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.