Brasenose College Information Security Policy (ISP v1.5)

1. Introduction
Brasenose 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, Alumni 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 Brasenose College’s information and its operational activities including but not limited to:

- Records held by the College relating to pupils, 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, and all staff and other persons (including students, Fellows, Lecturers, JCR/HCR 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
Brasenose 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 is owned by the college 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 on college systems and owned devices.
• 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 Brasenose 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 Information Security framework and for issuing and reviewing policy statements and procedures to support Brasenose College, consistent with the University’s 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 DPO is responsible for coordinating the management of information security, maintaining this Information Security Policy and providing advice and guidance on its implementation.

It is noted that failure to adhere to this Policy may result in the College suffering financial loss (arising both as 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. Access to Information and Information systems

7.1.1 Information assets shall be owned by a named section 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.
- PCs and other devices in lockable areas. Exits covered by CCTV
- “Clean desk” policies.
- 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 regularly. These passwords should be changed on at least a yearly basis.
- The use of strong authentication (minimum length, high complexity, non-reusable passwords).
- Users to have the ability to change their passwords at any time
- 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 is responsible for the security of their own password. If a password of 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.
- 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.
• To allow for potential investigations, access records should be kept for a minimum of six months, or for longer, where considered appropriate.
• External access to the College’s administered networks via a combination of remote access via Brasenose College VPN Service provided by the college ICT Office and Remote Desktop to a user’s personal terminal on a non-standard secure Remote Desktop Port.

7.1.3. Information owners shall review access permissions on a biannual 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 leaver’s 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. Domain administrator privileges – those that are capable of overriding system and application controls on multiple devices college wide – shall be restricted to those persons who are authorised to perform systems administration only. 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.
7.1.9 All internal documents that contain personal or sensitive information and which may be distributed internally via email should have password security applied to reduce risk of accidental distribution.

7.2. Use of Personal Computer Equipment and Removable Storage

7.2.1. Brasenose College recognises that there may be occasions when staff need to use portable equipment provided by the college, to access information (including personal data). The college must ensure all such devices provided are fully encrypted before deployment and users are aware of this policy.
7.2.2. The College recognises that there may be occasions when staff need to use their own computing equipment to access information (including personal data and emails). Users should ensure such devices are password protected and where appropriate and reasonable, with support of the college ICT department, encrypted. Departmental Heads reserve the right to revoke access to systems on personal devices where data contained/transmitted is deemed sensitive or the personal device is not suitable.
7.2.3. It is good practice and required that:
• Privately owned computing equipment used to access College information or connect to the College network must be password protected, have up-to-date anti-virus software installed, all relevant operating system updates and all third party program updates the ICT Office deems necessary.
• If the DPO allows College information containing personal data concerning pupils, students, alumni or staff to be saved onto non-encrypted removable storage or college owned portable equipment, it shall be encrypted before storage. A Risk Assessment must also be completed.
• Brasenose 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,
or portable device provided by the college, is uploaded onto College systems, it shall be deleted from the removable storage device).

- The use of personal devices to access emails is permissible, but in the case of college non-academic staff line managers reserve the right to revoke such permission. It is advised that users seek guidance from either the College ICT Office or their local ICT Support in ensuring that the setup of the email connections is secure, devices are secured with key locks/passwords and, where appropriate or feasible, device encryption is used. Users should understand and be able to perform the ‘remote wipe’ feature available in the Nexus email system should the device be lost.
- The College reserves the right to stop transmission or access to any of the data it owns if this policy is not followed.

7.3 Servers

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

All internal servers deployed in the College are to be managed by the ICT department unless permission is granted by the DPO. Configuration policies are to be created and updated on all servers.

7.3.1 Servers must be physically located in an access-controlled and environment-controlled room.
7.3.2 Servers should be backed up off site to the University’s HFS
7.3.3 Servers must be registered with the Brasenose College IT Staff. If the server is not be managed by college ICT staff, 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 IT team. The IT Manager (or in absence, Infrastructure Officer) for the College must:

- Ensure ICT Staff [network administrators] 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)
- 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 recommend 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/

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 should be included in the Staff 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. Software Compliance

7.6.1. 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.
7.6.2. 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
7.6.3. College’s software shall not be given to any outsiders, including pupils/students.
7.6.4. The IT team shall maintain a register of authorised software, including the licence information. All licences and media shall be held securely by the IT team.
7.6.5. Licensed software shall be removed from any computer that is to be disposed of outside of the College.
7.6.6 Further Software Usage Policies should be included in the Staff Handbook.
7.6.7 Purchase of software by any member/department of the college for use on a college device must first satisfy the college’s Software Purchase Policy found in Appendix 2 of this document.

7.7. Clear Desk/Clear Screen

7.7.1. 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.
7.7.2. 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.
7.7.3. Documents shall be immediately retrieved from printers, photocopiers and fax machines.
7.7.4. All desktop computers must be logged off or locked automatically after 10 minutes (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.

7.7.5. 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.

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

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

7.8. Information Backup

7.8.1. 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.

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

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

7.8.4. 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

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

7.8.6. Restoration procedures shall be regularly checked and tested to ensure that they are effective.

8.0 Computer Equipment Disposal

Brasenose 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.

Older CRT computer monitors are defined as hazardous waste, and arrangements for their disposal must be handled through the IT Manager.

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

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

8.1.1. Reasonable efforts should be made to see if any other unit is able to make use of the equipment.
8.1.2. Equipment that has residual value may be sold, either to University members or outside bodies, subject to the University's financial guidelines.

8.1.3. Where equipment has limited resale value, consideration should be given to whether it can be donated to any charitable or community project. If the equipment cannot be reused, then it should be recycled or disposed of in an environmentally-friendly manner.

8.1.4. Older CRT computer monitors and batteries will be disposed of in line with the University Policy UPS S5/11 on the disposal of hazardous waste.

8.1.5. Disks that have contained information classed as confidential or sensitive must be secure wiped using a tool such as PGP or DBAN or physically destroyed.

9.0 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. The College Data Protection Breach Policy (Annex 1 of this Policy) 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 as per the college’s Data Protection Breach Policy (Annex 1). All investigations should be carried out urgently and reviewed once the issue has been resolved.

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

10.0 Governance

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

11.0 Enforcement

11.1 Breaches of the Systems and Data Access Control Policy could lead to civil or criminal actions against the individual or the College.

11.2 Non-compliance with the general principles and conditions of this policy may lead to disciplinary action being taken up to and including dismissal.
Annex 1 - BRASENOSE DATA PROTECTION BREACH POLICY

This policy is part of the Information Security Policy. Please refer to the Information Security Policy for more details on how data is protected and secured by the College, and what duties each individual has to ensure that data is secure.

Policy Statement

Brasenose College holds large amounts of personal and sensitive data. Every care is taken to protect personal data and to avoid a data protection breaches (see full Information Security Policy). In the unlikely event of data being lost or shared inappropriately, it is vital that appropriate action is taken to minimise any associated risk as soon as possible.

Purpose

This policy sets out the procedure to be followed by all Brasenose College staff if a data protection breach takes place.

Scope

This policy applies to all personal and sensitive data held by Brasenose College.

Types of Breach

Data protection breaches could be caused by a number of factors. Some examples are:

- Loss or theft of data or equipment on which data is stored
- Inappropriate access controls allowing unauthorised use
- Equipment Failure
- Human Error
- Unforeseen circumstances such as fire or flood
- Hacking
- Offences where information is obtained by deception

Immediate Containment/Recovery

1. The person who discovers/receives a report of a breach must inform their line manager. If the line manager is not available then the breach must be reported to the Bursar, ICT Manager or Domestic Bursar. If the breach occurs or is discovered outside normal working hours, it should be reported as soon as is practicable.

2. The line manager must ascertain whether the breach is still occurring. If so, steps must be taken immediately to minimise the effect of the breach. An example might be to shut down a system, or to alert relevant staff. If in doubt, ask for assistance from ICT staff.
3. The line manager must inform the Data Protection Officer as soon as possible. Currently, that is the Bursar. In his absence please inform either the ICT Manager or Domestic Bursar.

4. The Data Protection Officer must also consider whether the police need to be informed. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future given the nature of information lost.

5. The line manager or Data Protection Officer must ensure that the appropriate steps are taken quickly to recover any losses and limit the damage. Steps might include:
   a. Attempting to recover lost equipment.
   b. Contacting any affected individuals or departments so that they are prepared for any potentially inappropriate enquiries ‘phishing’ for further information on the individual concerned. Consideration should be given to a global email. If an inappropriate enquiry is received by staff, they should attempt to obtain the enquirer’s name and contact details if possible and confirm that they will ring the individual making the enquiry back. Whatever the outcome of the call, it should be reported immediately to the Data Protection Officer.
   c. Contacting the relevant teams so that they can be prepared to handle any press or other enquiries that may result.
   d. The use of back-ups to restore lost/damaged/stolen data.
   e. If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use.
   f. If the data breach includes any entry codes or passwords, then these codes must be changed immediately, and the relevant agencies and members of staff informed.

Investigation

In most cases, the next stage would be for the College to fully investigate the breach and ascertain whose data was involved in the breach, the potential effect on the data subject and what further steps need to be taken to remedy the situation. The Data Protection Officer must ensure the investigation occurs, and the investigation will usually involve the ICT Manager and the relevant line manager.

The investigation should consider the type of data, its sensitivity, what protections are in place (e.g. encryption), what has happened to the data, whether the data could be put to any illegal or inappropriate use, how many people are affected, what type of people have been affected (the public, suppliers etc) and whether there are wider consequences to the breach.

A clear record should be made of the nature of the breach and the actions taken to mitigate it.

The investigation should be completed urgently and wherever possible within 24 hours of the breach being discovered/reported. A further review of the causes of the breach and recommendations for future improvements can be done once the matter has been resolved.
Notification

Some people/agencies may need to be notified as part of the initial containment. However, the decision will normally be made once an investigation has taken place.

The Data Protection Officer should, after seeking legal advice, decide whether anyone should be notified of the breach. The DPO should also liaise with the College Accountant about informing the insurers.

In the case of significant breaches, the Information Commissioner’s Office (ICO) should be notified. Every incident should be considered on a case by case basis. The following points will help you to decide whether and how to notify:

• Are there any legal/contractual requirements to notify?

• Will notification help prevent the unauthorised or unlawful use of personal data?

• Could notification help the individual – could they act on the information to mitigate risks?

• If a large number of people are affected, or there are very serious consequences, you should notify the ICO. The ICO should only be notified if personal data is involved. There is guidance available from the ICO on when and how to notify them, which can be obtained at


• Consider the dangers of over-notifying. Not every incident warrants notification and over-notification may cause disproportionate enquiries and work.

• The notification should include a description of how and when the breach occurred and what data was involved. Include details of what you have already done to mitigate the risks posed by the breach.

• When notifying individuals, give specific and clear advice on what they can do to protect themselves and what you are willing to do to help them. You should also give them the opportunity to make a formal complaint if they wish (see the Council’s Complaints Procedure).

Review and Evaluation

Once the initial aftermath of the breach is over, the Data Protection Officer should fully review both the causes of the breach and the effectiveness of the response to it. A report should be written and sent to the next available meetings of the relevant governance committees for discussion. If systemic or ongoing problems are identified, then an action plan must be drawn up to put these right. If the breach warrants a disciplinary investigation, the manager leading the investigation should liaise with Human Resources for advice and guidance.

This policy may need to be reviewed after a breach or after legislative changes, new case law or new guidance. Consideration should be given to reviewing this policy on an annual basis.
Implementation

This policy takes effect immediately. All managers should ensure that staff are aware of this policy and its requirements. This should be undertaken as part of induction and supervision. If staff have any queries in relation to the policy, they should discuss this with their line manager or the Chief Officer Legal & Governance.

Useful Contacts

Data Protection Officer (PP) 01865 277871
bursar@bnc.ox.ac.uk

ICT Department 01865 277513
computer.office@bnc.ox.ac.uk

ICT Manager 01865 287149
john.kinsey@bnc.ox.ac.uk