WADHAM
COLLEGE
UNIVERSITY OF OXFORD

Wadham College

Information Security Policy

Contents

1. Purpose........ 1
2. Scope........ 2
3. Objectives........ 2
4. Information Security Policy Framework (ISPF)........ 2
5. Responsibilities........ 3
6. Compliance........ 3
7. Review and Development........ 3

Revision history

Version	Date	Changes & Approvals
0.1	22 May 2018	Draft for Finance Committee approval
1.0	23 May 2018	Approved for publication by Governing Body

1. Purpose

This policy outlines Wadham College's approach to information security management and provides the guiding principles and responsibilities to ensure Wadham College's security objectives are met.

2. Scope

This policy is applicable across Wadham College and individually applies to:

- all individuals who have access to Wadham College information and technologies, including students, Fellows, staff, Lecturers, SU/MCR members and affiliate members;
- all facilities, technologies and services that are used to process Wadham College information;
- information processed, in any format, by Wadham College pursuant to its operational activities;
- internal and external processes used to process Wadham College information; and
- external parties that provide information processing services to Wadham College.

3. Objectives

Wadham College's objectives for information security are that:

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

4. Information Security Policy Framework (ISPF)

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

- all staff complete information security awareness training;
- information security risk is adequately managed and risk assessments on IT systems and business processes are performed where appropriate;
- all relevant information security requirements of Wadham College are covered in agreements with any third-party partners or suppliers, and compliance against these is monitored;
- appropriate information security controls are implemented to protect all IT facilities, technologies and services used to access, process and store Wadham College information;
- all information security incidents are reported in a timely manner via appropriate management channels, information systems are isolated, and incidents properly investigated and managed;
- Information Asset Owners are identified for all Wadham College information assets, assets are classified according to how critical and sensitive they are, and rules for their use are in place; and

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

To provide the foundation of a pragmatic information security framework, Wadham 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 Wadham 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 the website.

5. Responsibilities

The following bodies and individuals have specific information security responsibilities:

- **The Warden** is accountable for the effective implementation of this information security policy, and supporting information security rules and standards, within Wadham College.
- **Governing Body** has executive responsibility for information security within Wadham College. Specifically, Governing Body has responsibility for overseeing the management of the security risks to Wadham College's staff and students, its infrastructure and its information.
- **The Data Protection Officer** is responsible for establishing and maintaining Wadham College's information security management framework to ensure the availability, integrity and confidentiality of Wadham College's information. The Data Protection Officer will lead on the definition and implementation of Wadham College's information security arrangements.
- **Users** are responsible for making informed decisions to protect the information that they process.

6. Compliance

Wadham 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 Wadham College and may result in enforcement action on a group and/or an individual.

7. Review and Development

This policy, and supporting ISPF documentation, shall be reviewed and updated by the Data Protection Officer and approved by Governing Body on an annual 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.

NOTE: This Information Security Policy should be read alongside other policy documents, handbooks and guides.