Lews Castle College UHI

Personal Data Breach Procedure

Contents

1. Introduction

This guidance supplements the College's Data Protection Policy. It sets out how the College will meet its obligations in the event of a data breach.

The guidance applies to all members of staff. All staff will be made aware of the guidance, and it will be made available both on the shared drive for staff policies and procedures and on the LCC website. All new members of staff will be made aware of the guidelines as part of their induction arrangements.

The guidance applies to contractors and agents acting for or on behalf of the College who may come into contact with personal data, and will be included in the College Contractor's Induction Programme.

2. What is a Data Breach?

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. It includes breaches that are the result of both accidental and deliberate causes. Personal data breaches can include:

- Access by an unauthorised third party
- Deliberate or accidental action (or inaction) by a data controller
- Sending personal data to an incorrect recipient
- Computing devices containing personal data being lost or stolen
- Alteration of personal data without permission
- Loss of availability of personal data, in digital or paper form

3. Reporting a Breach or Possible Breach

The GDPR introduces a duty on all organisations to report certain types of personal data breach to the Information Commissioner's Office within 72 hours of becoming aware of the breach.

All staff have a responsibility to report a data breach or a potential breach **as soon as they become aware of it**.

Any breach or potential breach should be reported to the Data Protection Officer (DPO), James Nock. This should be done by email to: dataprotectionofficer@uhi.ac.uk. This should be copied to the Principal as Data Controller, email sue.macfarlane@uhi.ac.uk

If email cannot be accessed, the telephone contact details for the Data Protection Officer are 013435 76813 mobile 07766 366765.

The Data Protection Officer works as part of a shared service arrangement. This means that cover is available during periods of absence on leave. If the DPO mailbox is not being monitored, an alternative email address will be available from the 'out of office' function on the account.

The information required at this first stage of reporting includes the following. Provide as much information as you can at this stage, but do not waste time gathering details.

a. When did the incident happen?
b. How did the incident happen?
c. If there has been a delay in reporting the incident, please explain the reasons for this
d. What personal data has been placed at risk?
e. Please specify if any financial or sensitive personal data (special categories*) has been affected, and provide details.
f. How many individuals have been affected, and how many data records are involved?
g. Are the affected individuals aware that the incident has occurred?
h. What measures were in place to prevent an incident of this nature occurring?

*Sensitive data or special categories includes information that would reveal: racial or ethnic origin; political opinions; religious or philosophical beliefs; trade-union membership; genetic; biometric; health; sex life or sexual orientation.

4. Containment and Recovery

The Data Protection Officer will undertake an impact assessment to identify measures required to contain or limit potential damage, and recover from the incident. The Data Protection Officer will liaise as required with the Principal and members of the College Management Team to ensure appropriate action is taken.

All staff are required to co-operate fully with actions identified by the Data Protection Officer in response to a data security breach.

5. Risk Assessment

Following immediate containment and recovery, the DPO will assess the risks associated with the breach including the potential adverse consequences to the individuals affected, and taking into account:

- The type of data involved
- Whether the data is sensitive
- If data has been lost or stolen, whether encryption protections are in place
- What has happened to the data, such as the possibility that it may be used to cause harm to the individual
- The level of detail that would be exposed and how this could affect the individual

6. Notification of Data Breaches

Following the Impact Assessment, the DPO will notify as required:

- Individuals affected by the breach
- The Information Commissioner's Office
- Other regulatory bodies
- Third parties such as the Police or bank or building societies

Any breaches that need to be reported to the Information Commissioner's Office will, where feasible, be reported within 72 hours of becoming aware of the breach.

7. Evaluation and Response

The DPO will maintain a record of data breaches, both actual and potential. Responses to any data breach, whether actual or potential, will be evaluated by the DPO in terms of their effectiveness.

Summary reports on any data breaches and responses to them will be included in data protection monitoring reports provided to the Board of Management.

8. Staff Responsibilities

All staff who are involved in processing data have a duty of care to ensure that data is processed in accordance with data protection principles. Processing includes obtaining, recording, holding and storing information and carrying out any operations on the data, including adaptation, alteration, use, disclosure, transfer, erasure and destruction.

All staff are required to comply with the ICT Acceptable Use and Information Security policies.

Any member of staff who identifies an actual or potential data breach must report it immediately following the procedures set out above.

All staff are required to co-operate fully with actions identified by the Data Protection Officer in response to a data security breach.

9. Related Policies and Procedures

Data Protection Policy
ICT Acceptable Use and Information Security Policies
Retention Schedule