Information Security Policy

Overview

Users of ICT (Information and Communications Technology) within the University are subject in the first instance to the University regulations (2002) with subsequent amendments. This is available for review at: https://www.ox.ac.uk/about/how-we-are-run/governance-finance/legislation/it-regulations-1-of-2002

Balliol College has a statutory duty to comply with all relevant legal and regulatory obligations relating to the use of information and communication technologies. This includes, but is not limited to, duties under data protection, intellectual property, equality, safeguarding, and counter-terrorism legislation. Accordingly, the College reserves the right to monitor IT use where necessary to ensure compliance with the law and with the College's acceptable use policy. Any suspected breaches will be reviewed and investigated by an independent panel of Balliol College members.

The University regulations (2002) alone do not fully provide for all the needs of a security policy covering ICT services within the College. This security policy provides additional policies and guidelines which apply to its services and users of ICT services within the College. Effective security is a team effort involving the participation and support of every University/College employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these policies and guidelines, and to conduct their activities accordingly.

Policy was approved by Executive Committee: November 2025
Next review: MT 2028
Created by Christopher Thompson – ICT Director

Introduction

Balliol College seeks to maintain the confidentiality, integrity and availability of information about its staff, students, visitors, and alumni, and its affairs generally including any other sensitive information such as research data. It is extremely important to the College to preserve its reputation and the reputation of Oxford University and its integral parts. Compliance with legal and regulatory requirements with respect to this Information is fundamental.

Objective

This Information Security Policy defines the framework within which information security will be managed by the College and demonstrates management direction and support for information security across the College. This policy is meant to keep information secure and highlights the risks of unauthorised access or loss of data.

In support of this objective, all users of data assets, whether they are manual or electronic, accept their roles and responsibilities in ensuring information is protected and are committed to:

- Treating information security seriously
- Maintaining an awareness of security issues
- Adhering to applicable security policies / following applicable guidance

Information relating to living individuals (such as may be found in Personnel, Payrolls, and Student Record Systems) should only be stored in the appropriate secure systems and is subject to legal protection. All users of the ICT system are obliged, under the terms of the UK GDPR (General Data Protection Regulation), to ensure the appropriate security measures are in place to prevent any unauthorised access to personal data, whether this is on a workstation or on paper. Data also pertaining to research and other intellectual information, and deemed sensitive by the College, shall also have the same measures taken to safeguard it against unauthorised access and or theft.

Scope and definitions

The scope of this Information Security Policy extends to all Balliol College's information and its operational activities, including but not limited to:

- Records relating to pupils, students, alumni, staff, academic staff, visitors, conference guests, and external contractors where applicable
- Operational plans, accounting records, and minutes
- All processing facilities used in support of the College's operational activities to store, process, and transmit information
- Any information that can identify a person, e.g. names and addresses
- Any research or academic information deemed sensitive or with commercial value.
- All data assets whether they are physical (paper) or digital.

This policy covers all data access and processing pertaining to the College, and all staff and other persons (including students, Fellows, Lecturers, JCR/MCR members, and other officers of the college not already part of these groups) must be familiar with this policy and any supporting guidance. Any reference to staff shall be regarded as relating to permanent, temporary, contract, and other support staff as applicable.

Policy

Balliol College aims, as far as reasonably practicable, to:

- Protect the confidentiality, integrity, and availability of all data it holds in its systems. This includes the protection of any device that can carry data or access data, as well as protecting physical paper copies of data wherever possible (e.g., clean desk policies).
- Meet legislative and contractual obligations
- Protect the College's intellectual property rights
- Produce, maintain and test business continuity plans in regard to data backup and recovery
- Prohibit unauthorised use of the College's information and systems
- Communicate this Information Security Policy to all people potentially accessing data
- Provide information security training to all people appropriate to the role. Training resources are available via the university infosec team - https://www.ox.ac.uk/about/digital/cybersecurity/cyber-security-training-at-oxford
- Report any breaches of information security, actual or suspected, to the Data Protection Coordinator (DPO) in a timely manner.

More detailed policy statements and guidance are provided within the Information Security Procedures document

Responsibilities

The Governing Body is responsible for establishing the framework, and to issue and review policy statements and procedures to support Balliol College and the Universities Ordinances and Regulations with which members of the University/College must comply.

Governing Body requires the relevant senior roles in College to be accountable for implementing an appropriate level of security control for the information owned by that department and processed by people accessing that data. Administrative staff are accountable to their heads of department and academic staff are accountable to the Senior Tutor.

Each person is accountable for operating an appropriate level of security control over the information and systems he/she uses to perform his/her duties.

Every user is required to obey all laws, including criminal, counterterrorism, copyright, defamation and obscenity laws. College will render all reasonable assistance to enforcement officials (Police and authorised University IT staff) for the investigation and prosecution of people using technology in violation of any law.

The College DPC (Data Protection Coordinator) is responsible for coordinating the management of information security, maintaining this Information Security Policy, and providing advice and guidance on its implementation.

It is noted that failure to adhere to this Policy may result in the College suffering potentially severe financial loss including fines, operational incapacity, and loss of reputation. Data access, processing, or destruction that fails to observe the provisions of this policy may result in disciplinary action.

The role of Data Protection Officer (DPO) is fulfilled by Moore ClearComm
6th Floor,9 Appold Street, London, EC2A 2AP, meagan.mirza@mooreclear.com

The role of College Data Protection Coordinator (DPC) is fulfilled by the Domestic Bursar.

Governance

This Policy will be reviewed regularly by the Data Protection Coordinator. Any changes will be approved by the appropriate authority. The policy will be reviewed at least once every three years by the Governing Body. The Governing Body remains responsible for ensuring appropriate resources are in place to achieve compliance with data protection laws in line with appropriate overall risk profile.

Annex: Additional information and definitions

Legal Definition of Personal Information

Personal data is defined as "…any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. [https://ico.org.uk]". Emails and contacts stored in an email system count as personal data, as do most CVs, references, and job applications.

Special category data is personal data which the UK GDPR classifies as more sensitive and needs more protection. Examples of special category data include race, ethnic origin, politics, religion, trade union membership, genetics, biometrics, health, sex life, sexual orientation.

Data Protection Principles

The data protection principles state that personal data shall be:

- processed (i.e. collected, handled, stored, disclosed, and destroyed) fairly, lawfully, and transparently. As part of this, the College must have a 'legal basis' for processing an individual's personal data (most commonly, the processing is necessary for the College to operate a contract with them, the processing is necessary to fulfil a legal obligation, the processing is in the legitimate interests of the College and does not override their privacy considerations, or they have consented to the processing);
- processed only for specified, explicit and legitimate purposes;
- adequate, relevant and limited;
- accurate (and rectified if inaccurate);
- not kept for longer than necessary; and
- processed securely.

Data Subject Rights

An individual's rights (all of which are qualified in different ways) are as follows:

- the right to be informed of how their personal data is being used. This right is usually fulfilled by the provision of 'privacy notices' (also known as 'data protection statements') which set out how an organisation plans to use an individual's personal data, who it will be shared with, ways to complain, and so on;
- the right of access to their personal data;
- the right to have their inaccurate personal data rectified;
- the right to have their personal data erased (right to be forgotten);
- the right to restrict the processing of their personal data pending its verification or correction;

- the right to receive copies of their personal data in a machine-readable and commonly-used format (right to data portability);
- the right to object: to processing (including profiling) of their data that proceeds under legal bases; to direct marketing; and to processing of their data for research purposes where that research is not in the public interest; and
- the right not to be subject to a decision based solely on automated decision-making using their personal data.

Accountability

The College is required under law to:

- comply with data protection law and hold records demonstrating this;
- implement policies, procedures, processes and training to promote data protection by design and by default;
- have appropriate contracts in place when outsourcing functions that involve the processing of personal data;
- maintain records of the data processing that is carried out across the College;
- record and report personal data breaches to the Information Commissioner's Office (ICO) within 72 hours of becoming aware;
- carry out, where relevant, data protection impact assessments on high risk processing activities;
- communicate with data subjects, when required;
- co-operate with the ICO as the UK regulator of data protection law; and
- respond to regulatory/court action and pay administrative levies and fines issued by the ICO.