Worcester College Information Security Policy

Contents

The following policy has been approved by the Governing Body of Worcester College. Any amendments to the policy require the Governing Body's approval. All Fellows, staff, students, and others handling information assets related to Worcester College are required to comply with this policy. Support and guidance is 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 annually 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.

Such information (for example Personnel, Payroll, Student Records) 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 (Data Protection Act 1998), 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 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

5.1. 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.

5.2. 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.

5.3. Where appropriate, information assets should be labelled and handled in accordance with their criticality and sensitivity.

5.4. Rules for the acceptable use of information assets should be identified, documented and implemented. Where these are held on or accessed through a computer system, the University's Regulations and Policies applying to all users of University ICT facilities is available from https://www.it.ox.ac.uk/rules.

5.5. 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.

5.6. Personal data must be handled in accordance with the Data Protection Act 1998 (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.

5.7. 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.

5.8. A higher level of security should be provided for 'sensitive personal data', which is defined in the DPA as data relating to ethnic or racial origin, religious beliefs, physical or mental health, sexual life, political opinions, trade union membership, or the commission or alleged commission of any offence.

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 relavent 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 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 (both by way of a fine of up to £500,000 imposed by the Information Commissioner's Office and also by way of damages sought by an individual whose data has been inappropriately handled), 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.

7.1 Access to Information and Information systems

7.1.1. Information assets shall be 'owned' by a named section within College. A list of information assets, and their owners, shall be maintained by the Data Protection Officer.

7.1.2. 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:
  - i. Locked storage facilities (supported by effective management of keys)
  - ii. Locks on rooms which contain computer facilities
  - iii. Securing of PCs and other devices to prevent theft
  - iv. "Clean desk" policies
  - v. 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:
  - i. The use of strong authentication (minimum length, high complexity, non-reusable passwords)
  - ii. Users to have the ability to change their passwords at any time
  - iii. 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 are 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.

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

7.1.4. 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.

7.1.5. 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.

7.1.6. 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".

7.1.7. 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.

7.2. Visitors to the College

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

7.3. Use of Personal Computer Equipment and Removable Storage

7.3.1. 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 for these purposes must be approved by the Data Protection Officer. Point 7.1.2 addresses this where information is to be transferred outside of the college property/ICT system. The same levels of control should be put in place for information which is held on a staff members' own computing equipment or on equipment provided from outside the College or on removable storage.

7.3.2. 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 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.

7.4. Email and Internet Use

The College's email systems are outsourced to the University's IT Services and is 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.

7.5. 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.

7.5.1. 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

7.5.2. 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.)

7.5.3. Use of wireless networks outside of college shall be permitted provided that member of staff 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.

7.5.4. Users using mobile computers and smart phones are required to ensure that software controls and updates are installed and regularly updated to protect the mobile computers and smart phones from viruses, spyware and similar malicious programmes. Regular updates of anti-malicious software files should occur automatically on connection to the Internet

7.5.6. 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.

7.6. Software Compliance

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

7.6.2. 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.

7.6.3. College's software shall not be given to any outsiders, including senior members/students.

7.6.4. 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.

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

7.7. Clear Desk/Clear Screen

7.7.1. 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.

7.7.2. 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.

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

7.7.4. 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.

7.7.5. 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.

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

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

7.8. Information Backup

7.8.1. 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.

7.8.2. 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. No systems of information should be held on local hard drives to avoid the risk of this information not being backed up.

7.8.3. Accurate and complete records of the back-up copies shall be produced and maintained.

7.8.4. The back-ups shall be stored in a remote location, which must:

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

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

7.8.6. 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.

8. Data Breach/Loss

8.1. Data breach policies shall be in place to handle loss of data. Such breaches shall include any breaches of this policy. Breaches include but are not limited to:

- data breach/loss/theft
- loss of equipment due to theft
- inappropriate access controls allowing unauthorised access
- equipment failure
- human error
- unforeseen circumstances such as fire and flood
- hacking
- ‘blagging’ offences where data is obtained by deception.

8.2. 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 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

Policies and 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, which can be found at https://www.it.ox.ac.uk/policies-and-guidelines/computer-disposal.

10. Policy Exceptions

10.1. 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 (utilize a process to manage risk).

10.2. 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 regularly by the IT Manager and Data Protection Officer.

Any changes will be approved by the Governing Body via the College IT Committee.