2014

LMH
Lady Margaret Hall

Information Security Policy

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

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 College employee and affiliate who deals with information and/or information systems. It is the responsibility of every 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

Lady Margaret Hall 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 the University of Oxford. Compliance with legal and regulatory requirements with respect to this information is fundamental.

2. Objective

This policy defines the framework within which information security will be managed by the College. The policy is meant to keep information secure and highlights the risks of unauthorized access or loss of data.

All users of information, whether physical 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 and following applicable guidance

Information relating to living individuals (such as may be found in personnel, payroll, and student and alumni record systems) should only be stored in the appropriate secure systems and is subject to legal protection. All users of such information are obliged, under the terms of the DPA (Data Protection Act 1998), to ensure the appropriate security measures are taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data, whether physical or electronic. 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.

3. Scope and definitions

The scope of this policy extends to all Lady Margaret Hall's information and its operational activities including but not limited to:

- Records relating to students, alumni, staff, visitors, conference guests and external contractors where applicable
- Operational plans, accounting records, and minutes
- All processing facilities used in support of the College's operational activities to store, process and transmit information
- Any information that can identify a person, e.g. names and addresses.

This policy covers all data access and processing pertaining to the College's information, and covers all staff and other users of information. Any reference to staff shall be regarded as relating to permanent, temporary, contract, and other support staff as applicable.

4. Policy

Lady Margaret Hall 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.
- 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 policy to all persons potentially accessing data
- Provide information security training to all persons appropriate to the role
- Report any breaches of information security, actual or suspected to the Data Protection Officer (DPO) in a timely manner.

More detailed 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 Lady Margaret Hall'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.

6. Responsibilities

The Governing Body of Lady Margaret Hall is responsible for approving this policy and ensuring that it is regularly reviewed.

Governing Body requires each student, academic staff member and support staff member of the College to be accountable for implementing an appropriate level of security control for College information that he/she uses, processes or accesses.

The DPO is responsible for coordinating the management of information security, maintaining this 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 Lady Margaret Hall.

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
- 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 1** 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 2**.
- 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 the Data Protection Act. The permission of the information asset owner should be sought before the release of personal or sensitive information.
- All shared computer systems will require users to authenticate before use, and will enable activities to be traced to an authenticated individual.
- To allow for potential investigations & 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. Lady Margaret Hall 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 3** for further recommended end user practices to prevent Virus problems.
- Information containing personal data concerning students, alumni or staff that is to be saved onto removable storage or privately owned computing equipment shall be encrypted before storage.

- The information 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.
- Lady Margaret Hall 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 Lady Margaret Hall, and to servers registered under any Lady Margaret Hall-administered network.

All internal servers deployed in the College must be owned by an operational group that is responsible for system administration. 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.

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 Lady Margaret Hall 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.

7.4. **Network Security**

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

- Ensure network 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.

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. 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.

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.

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 by 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

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

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

8. Computer Equipment 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.

9. Data Breach/Loss

9.1. Data breach procedures shall be in place to handle any 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 ICT Manager 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.

10. Governance

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

The Governing Body of Lady Margaret Hall has approved this policy on.

DATE:_____ MINUTE:_____

Appendix 1 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 for system-level access and six for user-level access, 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 2 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 3 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.

  -

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/)
SSO	The University of Oxford Single Sign-On username
VPN	Virtual Private Network as supplied by IT Services