Information Security Policy

The following policy has been approved by Keble College. Any amendments to the policy require the College's approval. Each department within the College is required to comply with this policy. Support and guidance for departments is offered by Keble College's HR Manager, Archivist & Records Manager or the IT Department 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.

The Governing Body will review this policy yearly to ensure any new developments are covered and protected.

Overview

Users of information, communications and technology (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

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

The College seeks to maintain the confidentiality, integrity and availability of information about its staff, students, visitors, and alumni and its affairs generally. It is extremely important to the College to preserve its reputation and the reputation of Oxford University and its integral parts. Compliance with legal and regulatory requirements with respect to this information is fundamental.

2. Objective

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, 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 Data Protection Act (Data Protection Act 1998), to ensure the appropriate security measures are in place to prevent any unauthorised access to personal data, whether this is on a workstation or on paper.

3. Scope and definitions

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

- Records relating to students, alumni, academic and non-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.

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

Keble 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 access to 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 their role
- Report any breaches of information security, actual or suspected to the Data Protection Officer (DPO), the Bursar, in a timely manner

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 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 the 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 the Data Protection Act 1998 (DPA) and in accordance with this policy.

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

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

6. Responsibilities

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

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.

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.

The Bursar, as Data Protection Officer is responsible for coordinating the management of information security, maintaining this Information Security Policy and providing advice and guidance on its implementation.

It is noted that failure to adhere to this Policy may 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.

7. Detailed Policies and Guidance

The following shall be complied with throughout Keble 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.

a. **Physical controls for information and information processing assets shall include:**
   - Locked storage facilities (supported by effective management of keys)
   - Locks on rooms which contain computer facilities. 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 (see section 7.8)
   - Encryption of sensitive or confidential information either transmitted or taken outside College's properties

b. Logical controls for information and information processing assets shall include passwords for systems access.

c. Passwords and password management systems shall follow good practice for security and use the following techniques:
   - All system-level passwords (e.g., root, enable, admin, application administration accounts, etc.) should be changed periodically, where appropriate, 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 where possible.
   - 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 where possible.
   - Passwords must not be inserted into email messages or other forms of electronic communication. Passwords must not be attached to or labelled onto portable devices.
   - Any exception to these provisions must be subject to a specific risk assessment and is only permitted where approval is given by the DPO.

d. Each user of the ICT system is responsible for the security of their own password. If a password of an account is suspected to have been compromised, the user must report the relevant incident to the IT team immediately and change all

passwords on all systems. For further standards on password protection refer to **Appendix 3**.

e. Access privileges shall be allocated based on the minimum privileges required and shall be authorised by the appropriate information owner or someone with authority to act on their behalf.

f. All shared computer systems will require users to authenticate before use, and will enable activities to be traced to an authenticated individual with exceptions listed in **Appendix 6**. Those systems listed will be subject to individual risk assessments and annual review.

g. To allow for potential investigations & traceability, network and service access records should be kept for a minimum of one year, or for longer, where considered appropriate.

h. 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. A leaver's line manager is 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. The College recognises that there may be occasions when staff or fellows need to use their own computing equipment to process information (including personal data). Staff arrangements will be at their line manager's discretion. 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:

a. **Privately owned computing equipment or mobile devices 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. Regularly updated Anti-virus software that has been approved by the IT Department must be used on all systems connected to the administered network or used to access personal or sensitive data.. Refer to Appendix 4 for further recommended end user practices to prevent Virus problems.**

b. Information containing personal data that is to be saved onto removable storage or privately owned computing equipment shall be encrypted before storage.

c. The information on removable storage devices should 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.

d. The 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 Keble College, and to servers registered under any Keble College-administered network.

All internal servers deployed in the College must be owned 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 where appropriate, such as the University hierarchical file store. (see section 7.9)

7.3.3. Servers must be registered with the Keble College IT 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

The College's *IT 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**

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

- Ensure IT staff are suitably trained in security
- Proper logs are kept in accordance with OxCERT 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

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)
- 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, where appropriate.

All network activity should be logged in accordance with OxCERT policy.

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

7.5.1. College's policy and procedure on staff use of email and the Internet is included in the Employee Handbook.

7.5.2. Virus or other malware warnings should be forwarded to IT 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:

a. Securing laptops and removable media whether in College or while travelling.

b. Avoiding taking laptops into areas with a high risk of theft and locking such equipment in the boot of a vehicle when leaving it unattended

7.6.2. 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 such as in Internet Cafés or hotels shall be permitted provided that the firewall software provided with the mobile computer or mobile devices are activated and appropriate methods of encrypting network connections used.

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.

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 Employee 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 **or PIN, and should not 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 administered 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 POLICE OR OTHER APPROPRIATE AUTHORITY IMMEDIATELY AND A CRIME REFERENCE NUMBER OBTAINED. IF THE DEVICE IS COLLEGE PROPERTY OR IS THOUGHT TO CONTAIN COLLEGE DATA THEN THE COLLEGE IT DEPARTMENT MUST BE NOTIFIED AS SOON AS POSSIBLE, NO LATER THAN THE NEXT WORKING DAY.**

7.7. **Software Compliance**

7.7.1. College will provide properly licensed and authentic installations of software to all users who need it for their duties, and will ensure the necessary authorisation has been obtained.

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

7.7.3. College's software shall not be given to any outsiders, including students.

7.7.4. The IT team shall maintain a register of authorised software, including the licence information. All licences and media shall be held securely in the IT 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 are included in the Employee 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 period appropriate to the environment (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.

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 or on any shared devices.

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. Backup of Electronic Information

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 IT 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 reasonable 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 where appropriate 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.

8. Computer Equipment Disposal

Keble 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".

Disks that have contained information classed as confidential or sensitive must be securely wiped using a tool that is certified as meeting industry standards or physically destroyed.

9. Data Breach/Loss

Most cases of Data Breach/Loss involve particular IP addresses and will involve an address on either the College's network or the University backbone. In order to allow traceability of security events, proper logs must be kept. Section *7.4 Network Security* details logging requirements in order to comply with this policy.

9.1. Data breach procedures shall be in place to handle loss of data. Such breaches shall include any breaches of this policy. Breaches include but are not limited to:
-data breach/loss/theft
-loss of equipment due to theft
-inappropriate access controls allowing unauthorised access
-equipment failure
-human error
-unforeseen circumstances such as fire and flood
-hacking
-'blagging' offences where data is obtained by deception.

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

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

10. Governance

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

Employee Declaration

I, [name], have read and understand the above *Information Security Policy for **Keble College***, and consent to adhere to the rules outlined therein.

Employee Signature	Date
Manager Signature	Date
IT Administrator Signature	Date

Any employee found to have violated these regulations may be subject to disciplinary action. IT staff will remove access rights to its systems and administered networks from users who contravene the policy guidelines above

Approved by Governing Body on 4th November 2015

Appendix 1

Category	Owner	Other Users/Delegates
Payroll and personal financial information	Financial Controller	Payroll Manager and Deputy Financial Controller, Accounts Assistant (MC), Bursar's PA, HR Manager
College financial information	Bursar	Financial Controller
Personal information on staff and workers	HR Manager	Bursar's PA, Payroll Manager and Deputy Financial Controller, Financial Controller, Accommodation Manager
Information held on University Card	College Office	Bursary Staff, IT Officer, College Office Staff, Financial Controller, IT Manager
Personal information on current students	Senior Tutor	College Office Staff, Bursary Staff, Porters Lodge
Personal information on prospective students	Senior Tutor	College Office Staff
Personal information on former students	Director of Development	Development Staff
Financial information on former students and donors	Director of Development	Development Staff
Security information on computer and network usage	IT Manager	IT Officer
Security information on door access	IT Manager	IT Officer
Security information on CCTV	Domestic Bursar	Head Porter
Personal information on Fellows	Warden	Warden's PA, HR Manager

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 IT systems.
- Do not share personal 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 IT 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, (eg. 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 IT 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.

Appendix 6 Exceptions for shared access systems without individual authentication

Shared Access Computers	**Notes**
Porters' Lodge	Immediate access needed by certain on-duty staff identifiable by rota
SCR Pantry	
Kitchen	
Dining Hall	
Workshop	
Facilities Co-ordinators	
Library Front Desk Staff PC	Limited access shared account used by on-duty library assistant
Library search terminals	Managed by central University IT Services; can be used with no authentication to access Internet; not connected to administered network
Fellows' PCs in shared offices	
Conference laptops	Used by visitors; not connected to administered network

Glossary

DPA	The Data Protection Act 1998
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 IT Services