LLYFRGELL GENEDLAETHOL CYMRU
THE NATIONAL LIBRARY OF WALES

Data Protection Policy

November 2020

This document is also available in Welsh

CONTENTS

INTRODUCTION

The National Library of Wales ("The Library") collects and uses information about people with whom it deals. These include employees, contractors and suppliers as well as members of the public who use its facilities and services.

The Library regards the fair and lawful treatment of personal information as very important to its successful operation and to maintaining confidence between the Library and those people.

The Library is fully committed to compliance with the requirements of the General Data Protection Regulation 2018 and related legislation and codes of conduct ("The Regulation"). The Regulation regulates the way it handles personal information which is collected in the course of its functions and gives certain rights to people whose personal information it may hold. The Library aims to ensure that all who have access to personal data held by it or on its behalf are fully aware of and abide by their duties and responsibilities under the Regulation.

This policy is a statement of the measures which the Library has adopted to ensure that it complies with the requirements of the Regulation.

SCOPE AND DEFINITIONS

The Data Protection Policy is relevant to all personal data that is obtained, held and used by the Library.

In this Policy, as in the Regulation itself, the following terms shall be defined as follows:

Personal Data (Article 4) Any information relating to an identified or identifiable natural person (data subject): 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 person.

Special Categories of Personal Data (Article 9) (known as Sensitive Personal Data under the Data Protection Act 1998)

Personal data consisting of information as to:

- racial or ethnic origin;
- political opinion;
- religious or other beliefs;
- trade union membership;
- physical or mental health;
- sexual life;
- genetic data

biometric data
criminal convictions or offences.

To control (personal data)	To determine the purposes for which and the manner in which any Personal Data are, or are to be, processed.
Data Controller	A person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any Personal Data are, or are to be, processed.
To process (personal data)	To obtain, record or hold the information or data or carry out any operation or set of operations on the information or data.
Data processor	Any person (other than an employee of the data controller) who processes the personal data on behalf of the Data Controller.
Data subject	An individual who is the subject of Personal Data.

THE PRINCIPLES OF DATA PROTECTION

The Regulation stipulates that anyone processing personal data must comply with the following principles. These Principles are legally enforceable (Article 5).

The Principles require that Personal Data:

1. shall be processed lawfully, fairly and in a transparent manner in relation to the data subject;
2. shall be collected for a specified, explicit and legitimate purpose or purposes and shall not be further processed in a manner incompatible with that purpose or 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;
3. shall be adequate, relevant and limited to what is necessary in relation to the purpose or purposes for which it is processed;
4. shall be accurate and where necessary, kept up to date;

5. 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 is processed;

6. 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;

The controller shall be responsible for, and be able to demonstrate compliance with the above principles.

All members of Library staff must observe these Principles when processing Personal Data.

THE DATA PROTECTION OFFICER

1.1 The National Library of Wales, as a corporate body, is the Data Controller under the Regulation and the Library's Board of Trustees, as the governing body of the Library, is ultimately responsible for the implementation of the Regulation within the Library.

1.2 The Library's Data Protection Officer (DPO), who is responsible for overseeing the Library's compliance with the Regulation and is the named contact with the Information Commissioner, is Pedr ap Llwyd, Chief Executive and Librarian, telephone: 01970 632952, e-mail address: dpo@llgc.org.uk. The Deputy Data Protection Officer is Carol Edwards, Governance Manager and Clerk to the Board of Trustees; telephone: 01970 632923, e-mail address: dpo@llgc.org.uk.

1.3 The Deputy DPO is responsible for immediately raising any serious breaches or risks of non-compliance with the Regulation with the Library's Accounting Officer. The DPO is also, with the assistance of the Deputy DPO, responsible for keeping this Policy up to date, ensuring that the Library's entry in the Data Protection Register (see 2.1) is updated regularly and producing an annual report on the Library's compliance with the Act.

1.4 The Director of Corporate Resources is chair of the Information Compliance Committee. The Committee meets at least once a quarter to discuss relevant developments in law, the Library's compliance with its requirements and any Subject Access Requests received.

1.5 Each Department has a Data Protection Coordinator who is a member of the

Information Compliance Committee. Each Data Protection Coordinator has a leading role in ensuring that the Personal Data held by their department is stored securely and is used appropriately, in accordance with the requirements of the Regulation. They are also responsible for notifying the Deputy Data Protection Officer of the type of Personal Data processed by their Department, and of any change or addition to the Personal Data that is processed by the department.

NOTIFICATION OF DATA HELD AND PROCESSED

2.1 The Library will prepare and make available a statement of the types of personal data that it holds and processes and the reasons why that data is held. The Library's Data Protection pages on the website will include a link to the Library's entry in the Data Protection Public Register which contains further information on the types of personal data held by the Library and the purposes for which it is processed.

2.2 Under certain circumstances, usually relating to employment, the Library is required to process Special Categories of Personal Data. Special Categories of Personal Data will always be processed in accordance with the further conditions listed in the Regulation. More information may be found in the Statement concerning the processing of special categories of personal data.

STAFF RESPONSIBILITIES: PROCESSING PERSONAL DATA

3.1 All members of Library staff have a responsibility to ensure that the Data Protection Principles (listed above) are observed at all times.

3.2 Members of staff should ensure that they are familiar with the Library's Data Protection Policy. **Any breach of the Data Protection Policy, whether deliberate or through negligence, may lead to disciplinary action being taken, or access to Library facilities being withdrawn, or even criminal prosecution.** Unauthorised disclosure is a valid reason for disciplinary action and may be considered gross misconduct which could lead to dismissal.

3.3 Members of staff should ensure that any Personal Data that they process is included in the Library's registration in the Data Protection Public Register. The DPO or the Deputy DPO is to be informed of any processing of Personal Data carried out by, or on behalf of, the Library in order to ensure that the Information Commissioner's Office has been notified.

3.4 All staff that supervise and collaborate with Data Processors (including volunteers, employees, students on work experience and external companies) have a duty to ensure that the requirements of Section 6 of this Policy have been met.

3.5 Although the Library has a dedicated form to complete when submitting a Subject Access Request, its completion by Data Subjects is not compulsory in order for the request to be valid (see section 7 of this Policy for more information on Subject Access Requests). Staff should give priority to any requests that may be regarded as Subject Access Requests and contact the DPO and/or Deputy DPO immediately.

3.6 Staff should ensure that the DPO and/or Deputy DPO have been notified of any proposed systems, documents or applications (such as spreadsheets or databases) that will be used to process Personal Data.

3.7 Managers should ensure that any guidelines, procedures or instructions given to staff are consistent with the Data Protection Principles and this Policy and that they are observed at all times.

3.8 Timely training will be provided for all staff that interact with the public on a regular basis and awareness sessions are held for all staff. There is a responsibility on managers to ensure that staff under their management are aware of their responsibilities under the Regulation. Managers and members of staff who need further information about the General Data Protection Regulation and the Library's Policy should contact the Library's Data Protection Officer and Human Resources Advisor to arrange appropriate training. The induction training given to all new members of staff will include awareness of the Regulation.

3.9 Staff should direct any internal enquiries relating to the processing of Personal Data to the Deputy DPO.

STAFF RESPONSIBILITIES: DATA SECURITY

4.1 It is a requirement of the Regulation that the Library Processes Personal Data securely. All staff are responsible for ensuring that:

- any Personal Data which they hold, whether in electronic or paper format, is kept, used, and, when appropriate, deleted securely at all

times; and

- personal information is not disclosed either orally or in writing, accidentally or otherwise to any unauthorised third party.

4.2 The technical measures taken by the Library to ensure that information is processed securely is described in the Information Security Policy and related sub-policies and procedures.

4.3 Each Data Protection Co-ordinator has a leading role in ensuring that appropriate technical and organisational measures are taken within their departments to ensure against unauthorised or unlawful processing of Personal Data and against loss or destruction of, or damage to, such data. They are also responsible for keeping the DPO or Deputy DPO informed of changes in the collection, use or deletion of personal data in their department.

STAFF RESPONSIBILITIES AS DATA SUBJECTS

5.1 In relation to their own Personal Data, each individual member of staff is responsible for:

- ensuring that any information provided by them in relation to their employment is accurate and up to date;
- notifying the Human Resources Unit of any change to the information submitted by them e.g. change of address;
- notifying the Human Resources Unit of any inaccuracies or alterations.

DATA PROCESSORS

6.1 Data Processors must process Personal Data in accordance with the Library's Data Protection Policy and the related procedures. It must be ensured that a Data Processing Agreement is signed where appropriate.

RIGHTS OF DATA SUBJECTS

7.1 All Data Subjects, which include members of staff as well as users, have the right to

- know what Personal Data relating to them is held and processed by the Library and the reasons for doing so and receive a response within one month (Subject Access Request)
- prevent processing that is likely to cause damage or distress;

- prevent processing for direct marketing;
- prevent automated decision making;
- claim compensation for misuse of their Personal Data;
- take action to deal with misuse or inaccuracies.
- take action to have any personal data deleted or removed where there is no compelling reason for its continued processing; certain exemptions exist (Article 17)

7.2 Any person who wishes to exercise the above rights is asked to submit a Subject Access Request in writing to the DPO. Individuals wishing to submit a Subject Access Request are requested to use the Library's Subject Access Request Form which can be sent either as an e-mail attachment or by post (using recorded delivery) to the DPO.

7.3 There is no charge for making a subject access request. Also, the DPO will require documents from the individual to establish his/her identity and confirm his/her address as well as details as to where they believe the requested information is held. This information should be submitted with the Subject Access Request Form to avoid delay. The receipt of the Form will be acknowledged by the Library.

7.4 The Library aims to comply with requests for access to Personal Data as quickly as possible, but will ensure that it is provided within one month unless there is good reason for the delay. In such cases the reason for delay will be explained in writing to the Data Subject making the request.

OBLIGATIONS OF LIBRARY USERS

8.1 Library users should ensure that all personal data supplied to the Library is accurate and up-to-date, and notify the Library of any changes (e.g. their home address).

8.2 Users who handle Personal Data contained in the Library's collections must adhere to clause 10.1 of this Policy.

CLOSE CIRCUIT TELEVISION (CCTV)

9.1 The Library uses close circuit cameras on the Library's premises for the purpose of security and safety. The cameras are used in accordance with the Information Commissioner Office's guidelines and more information about

the Library's use of close circuit cameras can be found in the CCTV Policy.

PERSONAL DATA AND THE LIBRARY'S COLLECTIONS

10.1 The Regulation may apply to collections that contain information about people who may still be living (depending on the way in which the information has been structured). Users who use these collections must ensure that:

- the subject of their research is informed of the nature of the research and has given consent to their Personal Data being used;
- the Deputy DPO is informed of the proposed research prior to its commencement; and that
- all information is kept securely.

10.2 In the case of bequests, donations and purchases, ownership of the items in question passes to the Library, and unless there is explicit provision to the contrary, the Library becomes the Data Controller with primary responsibility for compliance with the Regulation.

10.3 In the case of deposits, whereby custody passes to the Library but ownership remains with the depositor, the Library will act as Data Processor. A contract will be signed between the Library and the depositor stating that the depositor remains the Data Controller, unless there is explicit provision to the contrary.

10.4 All depositors must have a clear understanding of their continuing interest in the records. This will be clearly stipulated in the deposit agreement or in amendments to existing agreements.

POLICY REVIEW

11.1 This Policy will be reviewed every three years unless there is a change in the Regulation, the guidance published by the Information Commissioner's Office or another specified reason for undertaking a review. The Information Compliance Committee shall oversee the review and amendments shall be approved by the Executive Team.

This policy is available in Welsh and English.

END