WADHAM
COLLEGE
UNIVERSITY OF OXFORD

Data Security Guidance

Contents

Revision history

Version	Date	Changes & Approvals
1.0	24 May 2018	Final version for circulation

1. 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. These are available on the College Regulations and Policies webpage.

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 Fellows, Lecturers and 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 General Data Protection Regulation[1].	× Disclose personal information to third parties without appropriate protection and the express permission of the Data Lead. × 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 relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier". 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. Special category personal data is more sensitive, and so needs more protection. This includes ethnic origin, politics, religion, trade union membership, genetics, biometrics, health, sex life, and sexual orientation. This type of data could create more significant risks to a person's fundamental rights and freedoms. For example, by putting them at risk of unlawful discrimination. Separate sensitive (special category) apply to information about criminal allegations, proceedings or convictions.

✓ Always save sensitive personal data in a secure location and encrypt as necessary.	
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. × Assume that all e-mails are genuine, and don't click on links or open any attachments for unexpected or unsolicited emails. × Trust public internet access points when handling confidential information. × Store data in public cloud storage facilities without appropriate protection. × Put payment card information into a website without checking that there is an HTTPS padlock symbol next to the website address. If in doubt, don't use that site to purchase goods or services. × Use different passwords for different websites.
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.). ✗ Use the same password for various University access needs. ✗ 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. 15 minutes is normal. In situations where special category data is processed, this should be a shorter period. ✓ Lock the screen when leaving a workstation. ✓ 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.	✗ Store sensitive or confidential data on an unencrypted file systems or USB keys. ✗ 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.

2. Best Practice Guidelines for Mobile and Remote Working

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. ✓ Ensure only trustworthy applications from reputable sources are installed.	× 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).

✓ 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.	× 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**
✓ Security mark the laptop/mobile device. ✓ 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 so that the breach can be mitigated.	× 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.

3. Best Practice Guidelines for Post and Couriers

KEEPING INFORMATION SAFE: DO	KEEPING INFORMATION SAFE: DO NOT
✓ Ensure that envelopes and parcels containing sensitive or confidential data are marked ‘private and confidential’. ✓ Double check the name and full postal address of the recipient. ✓ Package securely to protect the contents from being tampered with or from any physical damage likely to arise during transit e.g. a tamperproof wallet. ✓ Choose an approved courier or secure mail method which can be tracked and is signed for.	× Do not leave opened post containing sensitive or confidential mail in post areas. × Do not leave sensitive or confidential mail in post area for longer than is necessary.

✓ E-mail or phone the recipient to let them know that the information has been sent to them and ask them to confirm receipt. ✓ Ensure incoming post is handled securely.	

4. Best Practice Guidelines for Telephone and Verbal Communication

KEEPING INFORMATION SAFE: DO	KEEPING INFORMATION SAFE: DO NOT
✓ Check to see whether confidential conversations may be overhead and take steps to prevent this. ✓ If using a phone in a public area ensure than you are not breaching confidentiality by disclosing personal data. ✓ Use a security pin code to protect access to answerphone messages. ✓ Ensure that answerphone messages that are played back cannot be overhead. ✓ Prior to discussing confidential and sensitive information on the telephone, verify the identity of the caller to ensure that you speaking to a person authorised to receive that information. It is recommended to ask the caller to provide their telephone number and phone the caller back as part of the verification process before disclosing any personal data.	× Do not share confidential information in public areas.