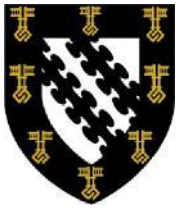

Information Security Policy

1. Purpose

The purpose of this policy is to provide a framework for Information Security at Exeter College and outlines the College's approach for all Information Security principles and define responsibilities.

2. Scope

This policy is applicable across **Exeter** College and individually applies to:

- all individuals who have access to **Exeter College** information and technologies;
- all facilities, technologies and services that are used to process **Exeter College** information;
- information processed, in any format, by **Exeter College** pursuant to its operational activities;
- internal and external processes used to process **Exeter College** information; and
- external parties that provide information processing services to **Exeter College**.

3. Objectives

Exeter College's objectives for information security are that:

a) a culture is embedded to ensure all teaching, research and administration activities consider information security;
b) individuals are aware of and are kept informed of their information security responsibilities;
c) information risks are identified, managed and mitigated to an acceptable level;
d) authorised users can access information securely to perform their roles;
e) facilities, technologies and services adequately balance usability and security;
f) implemented security controls are pragmatic, effective and measurable;
g) contractual, regulatory and legal obligations relating to information security are met; and
h) incidents are effectively managed and resolved, and learnt from to improve information security.

4. Information Security Policy Framework (ISPF)

Information is critical to **Exeter College** operations and failure to protect information increases the risk of financial and reputational losses. Exeter College is committed to protecting information, in all its forms, from loss of **confidentiality**, **integrity** and **availability** ensuring that:

a) All college members are appropriately trained in Information Security and in particular that **all** staff complete information security training (as a minimum this must include University of Oxford Information Security Awareness Module) and are familiar with all Exeter College Information Security Policies
b) information security risk is adequately managed and risk assessments on IT systems and business processes are performed where appropriate;
c) all relevant information security requirements of **Exeter College** are covered in agreements with any third-party partners or suppliers, and compliance against these is monitored;

d) appropriate information security controls are implemented to protect all IT facilities, technologies and services used to access, process and store **Exeter College** information;

e) all information security incidents are reported in a timely manner via appropriate management channels, information systems are isolated, and incidents properly investigated and managed;

f) Information Asset Owners are identified for all **Exeter College** information assets, assets are classified according to how critical and sensitive they are, and rules for their use are in place; and

g) Information security controls are monitored to ensure they are adequate and effective.

To provide the foundation of a pragmatic information security framework, **Exeter College** will implement a set of minimum information security controls, known as the baseline, either as published by the University's Information Security team or of equivalent strength. Where research, regulatory or national requirements exceed this baseline, controls will be increased at necessary service or project level. Where it is not possible or practicable to meet the baseline, exceptions will be documented to justify the deviation and appropriate compensating controls will be put in place. The baseline will support **Exeter College** in achieving its information security objectives.

The policy and the baseline shall be communicated to users and relevant external parties, and linked to from a website.

5. Responsibilities

The following bodies and individuals have specific information security responsibilities:

- **The Rector** is accountable for the effective implementation of this information security policy, and supporting information security rules and standards, within **Exeter College**.
- **Governing Body** has executive responsibility for information security within **Exeter College**. Specifically, **Governing Body** has responsibility for overseeing the management of the security risks to **Exeter College's** staff and students, its infrastructure and its information.
- **The Finance & Estates Bursar** is responsible for establishing and maintaining **Exeter College's** information security management framework to ensure the availability, integrity and confidentiality of **Exeter College's** information. The Finance & Estates Bursar will lead on the definition and implementation of Exeter College's information security arrangements.
- **The IT Manager** has responsibility for implementing and managing the IT technical controls.
- **Users** are responsible for making informed decisions to protect the information that they process.

6. Compliance

Exeter College shall conduct information security compliance and assurance activities, facilitated by the Conference of Colleges Information Security Working Group, to ensure information security objectives and the requirements of the ISPF are met. Wilful failure to comply with the policy and baseline will be treated extremely seriously by **Exeter College** and may result in enforcement action on a group and/or an individual.

Review and Development

This policy, and supporting ISPF documentation, shall be reviewed and updated by The Bursar and approved by **Governing Body** on a regular basis to ensure that they:

- remain operationally fit for purpose;
- reflect changes in technologies;

- are aligned to industry best practice; and
- support continued regulatory, contractual and legal compliance.

This Information Security Policy should be read in conjunction with the following Colleges policies on

- Exeter College Acceptable Use Policy
- Exeter College Mobile Device Security Policy
- Exeter College Information Security Incident Management Policy
- Data Protection Policy

Internal:

- Exeter College Change Management Policy (IT)

By College Order 22/070, this policy was approved by Governing Body on 15th June 2022 with immediate effect, and is to be reviewed by 30th June 2026, and was also approved for display on the website.