Wadham College Information Security Policy

1. Introduction

In July 2012 the University of Oxford approved its Information Security policy that had been created to protect the University from serious information security breaches. The policy was developed in line with the Data Protection Act 1998 (DPA) and encompasses the basic security requirements needed to ensure the University remains upholding of current UK legislation. Recent changes made by the Information Commissioner's Office (ICO) require that all legal entities that handle information must be mindful of their duty of care under the DPA and that a failure to meet this, that results in a serious breach of the Act, will incur a large fine and possible reputational damage.

The Conference of Colleges information security working group has taken the University's Information Security Policy and used it to develop a suitable college information security template policy. Wadham College is using this template to help form the basis of its own policy.

2. Objective

This information security policy is meant to ensure that all information within the College is secure and only accessible to those who require it to fulfil their College or University responsibilities. This information may be electronic or paper based but must be stored in appropriately secure systems. All users of the College systems are obliged under the terms of the DPA to ensure that appropriate security measures are in place to prevent unauthorised access to personal data.

This policy will offer guidance on how to identify what information and risks are present and how to mitigate these. Guidance is also offered with respect to standard working practices.

3. Scope and definitions

The scope of this information Security Policy extends to all Wadham College's information including but not limited to:

- Records relating to students, alumni, 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, DOB and addresses

This policy covers all data access and processing within the College and through remote or mobile working. All College members (students, Fellows, staff, Lecturers, SU/MCR members and affiliate members) must be familiar with this policy and any appropriate supporting documentation. The Policy should be read in conjunction with the College's Data Protection Policy and relevant sections of the staff and student handbooks and the guides for Fellows and Lecturers.

4. Policy

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

- Protect the confidentiality, integrity and availability of all data it holds within 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
- Meet legislative and contractual obligations
- Protect the College's intellectual property rights
- Produce, maintain and test business continuity plans particularly with respect to data backup and recovery
- Prohibit unauthorised use of the College's information and systems
- Communicate this Information Security Policy to all persons potentially accessing data
- Provide information security training to all persons appropriate to the role
- Report any breaches of information security, actual or suspected to the Data Protection Officer (DPO) in a timely manner

More detailed guidance is provided in the supporting documentation to this Policy.

5. Responsibilities

The Governing Body is ultimately responsible for establishing the framework and for issuing and reviewing policy statements and procedures to support Wadham College and the University's Ordinances and Regulations with which members of the University must comply.

Governing Body requires the head of each department within College to be accountable for implementing an appropriate level of security control for the information owned by that department and processed by persons accessing that data.

Each person is accountable to their head of department for operating an appropriate level of security control over the information and systems they use to perform their duties.

The DPO 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 financial loss (arising both as fines of up to £500,000 imposed by the Information Commissioner's Office and by way of damages sought by an individual whose data has been inappropriately handled), operational incapacity, and loss of reputation. Data access or processing that fails to observe the provisions of this policy may result in disciplinary action.

May 2015

Appendices

1. Responsibilities of Information Owners
2. Best Practice Guidelines for all Computer Users
3. Mobile and Remote Working Guidelines
4. ICT Arrangements and Responsibilities

Glossary

DPA	The Data Protection Act 1998
DPO	Data Protection Officer
ICO	Information Commissioner's Office
ICT	Information, Communications & Technology
ICTC	University of Oxford Information, Communications & Technology Committee (http://www.admin.ox.ac.uk/ictc/)
OxCERT	The University of Oxford's Computer Emergency Response Team
SSO	The University of Oxford Single Sign-On username.

Appendix 1: Responsibilities of Information Owners

Information assets shall be 'owned' by a named person within Wadham College, normally the most appropriate College Officer or Head of Department. A list of information assets, and their owners, shall be maintained by the Data Protection Officer.

The responsibilities of Information Owners shall include:

- Preparing and keeping updated a list of information assets for which they are responsible, including classifying the kind of data held and any resulting requirements such as encryption or password-protection.
- Ensuring that access to information is restricted to authorised users and granted on the basis of the minimum privileges required for a member of staff to fulfil their duties.
- Ensuring that staff or others handling data on the College's behalf complete appropriate training.
- Maintaining a record of those engaged in remote / mobile working and making sure they have received the relevant guidelines.
- Implementing appropriate practical, physical and logical controls in the areas for which they are responsible including:
    - Locked storage facilities (supported by effective management of keys)
    - Locks on rooms which contain computer facilities. Electronic locks should have their database systems reviewed at frequent intervals to ensure user access control is up-to-date.
    - Securing of mobile computers and other devices to prevent theft, where other physical controls such as locked doors or available secure storage cabinets are not available.
    - Clean desk and screen practices.
    - Encryption of data either transmitted or taken outside of Wadham College, appropriate to the level of risk assessment of the data.
    - Robust password management systems, encouraging users to follow the best practice guidelines (minimum length, high complexity, non-reusable passwords which are changed at regular intervals).
- Ensuring, with the HR and IT Departments, that all employees, contractors and third party users have information and physical access permissions granted expediently on joining the organisation, updated on changes in role and revoked on leaving the organisation.
- Completing leavers' checklists and communicating those lists to appropriate sections of College. Leavers will be required to return all of the Wadham College's assets in their possession upon termination of their employment, contract or agreement. To allow for potential investigations and traceability, access records will be retained for a minimum of six months or longer where considered appropriate.
- Ensuring that access to physical information assets - for example printed paper documents, and media containing information – is governed as appropriate by the above principles.
- Any exception to these provisions must be subject to a specific risk assessment and is only permitted where approval is given by the DPO.

Appendix 2: Best Practice Guidelines for all Computer Users

All members of the College have a responsibility to protect the confidentiality and integrity of the College's information assets and systems and to be aware of the legal requirements in this regard. The following guidelines should be read in conjunction with the College's data protection policy and acceptable use policies for computing resources provided in the staff and student handbooks and the guides for fellows' and lecturers.

KEEPING INFORMATION SAFE: DO	KEEPING INFORMATION SAFE: DO NOT
✓ Ensure you are familiar with the College's policies on information security, data protection and the acceptable use of computing resources. ✓ Be aware of the nature of the data you are handling and any resulting security risks and requirements. ✓ Handle any information received from an external organisation in a way that meets the security expectations of the organisation providing the data as well as the College. ✓ Complete the online training module provided by the University at http://www.it.ox.ac.uk/infosec/module/. This is required for all administrative staff with access to personal data on students, alumni or staff. ✓ Refer to the University's guidance on all aspects of computer use including security available at http://www.it.ox.ac.uk/want/get-started ✓ Ensure that you permanently delete any College-related information saved on any personal computer equipment if you leave the College.	× Assume that information security is not relevant to you. All information of a confidential nature or of value is at risk no matter whether this is related to studying, teaching, research, the running of the College or other areas of College life. × Use a mobile or remote storage device or your own computer equipment for your work without appropriate safeguards in place (see further guidelines on mobile and remote working below).
PERSONAL DATA: DO	**PERSONAL DATA: DO NOT**
✓ Take particular care with information which is classed as personal data or sensitive personal data as defined under the Data Protection Act[1] ✓ Always save sensitive personal data in a secure location and encrypt as necessary.	× Disclose personal information to third parties without appropriate protection and the express permission of the information asset owner. × Manipulate any reports containing sensitive data provided in an anonymised form in such a way that individuals could be identified.

[1] Personal data is defined as "Any information that links one or more identifiable living person with private information about them" or "Any source of information about 1000 identifiable individuals or more, other than information sourced from the public domain". This could be in any form, paper or electronic, including database records, emails and contacts stored in an email system as well as CVs, references, job applications, and information downloaded from the web. Sensitive personal data refers to racial or ethnic origin, political opinions, religious beliefs or other beliefs of a similar nature, trade union membership, physical or mental health or condition, sexual life, and information related to the commission or alleged commission of an offence.

COMPUTER USE: DO	COMPUTER USE: DO NOT
✓ Only use software as licenced. The College will provide properly licensed and authentic installations of software to all users who require it in the course of their duties. ✓ Take full responsibility for the security of your username and passwords (see further advice below). If you suspect that an account has been compromised, report this immediately to the ICT team and change all passwords on the system. ✓ Remember that email is not necessarily private or secure. Consider carefully the content of messages and be wary of relying on facilities such as the autofill of email addresses or "reply all" which might result in sensitive information being sent to the wrong person. ✓ Be alert to fraudulent attempts to gain access to data through 'phishing' emails. ✓ Use social networks safely. Comprehensive guidance is available at http://help.it.ox.ac.uk/infosec/protectyourself/index.	× Copy software or load unauthorised/unapproved software onto a College computer including mobile equipment. The ICT manager is responsible for giving authority and approval for software suitable for loading on College equipment. × Trust public internet access points when handling confidential information. × Store data in public cloud storage facilities without appropriate protection.
VIRUS PROTECTION: DO	**VIRUS PROTECTION: DO NOT**
✓ Forward virus or other malware warnings to the ICT staff for checking and distribution. ✓ Always run the standard, supported anti-virus software which is available from the University. ✓ On personally owned or remote systems, ensure that updates are performed frequently, and that a licence is renewed annually. College installed anti-virus software will be configured to update automatically. ✓ Delete spam, chain, and other junk email without forwarding. ✓ Always scan a USB key or other removable media from an unknown source for viruses before using it. ✓ Back-up critical data and system configurations on a regular basis and store the data in a safe place.	× Forward virus or malware warnings to other users. × NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately and then empty your Trash/Recycling Bin. × Never download files from unknown or suspicious sources.

PASSWORDS: DO	PASSWORDS: DO NOT
✓ Change passwords regularly in line with the password policies. ✓ Refer anyone who demands a password from you to this document or have them call the local ICT Staff ✓ **Use strong passwords with the following characteristics** • Contains both upper and lower case characters (e.g., a-z, A-Z) • Digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./) • At least 7 alphanumeric characters long and is a passphrase (Ohmy1stubbedmyt0e). • Is not a single word in any language, slang, dialect, jargon, etc. • Is not based on personal information, names of family, etc. • Is never written down or stored on-line in the clear / unless encrypted. Passwords should be easily remembered but still complex and difficult to guess. One way to do this is create a password based on a song title, affirmation, or other phrase personal to you. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.	× Use the same password for University accounts as for other non-University access (e.g., personal ISP account, personal email, banking etc.). × Share a password with ANYONE × Talk about a password in front of others × Hint at the format of a password (e.g., "my family name") × Reveal a password on questionnaires, security forms, in an email message or over the phone. The University and College would **never** ask you for log-in details of your accounts or prompt you to click a link and log in. × Use the "Remember Password" feature of applications (e.g., Outlook, Firefox, Safari) × Write passwords down and store them anywhere in your office × Store passwords in a file on ANY computer system (including Blackberries, iPhones, Palm Pilots or similar devices) without encryption.
PRACTICAL MEASURES: DO	**PRACTICAL MEASURES: DO NOT**
✓ Log off, or set up automatic locking after a suitable period, on your desktop computer to ensure that this does not become a potential means to gain unauthorized access to the network. ✓ Secure unattended laptop computers, mobile telephones and other portable assets and keys (e.g. in a locked office or student room, within a lockable desk, or by a lockable cable). ✓ Secure all confidential information, whether marked up as such or not, within a locked office or in a locked desk or filing cabinet. ✓ Retrieve documents immediately from printers, photocopiers and fax machines.	× Leave confidential information up on a screen or visible on a desk where it could be seen by someone coming in to the room. × Leave any confidential information in a room at the end of a meeting.

✓ Discard confidential printed information in an approved confidential waste container as soon as reasonably practical or keep the papers secure until that time. ✓ Close windows when leaving a room.	
DATA BREACH/LOSS: DO	**DATA BREACH/LOSS: DO NOT**
✓ Report any data breach immediately to the ICT department and, if applicable, to your head of department. Breaches can include: ○ loss or theft of data or equipment ○ 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	× Delay reporting a possible breach because you are worried about the consequences or hope that information will not have been compromised. It is important to deal with any concerns as soon as possible.

Appendix 3: Mobile and Remote Working Guidelines

Wadham College recognises that there may be occasions when members of College need to use their own computing equipment or mobile device or a College-owned mobile device to access or process information. The same levels of control and protection should be applied to information which is transferred outside of College property and ICT systems as for information stored and handled internally. Please follow the guidelines below and ensure that you take all sensible and reasonable steps to protect equipment, including mobile phones, from damage, loss or theft.

PROTECTING INFORMATION OUTSIDE COLLEGE: DO	PROTECTING INFORMATION OUTSIDE COLLEGE: DO NOT
✓ Ensure that up-to-date anti-virus software and a firewall are installed on any computing equipment or mobile devices used to process College information or connect to the College network or internet. Anti-virus software provided via a College site-license must be used on all systems connected to the network. Contact the ICT team for further advice. ✓ Ensure that regular updates of anti-malicious software files occur automatically on connection to the Internet. ✓ Have encryption enabled or software installed to encrypt data on the device. Any information containing personal data should normally be encrypted before storage. ✓ Take care in public places (stations, airports, trains, etc.) to ensure that confidential information cannot be viewed by others. ✓ Delete all your work before returning a loan laptop or other device.	× Take confidential data with you when travelling abroad if this can be avoided. Immigration officers in the UK or overseas may require files or devices to be decrypted. Use the University's secure facilities for remote access such as OxFile, WebLearn and Sharepoint instead. × Retain Wadham College information on mobile or removable storage devices longer than necessary (i.e. once information that has been updated on a personal computer or mobile device is uploaded onto College systems, it should be deleted from the removable storage device). × Leave confidential information that you may have printed at home or while travelling accessible to others or dispose of this without shredding it first. × Store, or forward by email, any confidential data downloaded from a secure source without re-applying suitable encryption or password protection. × Use public cloud-based services unless approved by the ICT team.
PROTECTING LAPTOPS AND MOBILE DEVICES: DO	**PROTECTING LAPTOPS AND MOBILE DEVICES: DO NOT**
✓ Secure laptops and removable media whether in college or while travelling. ✓ Avoid taking laptops into areas with a high risk of theft. ✓ Lock equipment in the boot of a vehicle when leaving it unattended. ✓ Ensure that all mobile devices are protected by a strong password of six characters or more, or PIN, and never share this with anyone. ✓ Set devices to lock after a short period of inactivity and turn on the remote wipe capability to mitigate the risks posed by loss or theft. ✓ REPORT ANY MOBILE DEVICE THAT IS STOLEN OR LOST TO THE ICT TEAM IMMEDIATELY, REGARDLESS OF DATE/TIME. If out of hours then contact via the Lodge. ICT can provide advice on what options are available.	× Allow others to use a College-owned device for which you are responsible. × Use external wireless access points unless the firewall software provided with the mobile computer you are using is activated. × Download apps on your own equipment unless you are sure they are from a trusted location (do not download apps on to a College device). × Connect to the College network on any mobile device that has undergone a 'jailbreak' procedure. This is prohibited.

Appendix 4: ICT Arrangements and Responsibilities

Servers

This policy specifically applies to server equipment owned and/or operated by College and maintained by the ICT department.

- Physical servers must be housed in a location where physical access and the server environment (power, temperature, and humidity) can be controlled.
- Servers should be backed up to a suitable and secure alternative location/s both onsite and offsite: refer to Information Backup within this section for further information.
- Servers must be catalogued by the ICT Team.

Network Security

Responsibility for management and security of the College's internal network rests with the ICT team, within which a network administrator must be nominated. The network administrator for the College must:

- Ensure network/systems administrators are suitably trained in security
- Proper logs are kept in accordance with University IT Services policies
- Protect physical network from interception/damage/interference
- Restrict unauthorized traffic using a firewall or equivalent device
- Regularly review and maintain network security controls and device configurations
- Identify security features, service levels and management requirements and include them in any network service agreements whether they are in-house or outsourced
- Use secure network connections for making any transfers of non-public information
- Ensure that a password expiry or account lock-out system is in place to automate and enforce the regular changing of passwords by users.

All College's networks must be monitored at all times. Monitoring must detect and log at least the following activities, as comprehensively as reasonably possible:

- Unauthorized access attempts on firewalls, systems, and network devices (only authorized systems and users should have access to the network)
- Port scanning
- System intrusion originating from a protected system behind a firewall
- System intrusion originating from outside the firewall
- Network intrusion
- Denial of services
- Any other relevant security events
- Login and log-off activities

All network activity should be logged in accordance with University IT Services policy. It is currently recommended that at least 60 days of logs be kept, and longer if possible to allow for any post-incident review. Logs must include identifiable data to enable traces back to specific events, computer systems, and specific users. Timestamps, MAC addresses, IP Addresses, and where possible usernames should be included in logging systems. These logs should be proactively monitored and reviewed as an early warning system for hacking or any other form of unauthorized activity.

Further information on network security and good practice can be found within the ITSS IS Toolkit http://www.it.ox.ac.uk/infosec/istoolkit/

Information Backup

The ICT team shall be responsible for ensuring that systems and information are backed up in accordance with the defined requirements.

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

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

- Be a sufficient distance to escape any damage from a physical disaster at the College
- 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

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.

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

Non-University Cloud Storage and Services

The use of cloud services for the processing and/or storage of personal or sensitive information should be risk assessed and adhere to all other sections of this policy.

Personal cloud services accounts may not be used for the storage, manipulation or exchange of College-related communications or College-owned data.

Computer Equipment Loan

All loan equipment shall have up-to-date anti-virus software and a firewall installed.

Checks shall be carried out that all information stored has been deleted before a returned device is assigned to another person.

Computer Equipment Disposal

Wadham College subscribes to the University policy for the disposal of equipment that no longer required. This policy may be found at http://www.ict.ox.ac.uk/oxford/disposal/.

- Reasonable efforts should be made to see if any other unit is able to make use of the equipment.
- Equipment that has residual value may be sold, either to University members or outside bodies, subject to the University's financial guidelines.
- Where equipment has limited resale value, consideration should be given to whether it can be donated to any charitable or community project. If the equipment cannot be reused, then it should be recycled or disposed of in an environmentally-friendly manner.
- Disks that have contained information classed as confidential or sensitive must be secure wiped using a tool such as PGP or DBAN or physically destroyed.

May 2015