The Company] Data Loss Notification Procedure

Introduction:

The purpose of this document is to provide a concise procedure to be followed in the event that [the Company] becomes aware of a loss of personal data. This includes obligations under law, namely the Irish Data Protection Act (1988), and the Irish Data Protection (Amendment) Act (2003).

The procedure is consistent with the guidelines issued by the Irish Data Protection Commissioner in 2010, and enshrined in Irish law.

Rationale:

The response to any breach of personal data (as defined by the legislation) can have a serious impact on [The Company]'s reputation and the extent to which the public perceives [The Company] 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 [The Company]. 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 [the Company]. 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, the Data Retention and Destruction Policy and the Data Retention Periods List.

What constitutes a breach, potential or actual?

A breach is a loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users, for an authorized 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 pc's and applications
- Emailing a list of students to someone 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 [the Company]'s Data Protection Officer (DPO) or IT Administrator (ITA).

Any employee who becomes aware of a likely data breach and fails to notify the DPO or IT Administrator will be subject to [The Company]'s disciplinary procedure.

A team comprising the DPO, ITA 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 [The Company] 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 Company] will make recommendations to the data subjects which may minimise the risks to them. [The Company] will then implement changes to procedures, technologies or applications to prevent a recurrence of the breach.

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.

Related Policies and Procedures:

- YYYYMMDD_Subject Access Request Procedure
- YYYYMMDD_Data Retention and Destruction Policy
- YYYYMMDD_Data Retention Periods List
- YYYYMMDD_Data Loss Incident Log