The Chester Beatty Library Data Protection Policy

Introduction

The purpose of this document is to provide a concise policy statement regarding the Data Protection obligations of the Chester Beatty Library (CBL). This includes obligations in dealing with personal data, in order to ensure that the organisation complies with the requirements of the relevant Irish legislation.

Rationale

The CBL must comply with the Data Protection principles set out in the relevant legislation. This Policy applies to all Personal Data collected, processed and stored by CBL in relation to its staff, service providers and clients in the course of its activities. The CBL makes no distinction between the rights of Data Subjects who are employees, and those who are not. All are treated equally under this Policy.

Scope

The policy covers both personal and sensitive personal data held in relation to data subjects by CBL. The policy applies equally to personal data held in manual and automated form.

All Personal and Sensitive Personal Data will be treated with equal care by CBL. Both categories will be equally referred to as Personal Data in this policy, unless specifically stated otherwise.

This policy should be read in conjunction with the associated Subject Access Request procedure, the Records Management Policy and the Data Loss Notification Procedure.

The Chester Beatty Library as a Data Controller

In the course of its daily organisational activities, CBL acquires, processes and stores personal data in relation to:

- Employees of CBL
- Visitors and users of CBL services
- Third party service providers engaged by CBL

In accordance with the Irish Data Protection legislation, this data must be acquired and managed fairly. Not all staff members will be expected to be experts in Data Protection legislation. However, CBL is committed to ensuring that its staff have sufficient awareness of the legislation in order to be able to anticipate and identify a Data Protection issue, should one arise. In such circumstances, staff must ensure that the Data Protection Officer is informed, and in order that appropriate corrective action is taken.

Due to the nature of the services provided by CBL, there is regular and active exchange of personal data between CBL and its Data Subjects. In addition, CBL exchanges personal data with Data Processors on the Data Subjects' behalf.

This is consistent with CBL's obligations under the terms of its contract with its Data Processors.

This policy provides the guidelines for this exchange of information, as well as the procedure to follow in the event that a Library staff member is unsure whether such data can be disclosed.

In general terms, the staff member should consult with the Data Protection Officer to seek clarification.

Subject Access Requests

Any formal, written request by a Data Subject for a copy of their personal data (a Subject Access Request) will be referred, as soon as possible, to the Data Protection Officer, and will be processed as soon as possible.

It is intended that by complying with these guidelines, CBL will adhere to best practice regarding the applicable Data Protection legislation.

Third-Party processors

In the course of its role as Data Controller, CBL engages a number of Data Processors to process Personal Data on its behalf. In each case, a formal, written contract is in place with the Processor, outlining their obligations in relation to the Personal Data, the specific purpose or purposes for which they are engaged, and the understanding that they will process the data in compliance with the Irish Data Protection legislation.

The Data Protection Principles

The following key principles are enshrined in Irish legislation and are fundamental to CBL's Data Protection policy.

In its capacity as Data Controller, CBL ensures that all data shall:

1. Be obtained and processed fairly and lawfully

For data to be obtained fairly, the data subject will, at the time the data are being collected, be made aware of:

- The identity of the Data Controller (CBL)
- The purpose(s) for which the data is being collected
- The person(s) to whom the data may be disclosed by the Data Controller
- Any other information that is necessary so that the processing may be fair.

The CBL will meet this obligation in the following way:

- Where possible, the informed consent of the Data Subject will be sought before their data is processed;
- Where it is not possible to seek consent, CBL will ensure that collection of the data is justified under one of the other lawful processing conditions – legal obligation, contractual necessity, etc.;
- Where CBL intends to record activity on CCTV or video, a Fair Processing Notice will be posted in full view;
- Processing of the personal data will be carried out only as part of CBL's lawful activities, and CBL will safeguard the rights and freedoms of the Data Subject;
- The Data Subject's data will not be disclosed to a third party other than to a party contracted to CBL and operating on its behalf.

2. Be obtained only for one or more specified, legitimate purposes

The CBL will obtain data for purposes which are specific, lawful and clearly stated. A Data Subject will have the right to question the purpose(s) for which CBL holds their data, and CBL will be able to clearly state that purpose or purposes.

3. **Not be further processed in a manner incompatible with the specified purpose(s)**

Any use of the data by CBL will be compatible with the purposes for which the data was acquired.

4. **Be kept safe and secure**

The CBL will employ high standards of security in order to protect the personal data under its care. Appropriate security measures will be taken to protect against unauthorised access to, or alteration, destruction or disclosure of any personal data held by CBL in its capacity as Data Controller.

Access to and management of staff and visitor/user records is limited to those staff members who have appropriate authorisation and password access.

5. **Be kept accurate, complete and up-to-date where necessary**

The CBL will:

- ensure that administrative and IT validation processes are in place to conduct regular assessments of data accuracy;
- conduct periodic reviews and audits to ensure that relevant data is kept accurate and up-to-date. The CBL conducts a review of sample data every 12 months to ensure accuracy; staff contact details and details on next-of-kin are reviewed and updated every two years;
- conduct regular assessments in order to establish the need to keep certain Personal Data.

6. **Be adequate, relevant and not excessive in relation to the purpose(s) for which the data were collected and processed**

The CBL will ensure that the data it processes in relation to Data Subjects are relevant to the purposes for which those data are collected. Data which are not relevant to such processing will not be acquired or maintained.

7. **Not be kept for longer than is necessary to satisfy the specified purpose(s)**

The CBL has identified an extensive matrix of data categories, with reference to the appropriate data retention period for each category. The matrix applies to data in both a manual and automated format.

Once the respective retention period has elapsed, CBL undertakes to destroy, erase or otherwise put this data beyond use.

8. **Be managed and stored in such a manner that, in the event a Data Subject submits a valid Subject Access Request seeking a copy of their Personal Data, this data can be readily retrieved and provided to them**

The CBL has implemented a Subject Access Request procedure to manage such requests in an efficient and timely manner, within the timelines stipulated in the legislation.

Data Subject Access Requests

As part of the day-to-day operation of the organisation, CBL's staff engage in active and regular exchanges of information with Data Subjects. Where a formal request is submitted by a Data Subject in relation to the data held by CBL, such a request gives rise to access rights in favour of the Data Subject.

There are specific time-lines within which CBL must respond to the Data Subject, depending on the nature and extent of the request. These are outlined in the attached Subject Access Request process document.

CBL's staff will ensure that, where necessary, such requests are forwarded to the Data Protection Officer in a timely manner, and they are processed as quickly and efficiently as possible, but within not more than 30 days from receipt of the request.

Implementation

As a Data Controller, CBL ensures that any entity which processes Personal Data on its behalf (a Data Processor) does so in a manner compliant with the Data Protection legislation.

Failure of a Data Processor to manage CBL's data in a compliant manner will be viewed as a breach of contract, and will be pursued through the courts.

Failure of CBL's staff to process Personal Data in compliance with this policy may result in disciplinary proceedings.

Definitions

For the avoidance of doubt, and for consistency in terminology, the following definitions will apply within this Policy.

Data	This includes both automated and manual data. Automated data means data held on computer, or stored with the intention that it is processed on computer. Manual data means data that is processed as part of a relevant filing system, or which is stored with the intention that it forms part of a relevant filing system.
Personal Data	Information which relates to a living individual, who can be identified either directly from that data, or indirectly in conjunction with other data which is likely to come into the legitimate possession of the Data Controller. (If in doubt, CBL refers to the definition issued by the Article 29 Working Party, and updated from time to time.)
Sensitive Personal Data	A particular category of Personal data, relating to: Racial or Ethnic Origin, Political Opinions, Religious, Ideological or Philosophical beliefs, Trade Union membership, Information relating to mental or physical health, information in relation to one's Sexual Orientation, information in relation to commission of a crime and information relating to conviction for a criminal offence.
Data Controller	A person or entity who, either alone or with others, controls the content and use of Personal Data by determining the purposes and means by which that Personal Data is processed.
Data Subject	A living individual who is the subject of the Personal Data, i.e. to whom the data relates either directly or indirectly.
Data Processor	A person or entity who processes Personal Data on behalf of a Data Controller on the basis of a formal, written contract, but who is not an employee of the Data Controller, processing such Data in the course of his/her employment.
Data Protection Officer	A person appointed by CBL to monitor compliance with the appropriate Data Protection legislation, to deal with Subject Access Requests, and to respond to Data Protection queries from staff members and service recipients
Relevant Filing System	Any set of information in relation to living individuals which is not processed by means of equipment operating automatically (computers),

	and that is structured, either by reference to individuals, or by reference to criteria relating to individuals, in such a manner that specific information relating to an individual is readily retrievable.

The Chester Beatty Library - Data Loss Notification Procedure

Introduction:

The purpose of this document is to provide a concise procedure to be followed in the event that the Chester Beatty Library (CBL) becomes aware of a loss of personal data. This includes obligations under law.

Rationale:

The response to any breach of personal data (as defined by the legislation) can have a serious impact on CBL's reputation and the extent to which the public perceives the CBL as trustworthy.

The consequential impact on the commercial brand can be immeasurable. Therefore, exceptional care must be taken when responding to data breach incidents. Not all data protection incidents result in data breaches, and not all data breaches require notification. This guide is to assist staff in developing an appropriate response to a data breach based on the specific characteristics of the incident.

Scope:

The policy covers both personal and sensitive personal data held by CBL. The policy applies equally to personal data held in manual and automated form.

All Personal and Sensitive Personal Data will be treated with equal care by CBL. Both categories will be equally referred to as Personal Data in this policy, unless specifically stated otherwise.

This policy should be read in conjunction with the associated Data Protection Policy, Subject Access Request Procedure and Records Management Policy.

What constitutes a breach, potential or actual?

A breach is a loss of control, compromise, unauthorised disclosure, unauthorised acquisition, unauthorised access, or any similar term referring to situations where persons other than authorised users, for an authorised purpose, have access or potential access to personal data in usable form, whether manual or automated.

This could mean:

- Loss of a laptop, memory stick or mobile device that contains personal data
- Lack of a secure password on PCs and applications
- Emailing a list of users/visitors to a third party in error
- Giving a system login to an unauthorised person
- Failure of a door lock or some other weakness in physical security which compromises personal data

What happens if a breach occurs?

Actual, suspected, or potential breaches should be reported immediately to CBL's Data Protection Officer (DPO).

A team comprising the DPO and other relevant staff will be established to assess the breach and determine its severity. Depending on the scale and sensitivity of data lost and the number of Data Subjects impacted, the Office of the Data Protection Commissioner and relevant regulatory bodies will be informed as quickly as possible following detection.

In certain circumstances CBL may (e.g. if required by the Office of the Data Protection Commissioner), inform the data subjects of the loss of their data and provide them with an assessment of the risk to their privacy. The CBL will make recommendations to the data subjects which may minimise the risks to them. The CBL will then implement changes to procedures, technologies or applications to prevent a recurrence of the breach.

Any employee who becomes aware of a likely data breach and fails to notify the DPO will be subject to CBL's disciplinary procedure.

When will the Office of the Data Protection Commissioner be informed?

All incidents in which personal data has been put at risk will be reported to the Office of the Data Protection Commissioner. The only exceptions to this policy are when the data subjects have already been informed, where the loss affects fewer than 100 data subjects, and where the loss involves only non-sensitive, non-financial personal data.

Where devices or equipment containing personal or sensitive personal data are lost or stolen, the Data Protection Commissioner is notified only where the data on such devices is not encrypted.

Data Loss Incident logging:

All data breaches will be recorded in an incident log as required by the Office of the Data Protection Commissioner. The log will maintain a summary record of each incident which has given rise to a risk of unauthorised disclosure, loss, destruction or alteration of personal data. The record will include a brief description of the nature of the incident and an explanation of why the Office of the Data Protection Commissioner was not informed. Such records will be provided to the Office of the Data Protection Commissioner upon request.