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 (see Exeter College Mobile Device Security Policy)
- The loss or theft of any device, personal or College owned, with a VPN client to connect to the University or College VPN (see Exeter College Mobile Device Security Policy)
- 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 Exeter IT at InfoSec@exeter.ox.ac.uk **immediately**.

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

Where a loss or theft is reported to a regulatory body such as the Police or British Transport, a copy of the report must be submitted to Exeter College IT Department.

4.3 Where the information security incident may have resulted in a breach of personal or sensitive data, no matter how small, this must **ALSO** be reported to the College Data Protection Officer (DPO) at dataprotection@exeter.ox.ac.uk **immediately**.

4.3 Exeter College IT Department will record and log the incident. Where the information security incident may include a loss of personal data then a record will also be made by the College Data Protection Officer (DPO) on the College Data Breach Log.

5. Investigation

5.1. The **IT Manager** will act as the Incident Manager in the first instance and will instigate a Response Team (if appropriate). The Incident Manager Role may be transferred to other officers of the College, as necessary, including the College Data Protection Officer (DPO). Transfer of the role of Incident Manager to the College DPO will be appropriate in situations where the incident results in or could potentially result in a breach of personal data.

5.2 In consultation with the DPO, the Incident Manager (if that person is not the DPO) will perform an initial investigation into the incident within 24 hours upon receipt of the incident being reported. The Incident Manager will :

- establish the nature of the incident
- classify the incident, for workflow response
- assess any risks to the College data, the College network and servers, and to the College overall, and the impact of the risks
- consider any legal or commercial consequences and decide if insurers need to be notified
- if personal or sensitive data has been or potentially has been exposed the College DPO should:
  - identify the associated individual(s) and compile an audit of all affected data subjects and decide if they need to be informed of the breach
  - contact the University Information Compliance Team where the breach also involves University data,
  - Decide if the matter should be reported to the ICO (if it does then this will need to happen within **72 hours** of the breach being identified).

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.

6.8 Report the incident to the ICO, if a decision was made to do so, within **72 hours**.

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 DPO has overall responsibility for reviewing all reported incidents which may have caused a data breach and for deciding on the appropriate actions, including whether to notify data subjects who may have been affected and whether or not to report the incident to the ICO.
- 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	19th June 2019
Last Review Date	04th June 2019
Policy Owner	IT Manager

Version History

1.1	Approved by Governing Body	16th May 2018
1.2	Approved by Governing Body (College Order 19/103)	19th June 2019