| Data protection reviews | Review submissions and maintain records | 8.2 |
| Personal Data Register | Monitor and ensure information is kept up to date and report to LLT | 7.2 |
| Data breaches | Determine and coordinate breach reporting to the ICO and data subjects | 16.1 |
| | Maintain records in the Register | 16.2 |
| Prior consultation | Coordinate consultation when required | 17.2 |
| Freedom of expression, | Prepare and maintain procedures and guidance, with | 21.1 |

| | | |
|---|---|---|
| archiving, and research | relevant support and input | |
| Training and support | Develop, provide, and help to determine frequency and scope of training and guidance | 23 |

### 22.7. Security and Cleaning Services Manager

| Responsibility | | Section |
|---|---|---|
| CCTV | Ensure compliance | 20.1 |
| | Maintain records in the Register | 20.3 |

### 22.8. Head of External Relations and Governance

| Responsibility | | Section |
|---|---|---|
| Direct marketing | Provide advice and assistance and ensure compliance | 19.1 |

### 22.9. In the absence of the Data Protection Officer

If the Data Protection Officer is absent from the Library, relevant obligations of that role shall in the interim be fulfilled as follows:

a. by a suitable deputy as nominated by the Data Protection Officer; or if not specified,
b. by the Data Protection and Records Assistant together with the Data Protection Officer's line manager; or if not available,
c. by the Data Protection and Records Assistant together with the Human Resources Manager; or if not available,
d. by a suitable role as nominated by the National Librarian and Chief Executive.

For the purposes of this section, the Data Protection Officer is considered absent from the Library when away from the organisation on a form of leave or when the role remains unfilled. The Data Protection Officer is not considered absent from the organisation when physically away from the organisation while working, for example when traveling for business, unless such is for an extended period, in which case the Data Protection Officer may seek to nominate a deputy in advance.

## 23. Training and support

The Library will provide suitable training and support in matters of data protection for all employees and in particular for roles with further specified responsibilities under sections 22.3 to 22.8, as well as for volunteers and other agents as required.

Training and support, including as relevant in the form of written guidance, internal or external training, e-learning, reading, and reference to third party resources, will be provided initially within three months of the commencement of this policy under section 1 and thereafter at the time of induction for all new employees and at regular intervals for all other staff as deemed appropriate or necessary by the Data Protection Officer, the Human Resources Department, and/or the Library Leadership Team, taking into account in particular any significant changes to the Library's constitution, functions, or resources and any significant external changes, such as in legislation or case law.

All employees and agents of the Library are responsible for familiarising themselves with policies, procedures, and guidance that have been made available and that relate to the protection of personal data, in particular in areas relevant to a post-holder's role. All employees and agents of the Library are responsible for consulting available guidance or seeking advice and assistance from their manager or the Data Protection Officer, at the earliest opportunity.

## 24. Regulatory environment

The following legislation is of particular relevance to the subject matter of this policy:

General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016)

Data Protection Act 2018

Privacy and Electronic Communications (EC Directive) Regulations 2003 (2003 No. 2426)

The following authorities are of particular relevance to the subject matter of this policy:

European Data Protection Board

Article 29 Working Party

Information Commissioner's Office

## 25. Related policies and procedures

Information Security Policy

Business Classification and Retention Scheme

Records Management Policy

Records Disposal Procedures

CCTV Procedures

## 26. Enforcement

Transgressions of this policy will be addressed by means of the Discipline Policy.

Failure to comply with Data Protection Legislation can be serious and may result in advisory or legal action against individuals, the Library, or other organisations. In rare cases actions undertaken in contravention of the Data Protection Legislation may constitute a criminal offence.

## 27. Review

This policy will be subject to initial review by 25 August 2018 and thereafter will be reviewed annually by the Data Protection Officer role-holder. Changes to this policy must be approved by the Library Leadership Team.

# Appendix I: Data protection principles

The data protection principles are set out in Article 5 of the General Data Protection Regulation (GDPR):

"1. Personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('**lawfulness, fairness and transparency**');
b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('**purpose limitation**');
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('**data minimisation**');
d) 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**');
e) 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 in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('**storage limitation**');
f) 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 confidentiality**').

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('**accountability**')."

*(Emphasis added)*

## Appendix II: Data protection reviews

Use the Data Protection Review Form to conduct a data protection review.

The form includes instructions and links to advice. The form is a sequence of questions about your activity and aspects of this policy. The form will guide you through which questions you need to answer based on what you are reviewing.

When you have completed the form submit it to the Data Protection Officer using the button after the last question.

The Data Protection Officer will assess your submitted review and communicate with you about any implications, actions, or changes that may be required so that you can process personal data safely.

Speak with the Data Protection Officer if you have any concerns about your review.

# Appendix III: Privacy notice template

All personal data processing activities need to be covered by a privacy notice, which sets out essential information for data subjects about our use of personal data and their rights in relation to the particular activity.

A new processing activity may already be covered by one of the Library's existing privacy notices. To check, look through privacy notices published on our website at www.nls.uk/privacy or consult with the Data Protection Officer.

If an existing notice doesn't cover a new processing activity, then a new notice needs to be produced. All notices must be available via www.nls.uk/privacy and individuals may be provided with a link to that page and/or the specific privacy notice relevant to the processing activity, although the information may also be communicated to individuals in other ways, for example in print.

Use the following template to prepare a new privacy notice if one is required. Fill in as much as you can, and submit the completed template to the Data Protection Officer.

| | |
|---|---|
| **Purpose** | |
| **Explanation of the purpose** | |
| **Legal basis** | |
| **Types of personal information** | |
| **Sources of personal information** | |
| **Recipients of the data** | |
| **Retention period** | |
| **Your rights in relation to this data** | |
| **Will the data be transferred to third parties?** | |
| **Will the data be transferred outside the European Union?** | |
| **Is it obligatory to supply this data and what are the consequences of not supplying the data?** | |
| **Will the data be used in automated decision-making?** | |

# Appendix IV: Data subject rights

The data subject rights under the General Data Protection Regulation (GDPR) are summarised below. Many of these rights only apply in certain situations, for example depending on the legal basis for processing.

Consult the Data Protection Officer for assistance in understanding or applying the data subject rights.

A summary of what each right provides is available from www.nls.uk/privacy. Further detail can be found in the GDPR, in guidance from the Information Commissioner's Office (www.ico.org.uk), or from the Data Protection Officer.

| Right | Citation |
|---|---|
| Notification | GDPR Art. 13-14 |
| Access | GDPR Art. 15 |
| Rectification | GDPR Art. 16 |
| Erasure ('right to be forgotten') | GDPR Art. 17 |
| Restriction of processing | GDPR Art. 18 |
| Portability | GDPR Art. 20 |
| To object to processing | GDPR Art. 21 |
| Withdraw consent | GDPR Art. 7 |

Not all rights apply to all processing activities. For example:

- subject to certain criteria, none of the data subject rights listed above may apply in respect of the processing of personal data for journalistic, academic, artistic, and literary purposes (Act Schedule 2 para. 26)
- subject to certain criteria, the rights of access, rectification, erasure, restriction of processing, and to object do not apply when personal data are processed for archiving purposes in the public interest (and the rights of portability and to withdraw consent are unlikely to apply)

# Appendix V: Special Categories Data Processing Document

A Special Categories Data Processing Document is required when special categories of personal data or personal data relating to criminal convictions and offences are processed in accordance with the following conditions:

1. the processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller or the data subject in connection with employment, social security or social protection;
2. the processing is in reliance on the exception in Article 9(2)(g) of the General Data Protection Regulation (substantial public interest) and a condition under Schedule 1 Part 2 of the Act; or
3. the processing is of personal data about a conviction or caution for an offence listed in Schedule 1 Part 3 paragraph 35(2) of the Act and the processing is necessary for the purpose of administering an account relating to the payment card used in the commission of the offence or cancelling that payment card.

(List subject to change in accordance with changes to the legislation. Seek guidance from the Data Protection Officer for confirmation.)

To complete a Document, use the Special Categories Data Processing Document template.

When you have completed the template submit it to the Data Protection Officer.

The Data Protection Officer will assess the Document and communicate with you about any implications, actions, or changes that may be required so that you can process personal data safely.

Speak with the Data Protection Officer if you have any concerns.

# Appendix VI: Data processor requirements

**Use of data processors by the Library**

Processing of personal data by a data processor must be governed by a contract or other legal act that is binding on the processor with regard to the Library and that sets out:

- the subject-matter and duration of the processing,
- the nature and purpose of the processing,
- the type(s) of personal data and categories of data subjects covered by the processing, and
- the obligations and rights of the Library as the data controller.

The contract or other legal act must state, in particular, that the processor:

a. processes the personal data only on documented instructions from the Library, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by law; in such a case, the processor shall inform the Library of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;
b. ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
c. takes all measures required pursuant to Article 32 of the GDPR (Security of processing);
d. respects the conditions referred to below for engaging another processor (is a 'sub-processor');
    i. the processor shall not engage another processor without prior specific or general written authorisation of the Library. In the case of general written authorisation, the processor shall inform the Library of any intended changes concerning the addition or replacement of other processors, thereby giving the Library the opportunity to object to such changes;
    ii. where a processor engages another processor for carrying out specific processing activities on behalf of the Library, the same obligations as set out in the contract or other legal act between the Library and the processor as referred to in Article 28(3) of the GDPR (and as outlined in this Appendix) shall be imposed on that other processor by way of a contract or other legal act, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the GDPR;
e. taking into account the nature of the processing, assists the Library by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Library's obligation to respond to requests for exercising data subject rights;
f. assists the Library in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR (Security of personal data) taking into account the nature of processing and the information available to the processor;
g. at the choice of the Library, deletes or returns all the personal data to the Library after the end of the provision of services relating to processing, and deletes existing copies unless law requires storage of the personal data;
h. makes available to the Library all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR and allow for and contribute to audits, including inspections, conducted by the Library or another auditor mandated by the controller.

The contract with the processor must be in writing (whether in electronic form or otherwise).

The above requirements are summarised from Article 28 of the GDPR. Any employee seeking to establish use of a new data processor should consult the Data Protection Legislation, guidance from the Information Commissioner's Office, and/or the Data Protection Officer for support in ensuring that all data processor requirements are met.

**The Library as a data processor**

Processing of personal data by the Library as a data processor must be governed by a contract or other legal act that is binding on the Library with regard to the data controller and that sets out the information required by the GDPR (in particular Article 28), as summarised above.

Any employee seeking to establish a processing activity with the Library functioning as a data processor should consult the Data Protection Legislation, guidance from the Information Commissioner's Office, or the Data Protection Officer for support in ensuring that all data processor requirements are met.