2018

The following policy has been approved by University College. Any amendments to the policy require the College's approval. Each faculty and department within University College is required to comply with this policy. Support and guidance for departments is offered by University College's ICT Team which in turn is supported by the central information security team, "InfoSec". 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.

University College's Governing Body requires that this policy is reviewed annually to ensure any new developments are covered and protected.

UNIVERSITY COLLEGE
INFORMATION SECURITY POLICY

Template v1.15 May, 2018

This page is intended as a digest of the attached intercollegiate policy on information security. For more detailed information, please refer to it.

The College will have due regard to the Data Protection Act 1998, the General Data Protection Regulation (GDPR) coming into full force May 2018, and any subsequent data protection legislation; to the Freedom of Information Act 2000, the Protection of Freedoms Act 2012 and the Human Rights Act 1998.

The terms of the GDPR make incumbent upon all those with access to personal data and sensitive personal data, whether they are gathering, holding or processing that data, a duty of keeping such data secure and treating it within an established lawful purpose (sometimes called the 'lawful basis'). The release of personal data or information outside of that lawful purpose must only be with the express permission of the individual to whom it relates. Breaches of the legislation can trigger large fines, and cause distress and anger to those whom they affect.

This makes it imperative that all members of University College dealing with such data should take steps to protect data, which include, but are not necessarily limited to, the following:

1. Preserving the security of such data in a physical sense by keeping sensitive documentation under lock and key, and by ensuring that networked devices (including tablets, smartphones, etc.) are kept secure and password- or PIN protected, and by using the recommended arrangements for the disposal of confidential waste;
2. Where required, encrypting sensitive data (e.g. when placed on portable devices such as flash drives);
3. Keeping anti-virus, firewall, and operating system software up to date and patched at all times, and making sure it is of the best available standard;
4. Not opening any suspicious emails or attachments, which may contain spyware and malware;
5. Taking extreme care when, for example, sending out mass mailings, and using the 'reply to all senders' facility in email;
6. Logging out of sensitive sites (e.g. OxCort, admissions databases such as ADSS, Nexus email) when they are not in use;
7. Exercising especial care when working outside College and University workspace, and particularly when using free wireless systems;
8. Always reading carefully, and acting upon, advice relating to security sent by University College (and, where relevant also, Faculty) ICT staff;
9. Avoiding, where sensitive information is concerned, commercial file-sharing sites such as DropBox, WeTransfer, and commercial 'cloud' services;
10. Considering carefully whether information would be better communicated non-electronically: by a face-to-face meeting, telephone conversation, or on paper (sent registered if committed to the ordinary post).

All members and employees of University College *should take care to read and understand the information relating to information security. They undertake to observe safe practice when they have access to sensitive personal data.*

Overview

Users of ICT within the University are subject in the first instance to the University ICTC regulations (2002) with subsequent amendments and available for review at: http://www.admin.ox.ac.uk/statutes/regulations/196-052.shtml

Further the University College has a statutory duty to have due regard for the need to prevent people from being drawn into terrorism (The 'Prevent' duty under the Counter-Terrorism and Security Act 2015). University College therefore reserves the right to monitor IT use in order to ensure compliance with the law and the College's acceptable use policy. Any suspected breaches will be investigated by an independent panel of University College members.

The ICTC regulations 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 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.

To avoid ambiguities, particular terminology is used when explaining the policies:

- **MUST** This word, or the terms **"REQUIRED"** or **"SHALL"**, mean that the item is an absolute requirement.
- **MUST NOT** This phrase, or the phrase **"SHALL NOT"**, mean that the item is absolutely prohibited.
- **SHOULD** This word, or the adjective **"RECOMMENDED"**, mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
- **SHOULD NOT** This phrase, or the phrase **"NOT RECOMMENDED"** mean that there may exist valid reasons in particular circumstances when the particular behaviour is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.

1. Introduction

University 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.

2. 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 unauthorized access or loss of data.

In support of this objective all users of data assets, whether they are manual or electronic – some example datasets and their owner are recorded in **Appendix 1** - 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 GDPR, 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 safe guard it against unauthorized access and or theft.

3. Scope and definition

The scope of this Information Security Policy extends to all University 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.

and the following definitions apply throughout the policy document

- 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 GDPR defines as more sensitive, and so needs more protection. Examples of special category data include race, ethnic origin, politics, religion, trade union membership, genetics, biometrics, health, sex life, sexual orientation.

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.

4. Policy

University 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 copy 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 regards 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 (see Section 9 of this policy).

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 first step in determining the appropriate level of security therefore is 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 University College's information assets; 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. Further information on the University's Regulations and Policies applying to all users of University ICT facilities are available from http://www.ict.ox.ac.uk/oxford/rules/.

5.5 Information security risk assessments should be reviewed 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 GDPR and in accordance with this policy.

5.7 GDPR 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 'special category data', which is defined in the GDPR 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 criminal offences.

6. Responsibilities

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

6.2 Governing Body requires the head of each department in 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.

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

6.4 Every user is required to obey all laws, including criminal, counter-terrorism, copyright, defamation and obscenity laws. College will render all reasonable assistance to enforcement officials for the investigation and prosecution of persons using technology in violation of any law.

6.5 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 material fines 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.

7. Detailed Policies and Guidance

The following shall be complied with throughout University College.

7.1. Access to Information and Information systems

7.1.1. Information assets shall be 'owned' by a named officer within College. A list of information assets, and their owners, shall be maintained by the DPO.

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

- 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. 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" policies (refer to section 7.8 of this policy)
  - Encryption of data either transmitted or taken outside College's properties. Encryption of data should be appropriate to the level of risk assessment of the data.
- Logical controls for information and information processing assets shall include passwords for systems access.
- Passwords and password management systems shall follow good practice for security and use the following techniques:
  - All system-level passwords (e.g., root, enable, admin, application administration accounts, etc.) should be changed on at least a quarterly basis, and an expiry policy should be configured to enforce this where possible.
  - The use of strong authentication (minimum length, high complexity, non-reusable passwords). Refer to **Appendix 2** for Password Construction Guidelines.
  - Users to have the ability to change their own passwords at any time

- Passwords to be changed at regular intervals appropriate to the information and resources being secured. A password expiry or account lock-out system to be in place to automate and enforce this process
- Passwords must not be inserted into email messages or other forms of electronic communication.
- Any exception to these provisions must be subject to a specific risk assessment and is only permitted where approval is given by the DPO.

- 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 ICT team immediately and change all passwords on all system. For further standards on password protection refer to **Appendix 3**.
- Access privileges shall be allocated based on the minimum privileges required to fulfil that member of staff's duties. Access privileges shall be authorised by the appropriate information owner or someone with authority to act on their behalf.
- Users must take particular care when disclosing information to third parties, to ensure that there is no breach of GDPR. The permission of the information asset owner should be sought before the release of personal or sensitive information.
- All shared computer systems, with the exception of open access kiosk-style browser-only systems, will require users to authenticate before use, and will enable activities to be traced to an authenticated individual.
- To allow for potential investigations and traceability, access records should be kept for a minimum of six months, or for longer, where considered appropriate.
- Access to the College's administered networks via remote access must require a login in order to get access to any system on the internal network.

7.1.3. Information 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. Appropriate processes shall be in place to ensure that all employees, contractors and third party users have information and physical access permissions granted expediently on joining the organisation, revoked on leaving the organisation, and updated on changes in role. Leavers will also be required to return all of the College's assets in their possession upon termination of their employment, contract or agreement. College Officers or other relevant roles are responsible for completing leavers checklists and communicating those lists to appropriate sections of College.

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 form part of 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 DPO once they have been reviewed and appropriate risk assessments made as to the validity of requirements and the skill levels of those requesting increased privileges.

7.1.8. Visitors to the College should be provided with specifically assigned credentials and should be appropriately authenticated and automatically disabled at the end of their term with the College.

7.2. **Use of Personal Computer Equipment and Removable Storage**

7.2.1. University College recognises that there may be occasions when staff need to use their own computing equipment to process information (including personal data). 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 removable storage.

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". Emails and contacts stored in an email system count as personal data, as do most CVs, references, and job applications.

7.2.2. It is good practice and required that:

- Privately owned computing equipment used to process College information or connect to the College 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 via a site-license must be used on all systems connected to the administered network. The preferred method of installation is via the Institute's automated software installation service. Refer to **Appendix 4** for further recommended end user practices to prevent Virus problems.
- Information containing personal data concerning pupils, students, alumni or staff that is to be saved onto removable storage or privately owned computing equipment shall be encrypted before storage.
- Special category data (covered by the GDPR) on removable storage devices must be protected from loss and/or theft. Removable storage devices must have encryption enabled, or software installed to encrypt data that is on the device.
- University College information shall not be retained on removable storage devices longer than necessary (i.e. once information that has been updated on a computer owned by a member of staff is uploaded onto College systems, it shall be deleted from the removable storage device).

7.3. **Servers** This policy specifically applies to server equipment owned and/or operated by University College, and to servers registered under any University College-administered network.

All internal servers deployed in the College must be administered by an operational group that is responsible for system administration. Approved server configuration guides must be established and maintained by each operational group. Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a process for changing the configuration guides, which includes peer review and approval.

7.3.1. Physical servers must be housed in a location where physical access and the server environment (power, temperature, and humidity) can be controlled.

7.3.2. Servers should be backed up to offsite storage, such as the University HFS. (Refer to section 7.9 of this policy for further information)

7.3.3. Servers must be registered with the University College ICT team. As a minimum, the following information is required to positively identify the point of contact:

- Server contact(s) and location, and a backup contact
- Hardware and Operating System/Version
- Main functions and applications, if applicable

Refer to **Appendix 5** for Server General Configuration Guidelines.

University College *ICT Staff will police its own policies in this area but will seek regular review and audit from the University IT Services and the wider IT support community in the University.*

7.4. **Network Security**

7.4.1. Responsibility for management and security of the College's internal network rests with the IT 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 be in-house or outsourced

- Use secure network connections for making any transfers of non-public information

7.4.2. 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

7.4.3. 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/

7.5. Email and Internet Use

Policy for the use of electronic mail is covered by the University's ICTC regulations of 2002 (with subsequent amendments) and available at http://www.admin.ox.ac.uk/statutes/regulations/196-052.shtml

Where email systems are hosted locally, it should be checked by the College's ICT Services Department on a regular basis to ensure that it is being appropriately updated in regards to spam/virus filters. All email that passes through the email system shall be content checked and scanned for viruses and inappropriate content and cross checked against an internet "black list" of banned email addresses. For centrally hosted email by UNIVERSITY IT SERVICES, their information policy will take precedence.

7.5.1. College's policy and procedure on staff use of email and the Internet should be included in the Staff Handbook.

7.5.2. Virus or other malware warnings should be forwarded to ICT staff for checking and distribution rather than sent to other users. Mass mailing users of address groups provided by the College is for work-related information only. This therefore excludes the use of the email system for advertising personal items for sale.

7.6. **Mobile Computing** (applies to any mobile hardware that is used to access College resources, whether the device is owned by the user or by the College.)

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

- securing laptops and removable media whether in college or while travelling;
- 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.

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

7.6.3. Use of external wireless access points shall be permitted provided that the firewall software provided with the mobile computer is activated.

7.6.4. Mobile computer and smart phone users 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.

7.6.5. Use of any mobile computing device owned by the College, or that is used to access College data (including email) must be in accordance with this Policy and the relevant section of the Staff Handbook.

7.6.6. Mobile Device Security

- **Any one** using mobile devices and related software for network and data access will, without exception, use secure data management procedures**.** All mobile devices must be protected by a strong password of six characters or more, **or PIN, and must never be shared with anyone.**
- Any mobile device that is used to access College should have the remote wipe capability of the device turned on to protect against potential loss or theft.

- It is prohibited to connect to the College network any mobile device that has undergone a 'jailbreak' procedure.
- Mobile devices should not be used to carry sensitive College data for any longer then absolutely necessary and should be encrypted if possible to protect any data that is on the device.

7.6.7. **ANY MOBILE DEVICE THAT IS STOLEN OR LOST MUST BE REPORTED TO THE ICT TEAM IMMEDIATELY, REGARDLESS OF DATE/TIME. USE THE OUT OF HOURS ICT SUPPORT LINE WHEN NEEDED.**

7.7. **Software Compliance**

7.7.1. College will provide properly licensed and authentic installations of software to all users who require it in the course of their duties.

7.7.2. Users of College computer equipment and software shall not 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.

7.7.3. College's software shall only be distributed and used as licenced.

7.7.4. The ICT team shall maintain a register of authorised software, including the licence information. All licences and media shall be held securely in the ICT team.

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

7.7.6 Further Software Usage Policies should be included in the Staff Handbook.

7.8. **Clear Desk/Clear Screen**

7.8.1. Outside normal working hours, all confidential information, whether marked up 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.

7.8.2. 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.

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

7.8.4. All desktop computers must be logged off or locked automatically after a suitable period* (unless required to remain on for operational purposes) to ensure that unattended computer

systems do not become a potential means to gain unauthorized access to the network. * it is suggested that 15 minutes is a suitable time

7.8.5. 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.

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

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

7.9. **Information Backup**

7.9.1. 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.

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

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

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

- be a sufficient distance to escape any damage from a physical disaster 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.

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

7.9.6. 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.

7.9.7. 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.

7.10. **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. Individuals must ensure

they do not make use of personal cloud services for the processing and/or storage of personal or sensitive information unless those services have also been risk assessed and adhere to all other sections of this policy.

7.11. **Homeworking**

We support homeworking in appropriate circumstances either occasionally (to respond to specific circumstances or to complete particular tasks) and in some cases on a regular (full or part-time basis). In addition, occasional or permanent homeworking can, in certain circumstances, be a means of accommodating a disability, and can be requested as a means of flexible working (please refer to your Head of Department and HR for more details, and assistance, if appropriate, in making a case).

If the College grants permission for you to work from home, this policy section defines the requirements that you must comply with.

7.11.1 **Working at Home: Equipment**

- It is your responsibility to ensure that you have sufficient and appropriate equipment for working from home. We are not responsible for the provision, maintenance, replacement, or repair in the event of loss or damage to any personal equipment used by you when working for us.
- It is your responsibility to ensure that your Home Equipment can meet the 'Data Security and Confidentiality' requirements contained in this Policy
- We are not responsible for any of the associated costs of you working from home including the costs of heating, lighting, electricity or telephone calls.

7.11.2 **Working at Home: Data Security and Confidentiality**

- You confirm that you have read and understood our policies relating to computer use, electronic communications and data security and that you will regularly keep yourself informed of the most current version of these policies.
- Your home equipment must be kept continuously up-to-date with respect to all current electronic communications and data security requirements that the College may specify.
- All College-related communications must be made through your College email address, save in only the most exceptional circumstances, e.g., confirmed central failure of the University's email system.
- If you discover or suspect that there has been an incident involving the security of information relating to the College, students or anyone working with us, you must report it immediately according to Section 9 of this Policy.

7.11.3 **Working at Home: Health and Security**

- When working at home you have the same health and safety duties and obligations as other staff. You must take reasonable care of your own health and safety and that of anyone else who might be affected by your actions and omissions.

8 Computer Equipment Disposal

University College subscribes to the University policy for disposal of equipment that is surplus to the requirements of the unit that originally purchased it .This policy may be found at http://www.ict.ox.ac.uk/oxford/disposal/

The University policy stresses the importance of the need to remove sensitive and confidential data from the hard disks of computers that are ready for disposal.

Before disposing of any computer system, it is vital to remove all traces of data files. Deleting the visible files is not sufficient to achieve this, since data recovery software could be used by a new owner to "undelete" such files. The disk-space previously used by deleted files needs to be overwritten with new, meaningless data - either some fixed pattern (e.g. binary zeroes) or random data. Similarly, reformatting the whole hard disk may not in itself prevent the recovery of old data as it is possible for disks to be "unformatted".

Almost every computer is bought with an operating system installed. A machine may therefore be legitimately disposed of with a freshly installed copy of the same system. However, no updated version of the operating system or other software should be installed without a valid licence. This should leave a machine in a suitable state for disposal unless there is confidential or sensitive information on the disk. These disks require a secure wipe and/or physical destruction.

8.1 Reasonable efforts should be made to see if any other unit is able to make use of the equipment.

8.2 Equipment that has residual value may be sold, either to University members or outside bodies, subject to the University's financial guidelines.

8.3 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.

8.4 Older CRT computer monitors and batteries will be disposed of in line with the University Policy UPS S5/11 on the disposal of hazardous waste (https://www1.admin.ox.ac.uk/safety/oxonly/upss511/hazardouswaste/).

8.5 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.

9 Data Breach/Loss & Incident Management

We are obliged under data protection law to report personal data breaches to the ICO (or, in the case of a personal data breach affecting individuals outside the UK, the relevant supervisory authority).

University College has appointed **Simon Buchanan of ClearComm Ltd as its Data Protection Officer (DPO).** The College's Data Protection Coordinator (DPC, currently the Finance Bursar) and the ICT Director (Christopher Thompson) will manage our relationship with the DPO.

If you know or suspect that a personal data breach has occurred:

- do not attempt to investigate or resolve the matter yourself;
- immediately record the incident in simple terms with an email to DataProtection@univ.ox.ac.uk; and
- inform your line manager and/or the Master.

The DataProtection@univ.ox.ac.uk email account is monitored 24/7 and is set up to issue alerts to the Master and the DPC.

You must also preserve all evidence relating to the potential personal data breach. Failure to comply with this policy may result in disciplinary action being taken against you.

9.1 Key Information

9.1.1 We must make our formal notification to the relevant supervisory authority – essentially, the Data Protection Officer - within 72 hours of the breach. The Master and/or the Data Protection Coordinator will inform the DPO. It is therefore crucial that you notify your line manager and/or the Master immediately so that we are able to comply with the law.

9.1.2 We may also need to inform the individual(s) whose data has been subject to the breach. Our DPO shall make the final determination in respect of any notifications to individuals. You are not permitted to notify individuals without prior consultation with, or instruction from, the Master.

9.1.3 All personal data breaches must be notified to our DPO who shall maintain a record of the incidents.

9.1.4 We shall document, with your mandatory cooperation, details of all breaches, their effects and any remedial action taken. We shall investigate whether or not each breach has occurred as a result of human error or a systemic issue, and see how a recurrence can be prevented. Prevention of recurrence may be through better processes, further training or other corrective steps. Failing to notify a breach when required to do so can result in University College incurring a significant fine and any adverse publicity arising from the failure may cause material reputation damage. Please note that failure to abide by our policies and procedures may result in disciplinary action.

9.2 How to Recognize a Personal Data Breach

9.2.1 A personal data breach is any failure that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data whether that failure was unintentional or otherwise.

9.2.2 A personal data breach will have occurred whenever any personal data are lost, destroyed, corrupted or disclosed. This includes circumstances where someone accesses the data or releases it without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

9.2.3 If in any doubt, record the issue via the DataProtection@univ.ox.ac.uk email account and the Master and DPC can work with DPO to make a determination of whether a breach has occurred.

9.3 Do We Have to Make a Notification to the Information Commissioner's Office?

9.3.1 Our DPO shall determine the need to notify the ICO and or the individual(s) affected. We may also need to notify organisations that regulate our activity, and the University of Oxford or other third parties.

9.3.2 In determining whether we must notify the ICO, our DPO shall take account of the latest requirements from the ICO, and establish the likelihood and severity of the resulting risk to people's rights and freedoms including consideration of the possible emotional distress and physical, material or non-material damage to the person such as but not limited to:

- loss of control over their personal data;
- limitation of their rights;
- discrimination;
- identity theft or fraud;
- financial loss;
- unauthorised reversal of pseudonymisation;
- damage to reputation;
- loss of confidentiality of personal data protected by professional secrecy; or
- any other significant economic or social disadvantage to the natural person concerned.

9.3.3 Where it is likely that there will be a risk then we must notify the ICO. Where our DPO determines that a notification is not required, a record shall be kept of the reasons for that decision.

9.3.4 We do not always have to notify individuals of a personal data breach having occurred, only where the breach is likely to result in a high risk to the individual(s) concerned.

9.4 Notification – Our Obligation

9.4.1 Our DPO shall submit our formal notification to the ICO (or, in the case of individuals outside the UK, the relevant supervisory authority) as soon as possible and in any event within 72 hours of being made aware of the breach. Time runs from the time at which the organisation becomes aware of the breach, i.e. that you become aware of the breach and not the time at which our DPO is made aware.

9.4.2 Notification must be made notwithstanding whether or not we are in possession of full details of the breach, damage caused or individuals affected.

9.4.3 In the event that we are not able to make our notification within 72 hours we must give notification immediately thereafter and give reasons for our delay.

9.5 Your Obligation

9.5.1 Record the breach with an email to DataProtection@univ.ox.ac.uk as this will create a dated record of the incident's discovery. Notify your line manager and/or the Master, who, with the Data Protection Coordinator, shall notify our DPO of the breach or issue that has been identified.

9.5.2 You must assist in providing information to the best of your knowledge. If you were not the individual to identify the breach but you are able to assist in providing relevant information, you must cooperate in providing this information so that we are able to make our notification promptly and in any event within the time limit.

9.5.3 When reporting a breach, we must provide:

- details of the breach or issue that has been identified including: a description of the nature of the personal data breach; the nature and approximate number of individuals potentially impacted, and the categories and approximate number of personal data records concerned;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

9.5.4 Where not all information is immediately available, you must provide the information to our DPO as it becomes available and in any event without undue delay. Our DPO shall update the ICO and any other notifiable person with corresponding promptness. Our DPO shall keep the ICO updated of any anticipated or actual delay.

9.6 Notifications to Individuals

Where our DPO has determined that we must notify the individual(s) concerned, we will set out, in clear and plain language, the nature of the personal data breach and, at least:

- the name and contact details of your data protection officer so that the individual(s) can request any further information they may require;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects.

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).
- Lack of resources

10.1 All exceptions to this policy must be approved by the DPO. 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 (for example, host names or IP addresses)
- 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

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

11 Governance

This Policy will be reviewed regularly by the Data Protection Officer. Any changes will be approved by the appropriate authority.

Further Good Practice guides on all topics covered in this policy can be found on OxCerts webpages at:
http://www.it.ox.ac.uk/infosec/istoolkit/

The Governing Body of University College has approved this policy on 13th June 2018 (agenda Item 8.1 under Unreserved Business).

Appendix 1

Data Systems	Location/'Owner'
Payroll	Treasury
Accounts	Treasury
Members Battels	Treasury
Alumni	Development Office
Admissions (u/g)	Academic Office
Admissions (p/g)	Academic Office
Book usage	Library
Various	Maintenance
Various	Bursary
GB & other Committee minutes & agendas	Academic Office

Appendix 2 A strong password has 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 fifteen 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.

Appendix 3 Recommended end user practices for password protection:

- Do not use the same password for University accounts as for other non-University access (e.g. personal ISP account, MRC Portal, option trading, banking, etc.).
- Do not use the same password for various University access needs. Select one password for the IT Services and University Administration systems using the SSO and a separate password for College ICT systems.
- Do not share passwords with anyone, including personal administrative assistants or secretaries.
- Do not reveal a password over the phone to ANYONE.

- Do not reveal a password in an email message.
- Do not reveal a password to a manager, unless exceptional circumstances make this an absolute requirement.
- Do not talk about a password in front of others.
- Do not hint at the format of a password (e.g., "my family name").
- Do not reveal a password on questionnaires or security forms.
- Do not share a password with family members.
- Do not reveal a password to co-workers while on holiday.
- If someone demands a password, refer them to this document or have them call the local ICT Staff.
- Do not use the "Remember Password" feature of applications (e.g., Outlook, Firefox, Safari).
- Do not write passwords down and store them anywhere in your office.
- Do not store passwords in a file on ANY computer system (including Blackberries, iPhones, Palm Pilots or similar devices) without encryption.
- Change passwords regularly in line with the password policies.

Appendix 4 Recommended end user practices to prevent virus problems:

- Always run the standard, supported anti-virus software which is available from the University.
- College installed anti-virus software will be configured to update automatically. On personally owned or remote systems, the user should ensure that updates are performed frequently, and that a licence is renewed annually.
- NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then empty your Trash/Wastebasket.
- Delete spam, chain, and other junk email without forwarding.
- Never download files from unknown or suspicious sources.
- 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.

Appendix 5 Server General Configuration Guidelines:

- Operating System configuration should be in accordance with approved University guidelines.
- Services and applications that will not be used must be disabled where practical.
- Access to services should be logged and/or protected through access-control methods such as TCP Wrappers, if possible.
- The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.
- Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication will do.
- Always use standard security principles of "least required access" to perform a function. Do not use privileged accounts when a non-privileged account will do.
- If a method for secure channel connection is available, privileged access must be performed over secure channels, (e.g. encrypted network connections using SSH or IPsec).
- All security related logs will be kept online for a minimum of 1 week.
- Security-related events will be reported to OxCERT, who will review logs and report incidents to ICT Services management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
    - Port-scan attacks
    - Evidence of unauthorized access to privileged accounts
    - Anomalous occurrences that are not related to specific applications on the host.

Glossary

DPA	The Data Protection Act 1998
DPO	Data Protection Officer
GDPR	General Data Protection Regulation, came into force 25 May 2018
HFS	Hierarchical File Store
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.
VPN	Virtual Private Network as supplied by ICT Services
PREVENT	Prevent is one of four strands of the government's counter-terrorism strategy, and aims to stop people becoming terrorists or supporting terrorism.