Information Security Policy

Balliol College seeks to maintain the confidentiality, integrity and availability of information about its staff, students, visitors and alumni and its affairs generally. Compliance with legal and regulatory requirements with respect to this Information is fundamental.

What we aim to do

Balliol College aims, as far as reasonably practicable, to:

- Protect the confidentiality, integrity and availability of all data it holds in its systems. This includes the protection of any device that can carry data or access data, as well as protecting physical paper copy of data wherever possible (e.g. clean desk policies).
- Meet legislative and contractual obligations
- Protect the College’s intellectual property rights
- Produce, maintain and test business continuity plans in regards to data backup and recovery
- Prohibit unauthorised use of the College’s information and systems
- Communicate this Information Security Policy to all persons potentially accessing data
- Provide information security training to all persons appropriate to the role
- Report any breaches of information security, actual or suspected to the Data Protection Officer (Domestic Bursar) in a timely manner

We must, therefore:

- Treat information security seriously
- Maintain an awareness of security issues
- Adhere to applicable security policies and follow guidance

- In particular, 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 1998 (DPA), 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 stored in filing cabinets in offices.

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.

How we do it:

**Governing Body Responsibilities**

Governing Body needs to approve the policy annually
The College has nominated an IT Fellow to oversee ICT within the College. She is also the Data Protection Officer.

The IT Fellow and DPO will ensure that the IT department adhere to the policy and will promote secure storage of both electronic and paper data.

**IT Department**

**Access to Information and Information systems**

In order to help keep electronic data secure, the IT department will restrict authorised users and some data may also be password protected. In addition the IT department will ensure:

- Visitors (both academic and conference guests) to the College are provided with specifically assigned credentials which are appropriately authenticated and automatically disabled at the end of their term with the College.

**Servers**

- Physical servers must be housed in a location where physical access and the server environment (power, temperature, and humidity) can be controlled.
- Servers should be backed up to offsite storage, such as the University HFS.
- Servers must be registered with the Balliol College Computing Department. 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
- Balliol College Computing Department 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.
- All internal servers deployed in the College must be administered by the systems administration team. Approved server configuration guides must be established and maintained and monitoring configuration compliance; a process for changing the configuration guides, which includes peer review and approval must be established.
  - All network activity should be logged in accordance with University IT Services policy. It is currently recommended that at least 60 days of logs be kept, and longer if possible to allow for any post-incident review. Logs must include identifiable data to enable traces back to specific events, computer systems, and specific users. Timestamps, MAC addresses, IP Addresses, and where possible usernames should be included in logging systems. These logs should be proactively...
monitored and reviewed as an early warning system for hacking or any other form of unauthorized activity.

- College will provide properly licensed and authentic installations of software to all users who require it in the course of their duties.
- The College’s software shall only be distributed and used as licenced.
- Backup for physical information assets - for example printed paper documents, and media containing information – shall be governed as appropriate by the same principles.

**Network Security**

Responsibility for management and security of the College’s internal network rests with the Computing Department. The IT Fellow must ensure that a systems administrator is suitable trained in security.

The systems Administrator must:

- Ensure proper logs are kept in accordance with OxCert policies (*The University of Oxford Computer Emergency Response Team (OxCERT) is based within the Networks and Telecommunications Group within the University of Oxford's IT Services - http://www.oucs.ox.ac.uk/network/security/about/*).
- Protect the physical network from interception/damage/interference
- Restrict unauthorised 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:

- Unauthorised access attempts on firewalls, systems, and network devices (only authorised 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 OxCert 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.

- Further information on network security and good practice can be found within the ITSS IS Toolkit [http://www.it.ox.ac.uk/infosec/istoolkit/]
Information Backup

- The Computing Department shall be responsible for ensuring that systems and information are backed up in accordance with the defined requirements.
- Accurate and complete records of the back-up copies shall be produced and maintained.
- The back-ups shall be stored in a remote location which must meet the following criteria:
  1. be a sufficient distance to escape any damage from a physical disaster at the College
  2. be accessible
  3. afford an appropriate level of protection to the back-up media in terms of its storage and transportation to and from the remote location

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

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.

Computer Equipment Disposal

Balliol 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/](http://www.ict.ox.ac.uk/oxford/disposal/)

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

Staff, Fellows, Students and Individuals

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

Data holders should make risk assessments of types of information they hold to determine the level of security required and these should be reviewed periodically. Everyone must ensure that physical controls for paper records will also exist including locked files and rooms, clear desk policy and encryption of data transmitted or taken outside the College.
Encryption of data should be appropriate to the level of risk assessment of the data.

Non-University Cloud Storage and Services

The use of cloud services for the processing and/or storage of personal or sensitive information should be risk assessed and adhere to all other sections of this policy. Personal cloud services accounts may not be used for the storage, manipulation or exchange of College-related communications or College-owned data

Personal and Commercially sensitive Data

Personal data must be handled in accordance with the Data Protection Act 1998 (DPA) and in accordance with this policy. This is the most sensitive of all data and must be kept securely in both electronic and paper forms.

Commercially and otherwise sensitive material should be distributed sparingly and disposed of securely (shredded)

- Privately owned computing equipment used to process College information or connect to the College network must have up-to-date anti-virus software installed
- Information containing personal data concerning pupils, students, alumni or staff that is to be saved on to removable storage or privately owned computing equipment shall be encrypted before storage if deemed appropriate.
- Sensitive data 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 if appropriate.
- Balliol 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).

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.)

- 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:
- Persons using computing equipment in public places shall ensure that confidential information cannot be viewed by unauthorised persons
- When using external wireless access points firewall software provided with the mobile computer must be activated.
- Mobile computer and smart phone users are required to ensure that software controls and updates are installed and regularly updated to protect the devises from viruses, spyware and similar malicious programmes. Such updates should occur automatically on connection to the Internet.
- 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.

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 suitable password or PIN, and that password or PIN must never be shared with anyone.

• **Mobile devices** should not be used to carry sensitive College data for any longer than absolutely necessary and any data on the device should be encrypted if possible.

**Clear Desk/Clear Screen**

• Outside normal working hours, all confidential information, whether marked up as such or not, shall be secured; for example in 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.

• Confidential printed information to be discarded must be placed in an approved confidential waste container (shredder box) as soon as reasonably practical and kept secure until that time.

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

• 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 unauthorised access to the network. It is suggested that 15 minutes is a suitable time.

• 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.

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

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

**Staff**

**Email and Internet Use**

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

Balliol does not operate an email system currently so centrally hosted email is monitored by ITS and their information policy will take precedence.

Balliol’s policy and procedure on staff use of email and the Internet is included in the Staff Handbook.

**Software Compliance**

• College will provide properly licensed and authentic installations of software to all users who need it.
• Users of College computer equipment and software shall not copy software or load unauthorised/unapproved software on to a College computer including mobile equipment. The IT Director is responsible for giving authority and approval for software suitable for loading on College equipment.

• Balliol’s software shall not be given to any outsiders, nor to students.

2. Data Breach/Loss

Data breach procedures shall be in place to handle loss of data. 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.

Any breach should be immediately reported to the Computing Department; 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/](http://www.it.ox.ac.uk/infosec/istoolkit/)

**Governance**

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

*Further Good Practice guides on all topics covered in this policy can be found on OxCert’s webpages at:* [http://www.it.ox.ac.uk/infosec/istoolkit/](http://www.it.ox.ac.uk/infosec/istoolkit/)

The Governing Body of Balliol College has approved this policy on:

DATE: 5 December 2016 MINUTE: CM16/227