Regent's Park College

Information Security Policy

1. Overview

Users of ICT within the University are subject in the first instance to the University IT regulations (2002) with subsequent amendments and available for review at: https://www.ox.ac.uk/about/how-we-are-run/governance-finance/legislation/it-regulations-1-of-2002.

The College has a statutory duty to comply with all relevant legal and regulatory obligations relating to the use of information and communication technologies. This includes, but is not limited to: duties under data protection, intellectual property, equality, safeguarding, and counter-terrorism legislation. Accordingly, the College reserves the right to monitor IT use where necessary to ensure compliance with the law and with the College's acceptable use policy. Any suspected breaches will be reviewed and investigated by an independent panel of College members.

The University 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/College 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.

2. Introduction

Regent's Park College seeks to maintain the confidentiality, integrity and availability of information about its staff, students, visitors, and alumni and its affairs generally, including any 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.

3. 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
- Undertaking mandatory information security and data protection training as and when required
- 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 UK GDPR (General Data Protection Regulations, 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 safeguard it against unauthorized access or theft.

4. Scope and definitions

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

- Records relating to pupils, students, alumni, administrative staff, academic staff, volunteers, 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
- All data assets whether they are physical (paper) or digital.

This policy covers all data access and processing pertaining to the College, and all staff and other persons (including Trustees, 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.

5. Policy

Regent's Park College aims 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. Training resources are available via the University.
- Report any breaches of information security (actual or suspected) to the Data Protection Officer (DPO: data.protection@regents.ox.ac.uk) immediately.

- Ensure that data is only accessible by staff who need it for their role.

More detailed policy statements and guidance are provided in Section 7 of this Policy.

6. Responsibilities

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

Governing Body requires the head of each department and area 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 they use to perform their duties.

Every user is required to obey all laws, including criminal, counterterrorism, copyright, defamation and obscenity laws. The College will render all reasonable assistance to enforcement officials (police and authorised University IT staff) for the investigation and prosecution of people using technology in violation of any law.

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 severe financial loss including fines, operational incapacity, and loss of reputation. Data access, processing or destruction 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 Regent's Park College.

7.1. **Access to Information and Information systems**

7.1.1. Information assets shall be 'owned' by a named officer within College. An information asset is any data, record or system that holds value to the College and must therefore be managed and protected appropriately. In the context of data protection, information assets include all forms of information – digital or physical – that the College creates, collects, store, processes or transmits, and that have importance to its operations, decision-making, or legal obligations.

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 7.10 of this policy)
- Encryption of data either transmitted or taken outside College's properties

- Logical controls for information and information processing assets shall include passwords for systems access, unique "per-user" accounts, role-based access control mechanisms, and multi-factor authentication (where available)
- 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. Usually this is on an annual basis in line with the University's guidance. 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 unless otherwise allowed by University policies or procedures. If a password must be shared with others in order to open secure documents or zip files, then please follow these guidelines:
  - Unless otherwise allowed in University policy and procedures, passwords must not be sent in clear text by e-mail or written on/in the document.
  - Staff must use university-approved secure methods for transmitting passwords. This could be the use of a person to person Teams Chat or text message.
  - Passwords must be **unique, strong, and changed** if there is any suspicion of compromise.
  - Responsibility for safeguarding shared passwords lies with both sender and recipient.
- 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 the password. 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.
- All shared computer systems will require users to authenticate before use, and will enable activities to be traced to an authenticated individual.
- 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 for the Shared drive, OneDrive and Sharepoint regularly.

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. 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 the IT team, who are authorised to perform systems administration or management functions.

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

7.2 UK GDPR and Data Protection

7.2.1 Users must take particular care when sharing or disclosing personal data[1] to any third party, to ensure compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, and the Data (Use and Access) Act 2025 (DUAA). Personal or special category data is shared within the collegiate universityin accordance with the University's data sharing protocol.

In certain circumstances—such as requests from law enforcement or other statutory bodies—information may be disclosed without consent where there is a legal requirement or lawful basis to do so. In such cases, users must verify the legitimacy of the request, ensure that only the minimum necessary information is shared, and record the decision and rationale for disclosure. All of these special circumstance disclosures must also be approved by the DPO.

[1] *Personal data is defined in the UK GDPR[1] as "Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." NB this only applies to living persons.*

7.2.2 To allow for potential investigations & traceability, electronic access logs (where available) should be kept for a minimum of six monthsr longer, Logs could include user and group memberships, authentication details, access activity, systems events, and audit trails. Logs are owned and managed by the IT team.

7.2.3 Further information on UK GDPR and Data Protection may be found on the College website.

7.3 Monitoring

7.3.1 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.

7.3.2 Any exception to these provisions must be subject to a specific risk assessment and is only permitted where approval is given by the Director of Operations.

7.4. Use of Personal Computer Equipment and Removable Storage

7.4.1 Regent's Park College recognises that there may be occasions when staff need to use their own computing equipment to process information (including personal data). Point 6.1.2 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.

7.4.2 Staff are responsible for ensuring that their own equipment is configured securely if they use it for College work. Further information can be found on the University intranet.

7.4.3. It is required that:

- Privately owned computing equipment used to process College information or connect to the College network must have appropriate and sufficient anti-virus protection. Refer to **Appendix 4** for further recommended end user practices to prevent computer viruses.
- No personal data shall be stored on removable storage devices unless absolutely necessary, and permission must be sought from the DPO. Removable storage devices must be password-encrypted. They must not in any circumstances leave College property.

7.5. Servers

This policy specifically applies to server equipment owned and/or operated by Regent's Park College, and to servers registered under any Regent's Park College-administered network.

7.5.1 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.

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

7.5.3. Servers should be backed up to offsite storage, such as the University HFS.

7.5.4. Servers must be registered with the Regent's Park 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

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

Regent's Park College IT team 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.

7.6. **Network Security**

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 administrators are suitably trained in security.
- Ensure that proper logs are kept in accordance with University IT Services policies.
- Review file system security to ensure users have only the access they need.
- 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.
- Remove permissive firewall rules once there is no longer a business requirement.
- Permit remote access to firewalls (e.g. for configuration or monitoring) only when there is a clear, documented business requirement and appropriate authorisation, subject to periodic review.
- 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)
- Port scanning
- System intrusion originating from a protected system behind a firewall

- System intrusion originating from outside the firewall
- Network intrusion
- Denial of services
- Any other relevant security events
- Login and log-off activities

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

Further information on network security and good practice can be found on the University intranet.

7.7. Email and Internet Use

Policy for the use of ~~electronic~~ mail is covered by the University's IT regulations.

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

7.7.2. 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.

7.7.3 Users are not permitted to use University IT or network facilities with the intention of drawing people into terrorism (under the University's statutory *Prevent* duty).

7.8. Mobile Computing

This applies to any mobile hardware that is used to access College resources, whether the device is owned by the user or by the College.

7.8.1. 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.
- Taking laptops with you at all times, and never leaving them (even locked in the boot) in an unattended vehicle.

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

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

7.8.4. 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 programs. Regular updates of anti-malicious software files should occur automatically on connection to the Internet.

7.8.5. 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.

7.8.6. Mobile Device Security

- **Anyone** 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 must never be shared with anyone.** Alternatively, biometrics may be used, but the use of face-recognition to access sensitive information is not recommended.

- Any mobile device that is used to access College resources 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. A **jailbroken device** is a smartphone, tablet, or other electronic device whose manufacturer-imposed operating system restrictions have been deliberately removed or bypassed. This is usually done by exploiting security vulnerabilities to gain "root" or administrator-level access.

ANY COLLEGE-PROVIDED MOBILE DEVICE THAT IS STOLEN OR LOST MUST BE REPORTED TO THE IT TEAM AND DPO IMMEDIATELY, REGARDLESS OF DATE/TIME. USE THE DATA PROTECTION MOBILE NUMBER OR THE UNIVERSITY CENTRAL IT SERVICE DESK WHEN NEEDED.

7.9. **Software Compliance**

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

7.9.2. 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 team is responsible for giving authority and approval for software suitable for loading on College equipment

7.9.3. 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.

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

7.9.5 Further Software Usage guidance is included in the Employee Handbook.

7.10. **Clear Desk/Clear Screen**

7.10.1. 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 secured if desks are to be left unattended in unlocked/open access offices.

7.10.2. 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.

7.10.3. Documents shall be immediately retrieved from printers and photocopiers.

7.10.4. 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 10-15 minutes is a suitable time.

7.10.5. Unattended laptop computers, mobile telephones and other portable assets and keys must be screen locked and/or otherwise secured e.g. in a locked office, within a lockable desk, or by a lockable cable.

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

7.10.7. The College shall ensure that members of staff have suitable storage facilities to enable them to comply with these procedures.

7.11. **Information Backup**

7.11.1. 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.

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

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

7.11.4. 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;
- be immutable and "air-gapped" to reduce risk of cyber/malware attacks.

Back-ups should be scanned as they are being created to avoid backing up malware. Up-to-date systems should be used to detect previously undetectable malware.

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

7.11.6. 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.

7.11.7 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.

7.12. Cloud Storage and Services

No cloud services other than approved University systems shall be used for storing, transmitting or otherwise processing personal data.

7.13 Use of AI

The University's guidance on the use of AI must be followed.

7.14 "Smart glasses" and similar devices

Consumer AI devices that are 'always on' – such as AI-enabled glasses with cameras, microphones, on-device processing, and facial or biometric identification bring serious risks to privacy, security, academic freedom and safety. They must not be used on College premises unless they are a disability aid for someone with a registered disability.

8. Computer Equipment Disposal

8.1 Regent's Park 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 on the University intranet.

8.2 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.

8.3 Older CRT computer monitors are defined as hazardous waste, and arrangements for their disposal must be handled through the IT team, who will arrange for their disposal.

8.4 The College IT team is responsible for the safe removal, disposal and erasure of all data of unneeded computer systems, in compliance with University procedures and regulations.

8.5 Disks that have contained information classed as confidential or sensitive must be securely wiped or physically destroyed.

8.6 Anyone seeking an exemption to this policy must make a request in writing to the DPO and the IT team.

9. Data Breach/Loss

9.1 Any actual or potential breach involving personal data (e.g. mis-directed e-mails or failure to BCC, confidential papers left unattended on photocopier/printer or in open areas etc.) must be reported to the DPO (data.protection@regents.ox.ac.uk) ***immediately*** in accordance with the Data Protection Policy.

9.2 Any actual or suspected data loss must be reported to the IT team (and to the DPO if any of the lost data is personal data).

9.3. Both the College IT team and the University Computer Emergency Response Team (OxCERT: oxcert@infosec.ox.ac.uk) must be informed about information security related incidents e.g. malware, ransomware, phishing emails, compromised passwords, or lost or stolen devices.

Employee Declaration

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

Employee 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.

Appendix 1

Data Systems	Location/'Owner'
Payroll	Director of Finance
Accounts	Director of Finance
Junior Members	Academic Office
Senior Members	Principal's Office
Alumni	Development Office
Admissions (u/g)	Academic Office
Admissions (p/g)	Academic Office
Book Usage	Library
Various	Maintenance
Various	Director of Operations
GB & Cttee minutes & agendas	Director of the Principal's Office/relevant committee secretary

Appendix 2 Creating a strong password

Please refer to the guidance on the University intranet. In summary:

Do

- Use a minimum of 16-character passwords for all University accounts.
- Use a password manager like LastPass or KeePass to generate and store long, random, complex passwords.
- If you must write down any password, keep it somewhere secure that only you can access.

Don't

- Use one long word, even an obscure one.
- Re-use passwords.
- Use something you have already used as an answer to a security question on any system.
- Use passwords based on personal information that another person might be able to guess or discover online. Examples include: your college or department, names of family, friends or pets, birthdays, car registrations, etc.

Appendix 3 Recommended ~~end user~~ practices for password protection:

- Do not use a single password for more than one service/account.
- 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.
- Do not write passwords down and store them anywhere in your office.
- Do not store passwords in a file on ANY computer without encryption.
- Change passwords regularly in line with the password policies.
- Use a password manager to securely store passwords. Reputable and widely-used options like LastPass, 1Password, KeePassXC and Bitwarden are good options.

Appendix 4 Recommended 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 systems, see the guidelines on the University intranet.
- 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 ask the IT team to 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 physical and application firewalls, 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 Oxford University Computer Emergency Response Team (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.