Worcester College

Information Security Policy

Contents

The following policy has been approved by the Governing Body of Worcester College. All Fellows, staff, students, and others handling information assets related to Worcester College are required to comply with this policy. Support and guidance are offered by the College's IT department, which in turn is supported by the central university's information security "InfoSec" team.

Information Security is not a new requirement, and to a large extent the policy and accompanying procedures formalise and regularise existing good practice within the College and wider university.

This policy will be reviewed at least biennially or sooner in the case of an incident to ensure any new developments are covered and protected.

1. Introduction

Worcester College seeks to maintain the confidentiality, integrity and availability of information about its staff, students, fellows, members, visitors, alumni, and its affairs generally. 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.

2. Objective

The objective of this Information Security Policy is, as far as reasonably practicable, to protect all sensitive information assets from all threats, whether internal or external, deliberate or accidental.

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

a. Treating information security seriously;
b. Creating a security-positive work environment;
c. Implementing controls that are proportionate to risk.

Information relating to living individuals (such as may be found in Personnel, Payroll, Student Records Systems) should only be stored in appropriate secure systems and locations, and is subject to legal protection. All users of the information and any ICT system are obliged, under the terms of the Data Protection Act 2018, to ensure the appropriate security measures are in place to prevent any unauthorised access to personal data, whether this is on an electronic device or on paper.

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 unauthorized access to or loss of data.

3. Scope and definitions

The scope of this Information Security Policy extends to all the information of Worcester College and its operational activities including but not limited to:

a. Records relating to students, alumni, staff, fellows, members, visitors, conference guests and external contractors where applicable;
b. Operational plans, accounting records, and minutes;
c. All processing facilities used in support of the College's operational activities to store, process and transmit information;
d. Any information that can identify a person, e.g. names and addresses.

This policy covers all data access and processing pertaining to the College, and all staff and other persons (including but not limited to 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.

4. Policy

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

a. 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 copy of data wherever possible;
b. Meet legislative and contractual obligations;
c. Protect the College's intellectual property rights;

d. Produce, maintain and test business continuity plans in regards to data backup and recovery;
e. Prohibit unauthorised use of the College's information and systems;
f. Communicate this Information Security Policy to all persons potentially accessing data;
g. Provide information security training to all persons appropriate to their role;
h. Report any breaches of information security, actual or suspected, to the Data Protection Officer and IT Department in a timely manner.

More detailed policy statements and guidance are provided in Section 7 of this Policy.

5. Risk Assessment and the Classification of Information

The degree of security control required depends on the sensitivity or criticality of the information. The appropriate degree of control therefore is determined by a process of risk assessment, in order to identify and classify the nature of the information held, the adverse consequences of security breaches and the likelihood of those consequences occurring.

The risk assessment should identify the information assets of Worcester College; define the ownership of those assets; and classify them, according to their sensitivity and/or criticality to the College or University as a whole. In assessing risk, the College should consider the value of the asset, the threats to that asset and its vulnerability.

Where appropriate, information assets should be labelled and handled in accordance with their criticality and sensitivity. The College follows Oxford University's definition and handling rules, changing 'University' to 'College' and 'University of Oxford' to 'Worcester College, Oxford' in all cases relating to College information assets. These rules are available at https://www.infosec.ox.ac.uk/handling-information#collapse1722301 .

Where information assets are held on or accessed through a computer system, the University's Regulations and Policies applying to all users of University ICT facilities apply. This is available from the University website[1].

Information security risk assessments should be repeated periodically and carried out as required during the operational delivery and maintenance of the College's infrastructure, systems and processes.

Personal data must be handled in accordance with the data protection principles as set out in Article 5 of the General Data Protection Regulation (GDPR), the Data Protection Act 2018 (DPA) and in accordance with this policy. "Personal data" means data which relate to a living individual who can be identified from those data, or together with other information which the College holds, or may hold, and includes any expression of opinion about the individual and any indication of the intentions of the College or any other person in respect of the individual.

The Data Protection Act requires that appropriate technical and organisational measures are taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

A higher level of security should be provided for 'special category data', which is defined in the GDPR as data revealing racial or ethnic origins, political opinions, religious or philosophical beliefs, trade union membership; and the processing of genetic data, biometric data for the purpose of uniquely identifying someone, data concerning health, or data concerning an individual's sex life or sexual orientation. This would be assessed using a Data Protection Impact Assessment.

[1] https://governance.admin.ox.ac.uk/legislation/it-regulations-1-of-2002

6. Responsibilities

The Governing Body is ultimately responsible for ensuring compliance with this policy and all data breaches within Worcester College.

The Governing Body requires the head of each department or the relevant college officers to be accountable for implementing an appropriate level of security control for the information under their responsibility and processed by persons accessing that data on behalf of College.

The Data Protection Officer, supported by the IT Manager, 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 involve the College in serious financial loss, embarrassment, legislative action or loss of reputation. Data access or processing that fails to observe the provisions of this policy may result in disciplinary action.

7. Detailed Policies and Guidance

The following shall be complied with throughout Worcester College.

i. Access to Information and Information systems

Information assets shall be 'owned' by a named section within College. A list of information assets (the Information Asset Register), and their owners, shall be overseen by the Data Protection Officer. Within the information Asset Register, the following definitions apply:

- **Information Asset Owner ("IAO")**
  The IAO will usually be a senior manager or College Officer.
  IAO has local responsibility for data protection and information security compliance in their area/department. They are responsible for ensuring that information assets are managed appropriately to meet the requirements of the organisation, and that the risks and opportunities are monitored. They should classify information assets and ensure that all users are aware of and have confirmed their understanding of the handling rules. They must authorise access to information assets within their responsibility.

- **Information Asset Manager ("IAM")**
  The IAM will usually be a departmental head or manager who has day-to-day familiarity with the systems used to manage information.
  The IAM supports the IAO in complying with their duties regarding the processing of personal data. The IAM should be the first point-of-contact for the Records Manager ("RM") when the RM undertakes the annual Retention Schedule Review; and for the Data Protection Officer for the annual ROPA review.

Access to information shall be restricted to authorised users and shall be protected by appropriate physical and/or logical controls.

a. Physical controls for information and information processing assets shall include:
   - Locked storage facilities (supported by effective management of keys)
   - Locks on rooms which contain computer facilities
   - Securing of PCs and other devices to prevent theft
   - "Clean desk" policies
   - Encryption of data either transmitted or taken outside the College's properties

b. Logical controls for information and information processing assets shall include passwords for systems access.
c. Passwords and password management systems shall follow good practice for security and use the following techniques:
    - The use of strong authentication passwords;
    - Users to have the ability to change their passwords at any time;
    - Passwords to be changed at regular intervals. A system to be in place to automate and enforce this process.
d. Access privileges shall be allocated to users based on the minimum privileges required. Access privileges shall be authorised by the appropriate information or system owner.
e. Each user of the ICT system is responsible for the security of their own password. If a password of an account is suspected to have been compromised, the user must report the relevant incident to the IT team immediately and change all passwords on all systems.
f. Users must take particular care when disclosing information to third parties, to ensure that there is no breach of the Data Protection Act. The permission of the information asset owner should be sought before the release of personal or sensitive information.

To allow for potential investigations, access records should be kept for a minimum of six months, or for longer, where considered appropriate.

Information and system owners shall review access permissions on an annual basis.

Access to physical information assets – for example printed paper documents, and media containing information – shall be governed as appropriate by the same principles as above.

An appropriate leavers and joiners process shall be in place to ensure that all employees, contractors and third-party users have information access permissions revoked and return all of the College's assets in their possession upon termination of their employment, contract or agreement. Line managers are responsible for completing a leaver's checklist and communicating that list to appropriate departments.

The circumstances under which the College may monitor use of its ICT systems, and the levels of authorisation required for this to be done, are the same as those set out in the University's "Regulations Relating to the use of Information Technology Facilities".

Access to operating system commands and the use of system utilities - such as administrator privilege - that might be capable of overriding system and application controls, shall be restricted to those persons who are authorised to perform systems administration or management functions. Such privileges shall be authorised by the Data Protection Officer and IT Manager only in line with individual job roles and responsibilities.

ii. Visitors to the College

Visitors to the College should be provided with temporary credentials, which are disabled at the end of their term with the College.

iii. Use of Personal Computer Equipment and Removable Storage

Worcester College recognises that there may be occasions when staff need to use computing equipment not provided by the College to process information (including personal data). The use of such equipment is governed by the College directive on the use of Self-Managed Devices which can be found on the College website. Exceptions to this policy must be approved by the IT Manager and Data Protection Officer.

It is good practice and required that:

a. Privately owned computing equipment used to process College information or connect to Worcester College's network must have up-to-date anti-virus software installed and, if the computer is to be connected to the Internet, a firewall. Anti-virus software is provided by a site-license and can be used on all systems connected to the administered network and installed via the University's IT Services website.
b. The information on removable storage devices holding personal data should be protected from loss and/or theft. Information containing personal data that is to be saved onto removable storage or privately owned computing equipment shall be encrypted before storage. Appropriate encrypted storage devices or software needed for College purposes can be requested from the IT Department.
c. College information shall not be retained on removable storage devices longer than necessary.

iv. Email and Internet Use

The College's email systems are outsourced to the University's IT Services and are subject to their rules. Their information policy will take precedence.

Mass mailing users of address groups provided by the College are for college-related information only. This therefore excludes the use of the email system for advertising personal items for sale.

The College's policy and procedure on staff and student use of email and the Internet is included in the relevant handbooks.

v. Mobile Computing

This applies to any mobile hardware that is used to access Worcester College resources and networks, whether the device is owned by the user or by the college.

Users with laptop computers and other mobile computing devices shall take all sensible and reasonable steps to protect them from damage, loss or theft. Such steps may include:

a. Securing laptops and removable media whether in college or while travelling.
b. Avoiding taking laptops into areas with a high risk of theft and locking such equipment in the boot of a vehicle when leaving it unattended

Users shall ensure that confidential information cannot be viewed by unauthorised persons when using computing equipment in public places (e.g. stations, airports, trains, etc.)

Use of wireless networks outside of college shall be permitted provided that the user ensures that the firewall software provided with the mobile computer is activated. Any sensitive data to be passed over an external wireless access point must be encrypted (this can be achieved via the use of secure websites or the University or College VPN).

Users using mobile computers and smart phones are required to ensure they comply with the College directive on the use of mobile devices found on the College website.

Any mobile computing device owned by the college that is stolen or lost must be reported to the IT department immediately, regardless of date/time. Contact the lodge out of hours when needed.

vi. Software Compliance

The College will provide legitimate copies of software to all staff users who need it, and will ensure the necessary authorisation has been obtained.

Users of Worcester College computer equipment and software shall not copy software or load unauthorised/unapproved software onto a College computer including mobile equipment. The IT

Manager is responsible for giving authority and approval for software suitable for loading on College equipment.

College software is generally licensed for the use of College members only and should not be distributed to any third parties.

The IT Department shall maintain a register of authorised software, including the licence information. All licences and media shall be held securely by the IT Department.

Licensed software shall be removed from any College-owned computer that is to be disposed of outside of the College.

vii. Clear Desk/Clear Screen

Outside normal working hours, all confidential information, whether marked as such or not, shall be secured; this may include within a locked office or in a locked desk. During normal office hours such information shall be concealed or secured if desks are to be left unattended in unlocked/open access offices.

Confidential printed information to be discarded shall be placed in an approved confidential waste container as soon as reasonably practical, or kept secure until that time.

Documents shall be immediately retrieved from printers, photocopiers and fax machines.

All desktop computers shall be logged off or locked automatically after a suitable period (unless required to remain on for operational purposes) to restrict access when the user is not at his or her desk.

Unattended laptop computers, mobile telephones and other portable assets and keys shall be secured e.g. in a locked office, within a lockable desk, or by a lockable cable.

Those in charge of meetings shall ensure that no confidential information is left in the room at the end of the meeting.

The College shall ensure that members of staff have suitable storage facilities to enable them to comply with this Policy.

viii. Information Backup

The requirements for backing-up information shall be defined based upon how often it changes and the ease with which lost data can be recovered and re-entered.

The IT department shall be responsible for ensuring that systems and information held on the College servers are backed up in accordance with the defined requirements, and that back-ups are deleted in line with agreed retention periods. No systems of information should be held solely on local hard drives to avoid the risk of this information not being backed up.

Accurate and complete records of the back-ups shall be produced and maintained. The back-ups shall be stored in a remote location, which must:

a. be a sufficient distance to escape any damage from a physical disaster affecting the main college server room;
b. be accessible;
c. afford an appropriate level of protection to the back-up media in terms of its storage and transportation to and from the remote location.

Back-up media shall be regularly tested to ensure that they can be relied upon for emergency use when necessary.

Restoration procedures shall be regularly checked and tested to ensure that they are effective and that they can be completed within the time allotted in the operational procedures for recovery.

ix. Working from home

Where staff are allowed to work from home, the College will provide suitable and appropriate equipment to support working from home. The University provides 'Working from home' advice[2].

Users shall ensure that appropriate steps are taken to restrict access to College information by third parties within the home environment – these should include:

a. Not sharing IT equipment with family members;
b. Ensuring they have a suitable space to make and receive phone calls / participate in meetings without the risk of being overheard;
c. Ensuring screens are locked when they are away from their home desks.

Users must use the College VPN and remote desktop service to access College data from home.

Whilst working from home or during periods of general disruption, there is an increased risk of cyber attacks, in particular phishing. Users should exercise caution when clicking e-mail links, etc and ensure they have completed the University Information Security training.

x. University/College Cards (Bod Card)

The University/College Card provides access to College facilities and services such as libraries and computing. It also acts as an ID whilst on College premises. It is therefore not permissible for anyone to use anything other than their own University/College card to access facilities or services within College.

By the same account, no College member should ever give, lend, share, use or borrow a University/College Card that is not their own.

Staff or students who are working and use their cards to access tills in the Hall, Bar or Café should not share it or let any other member of staff use it to log in to the till, as they will remain accountable for the logged in use and for any transaction made on the till.

xi. Information Security Training

All users with access to information held on the College's computing infrastructure must complete annually the Information Security Training provided by the University.

8. Data Breach/Loss

The College has a Data Breach Procedure which can be found on the College website. Breaches can include but are not limited to:

a. data breach/loss/theft
b. loss of equipment due to theft
c. inappropriate access controls allowing unauthorised access
d. equipment failure
e. human error
f. unforeseen circumstances such as fire and flood

[2] https://infosec.ox.ac.uk/article/working-from-home-advice

g. hacking
h. 'blagging' offences where data is obtained by deception.

Any breach should be immediately reported to the IT department, Data Protection Officer and to the appropriate head of department. All investigations should be carried out urgently and reviewed once the issue has been resolved. Responsibility for the internal reporting of any data breach is up to the information owner, or the person who first notices that a breach has occurred.

9. Computer Equipment Disposal

Procedures must be in place for the secure disposal/destruction of confidential information. The College complies with the University's policy on the disposal of old computers when disposing of computers owned by the College.

10. Policy Exceptions

An exception to a published policy or procedure may be granted in any of the following situations:

- Temporary exception, where immediate compliance would disrupt critical operations.
- Another acceptable solution with equivalent protection is available.
- A superior solution is available. An exception will be granted until the solution can be reviewed, and standards or procedures can be updated to allow the better solution.
- A legacy system is being retired (utilise a process to manage risk).

All exceptions to this policy must be approved by the Data Protection Officer and IT Manager.

All requests for exception must include:

- Description of the non-compliance
- Anticipated length of non-compliance
- Assessment of risk associated with non-compliance
- System(s) associated
- Data Classification Category(s) of associated system(s)
- Plan for alternate means of risk management
- Metrics to evaluate success of risk management (if risk is significant)
- Review date to evaluate progress toward compliance

11. Governance

This Policy will be reviewed at least biennially or sooner in the case of an incident by the IT Manager and Data Protection Officer. Any changes will be approved by the Governing Body via the College IT Committee.

Version	Date	Author	Rationale
0.1	October 2017	Jonathan Young	First draft
0.2	September 2019	Mark Bainbridge	Annual Review
0.3	October 2019	Jonathan Young	Annual Review
1.1	March 2021	Mark Bainbridge and Jonathan Young	Addition of section 7.ix
1.2	May 2023	Mark Bainbridge and Hamayun Minhas	Amendment to section 7 including University Cards and Information Security Training. Approved at IT Committee, TT23.

1.3	May 2025	Mark Bainbridge and Hamayun Minhas	Link to University classification and handling rules added to section 5. Definitions of Information Asset Owner and Manager added to section 7.i. At section 8, explicit mention of data retention periods for back-ups added.