

Data Breach Incident and Notification Policy



INTRODUCTION

Lady Margaret Hall utilises various information systems and holds a large amount of data/information which may include personal or sensitive personal information.

Care should be taken to protect these information assets from incidents (either accidentally or deliberately) that could compromise their security.

In the event of a suspected data breach, it is vital that appropriate actions are taken to minimise associated risks.

PURPOSE

The purpose of this policy is to set out the procedure that should be followed to ensure a consistent and effective approach is in place for managing data breach incidents across Lady Margaret Hall.

SCOPE

This policy applies to all Lady Margaret Hall staff, students, contractors and third party agents handling College and University information assets.

RELATIONSHIP WITH OTHER POLICIES

This Policy is related to the College Information Security Policy.

RESPONSIBILITIES

All users of Lady Margaret Hall information assets are required to familiarise themselves and comply with this policy.

All individuals who access, use or manage Lady Margaret Hall's information are responsible for reporting data breach incidents immediately to the ICT Manager and DPO.

COMPLIANCE

Lady Margaret Hall has an obligation to comply with relevant statutory, legal and contractual requirements. The Data Breach Incident and Notification Policy is part of the Information Security suite of policies, designed to ensure data breach and information security incidents are reported promptly and managed properly to mitigate any risks to the confidentiality, integrity and availability of College information and information systems.

Failure to adhere to this policy will be addressed by necessary disciplinary actions in accordance with Lady Margaret Hall's Disciplinary Procedures and relevant contractor and third party contractual clauses relating to non-conformance with the Information Security Policy and related policies.

DEFINITION OF AN INCIDENT

An incident in the context of this policy is an event which has caused or has the potential to cause damage to Lady Margaret Hall's information assets or reputation. Examples are:

Data Breach Incident and Notification

Policy

- Accidental loss or theft of confidential or sensitive data or equipment on which such data is stored (e.g. loss of paper record, laptop, iPad or USB stick)
- Unauthorised use, access to or modification of data or information systems (e.g. sharing of user login details (deliberately or accidentally) to gain unauthorised access or make unauthorised changes to data or information systems)
- Unauthorised disclosure of sensitive or confidential information (e.g. email sent to an incorrect recipient or document posted to an incorrect address or addressee)
- Compromised user account (e.g. accidental disclosure of user login details through phishing)
- Failed or successful attempts to gain unauthorised access to University information or information systems
- Equipment failure
- Malware infection
- Disruption to or denial of ICT services

INCIDENT REPORTING

1. At the point that a data breach is suspected, the person who has identified the incident must notify their line manager or head of department immediately. If the person has been the cause of the incident or part of a process that has led to the incident, the person should not continue with that process until investigation has completed.
2. The line manager or head of department must report the incident within an hour to the ICT Manager and the DPO (as the primary point of contact). The report should include full and accurate details of the incident, including who is reporting the incident, what type of incident it is, if the data relates to people, and how many people are involved. The DPO will keep a log of this information. The DPO contact details are dpo@lmh.ox.ac.uk, and phone 01865 274300.

INCIDENT INVESTIGATION

1. The DPO will work with the person reporting the incident and ICT Manager to investigate the potential breach. This investigation should take no more than 48 hours. The investigation will establish the nature of the incident, the type of data involved, and where personal data is involved, who the subjects are and how many personal records were breached. The investigation will consider the extent of a system compromise or the sensitivity of the data involved, and a risk assessment will be performed as to what might be the consequences of the incident, for instance whether harm could come to individuals or whether data access or ICT services could become disrupted or unavailable.
2. If the investigation finds a possible breach then depending on the importance of the breach the DPO may seek advice from the University. The Data Protection Officer reserves the right to seek the advice from the central University Information Security Team (IST) on any matter that is not trivial.
3. If the University security team are satisfied that the integrity of the University and the College are still intact, the breach can be dealt with internally. A review of internal procedure and process may be needed, or the University may ask for a more detailed investigation to be carried out, by an external company or the University's own security team.

BREACH NOTIFICATION

1. If it is agreed that a data breach has occurred, then the College DPO will inform the Head of House and then fill out a Breach Notification form for the IST. The IST will then alert the ICO and provide a copy of the Breach Notification form. This report will be issued within 72 hours of the incident notification.

Data Breach Incident and Notification Policy



2. Depending on the seriousness of the Breach, the Head of House will make the decision to inform any external organisation, such as the police or other appropriate regulatory body. The Head of House will also make the decision as to whether or not individuals whose personal data have been affected by the incident will be notified, to enable them take steps to protect themselves.

CONTAINMENT AND RECOVERY

The relevant individuals will determine the appropriate course of action and the required resources needed to limit the impact of the incident. This might require isolating a compromised section of the network, alerting relevant staff or shutting down critical equipment.

Appropriate steps will be taken to recover system or data losses and resume normal business operation. This might entail attempting to recover any lost equipment, using backup mechanisms to restore compromised or stolen data and changing compromised passwords.

Advice from experts across the University may be sought in resolving the incident promptly and appropriately.

REVIEW

Once the incident is contained, a thorough review of the event will be undertaken by the Estates Bursar or Head of House. The report will detail the root cause of the incident and contributory factors, the chronology of events, response actions, recommendations and lessons learned to identify areas that require improvement.

Recommended changes to systems, policies and procedures will be documented and implemented as soon as possible thereafter.

RELATED POLICIES, PROCESSES AND STANDARDS

<http://www.lmh.ox.ac.uk/about-lmh/further-information/privacy-and-data-protection>

Data Breach Incident and Notification Policy



DOCUMENT CHANGE LOG

Version	Date changed	Notes
1.0	16/05/2018	Version 1.0 published