



Exeter College Information Security Incident Management Policy

1. Purpose

Information Security Incidents can expose personal and sensitive College data to those who should not have access to this data, potentially causing reputational damage and the risk of incurring substantial fines. This policy covers the appropriate response of all members of the College when an incident occurs.

2. Scope

This policies apply to

- All members of the College (College staff, fellows, other academic staff, students and other individuals considered as members or affiliates) with access to the College network or IT facilities.

3. Definition

An information security incident is defined as:

“An event whereby any service or information stored or processed by the College has been, or potentially has been lost, destroyed, altered, copied, transmitted, stolen, used or accessed unlawfully or by unauthorised individuals accidentally or on purpose.”

This includes but not limited to:

- The loss or theft of any device, personal or College owned, storing College data or a University email account
- The loss or theft of any device, personal or College owned, with a VPN client to connect to the University or College VPN
- An attempt by unauthorised persons to gain access to data or computer systems of the College or University
- The presence of a computer virus or ransomware on any device that has access to the College or University network systems
- A user account compromised by phishing scam
- Email containing personal data sent in error to the wrong recipient
- Loss of a University Card
- Loss of any staff or student or alumni paper-based records

4. Reporting

- 4.1. All incidents or suspected incidents must be reported to InfoSec@exeter.ox.ac.uk as soon as a risk is identified, ideally within 24hrs. Where a loss of personal or sensitive data may have occurred, this must be reported no later than 24hrs but ideally as soon as the loss is noticed. Where a loss or theft is reported to a regulatory body such as the police or the British Transport, a copy of the report must be submitted to the IT department.
- 4.2. The report should include full and accurate details of the incident containing:
 - The nature of the incident (theft or loss of equipment, hacking, etc.)
 - What type of data (not the data itself) was involved
 - Details of any 3rd parties involved
- 4.3. The Computing team will record and log the incident.

5. Investigation

- 5.1. The **IT Manager** will act as the Incident Manager.
- 5.2. The Incident Manager will perform an initial investigation into the incident as soon as practically possible upon receipt of the incident being reported. The Incident Manager will establish the:
 - nature of the incident
 - classify the incident, for workflow response
 - if personal or sensitive data has been exposed the College should identify the associated individual(s)
 - Assess any risks to the College data, the College network and servers, and to the College overall, and the impact of the risks
 - any legal or commercial consequences
- 5.3. The Incident Manager will instigate a Response Team if appropriate and the Incident Manager Role may be transferred to other officers of the College, as necessary, including the **College Data Protection Officer (DPO)**.
- 5.4. Where a breach of personal or sensitive data has happened then the DPO must be informed.

6. Response

- 6.1. The Incident Response Team will determine the appropriate course of action and resources required to limit the impact of any data breach. This may mean isolating devices and servers from the network, or making entire networks or services unavailable.
- 6.2. The Incident Manager must inform the University Information Security team and obtain any specialist advice on how best to respond.
- 6.3. The Incident Manager will record all actions taken and decisions made in the incident log.
- 6.4. Where criminal activity may have taken place then all efforts will be made to preserve evidence; this may take precedence over system recovery.
- 6.5. Appropriate steps will be taken to recover the data or restore services to resume to “business as normal” state.
- 6.6. Named individuals exposed in any data breach must be contacted with details of the incident and any risks to them.
- 6.7. College staff should not pressurise the Incident Response Team or the IT Department to restore services at the expense of due diligence in carrying out their duties.

7. Review

- 7.1. The IT Department will review each incident to identify new risks, new response work flows, and changes to procedures or policies required to prevent similar incidents and to highlight any non-conformance with policy, which may result in disciplinary proceedings.
- 7.2. The review will be forwarded to Finance & Estates Bursar for evaluation by the IT Committee and to take a proposal to the Governing Body if a change to policy is recommended.

8. Responsibilities

- The **End User** is responsible for reporting all incidents to the Computing Team.
- The **IT Department** is responsible for recording all security incidents; limiting spread of incidents and containing data loss; and implementing technical controls to prevent security incidents.
- The **IT Committee** is responsible for reviewing incidents and recommending changes to Governing Body.
- **Governing Body** is responsible for approving changes to policy in light of security incidents

Document Control

Date Approved	16 th May 2018
Last Review Date	16 th May 2018
Policy Owner	IT Manager

Version History

1.1	Approved	16 th May 2018
-----	----------	---------------------------