Brasenose College Information Security Policy (ISP v1.7)

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 unauthorised 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, Payroll, 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 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.

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 copies 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 processing or handling college 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) within 24 hours.

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 General Data Protection Regulations and in accordance with this policy.

5.7 The GDPR 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 'special category data', which is defined in the GDPR as data relating to race, ethnic origin, religion, genetics, biometrics (where used for ID purposes), health, sexual life, sexual orientation, politics, or trade union membership.

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 ensuring the College has an appropriate information security policy and that it is followed. In particular, the DPO needs to oversee subject access requests and responses to data breaches.

The ICT Manager assists the DPO by coordinating the day to day 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 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.

There are two tiers of fine imposable on the college:

The lower level of fine, up to €10 million or 2% of the college's annual turnover (whichever is greater), will be considered for infringements listed in Article 83(4) of the General Data Protection Regulation.

This includes infringements relating to:

Integrating data protection 'by design and by default'
Records of processing activities
Cooperation with the supervising authority
Security of processing data
Notification of a personal data breach to the supervisory authority
Communication of a personal data breach to the data subject
Data Protection Impact Assessment
Prior consultation
Designation, position or tasks of the Data Protection Officer
Certification

The higher level of fine, up to €20 million or 4% of the college's annual turnover (whichever is greater), will be considered for infringements listed in Article 83(5) of the General Data Protection Regulation.

This includes infringements relating to:

The basic principle for processing, including conditions for consent, lawfulness of processing and processing of special categories of personal data
Rights of the data subject
Transfer of personal data to a recipient in a third country or an international organisation

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 Brasenose 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 Brasenose information and information processing assets shall include passphrases for systems access.

Passphrases and passphrase management systems shall follow good practice for security and use the following techniques:

- All system-level passphrases (e.g., root, enable, admin, application administration accounts, etc.) should be changed regularly. These passphrases should be changed on at least a yearly basis.
- The use of strong authentication (minimum 14-character length, non-reusable passphrases) will be used when accessing Brasenose Information.
- Users to have the ability to change their passphrases at any time
- Passphrases protecting Brasenose information or systems 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 any ICT system that stores, accesses or processes Brasenose Information is responsible for the security of their own passphrase. If a passphrase of an account is suspected to have been compromised, the user must report the relevant incident to the College ICT team immediately and change all passphrases on all systems that uses the compromised passphrase.
- 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 secure remote access service maintained by the college ICT Office

7.1.3. College ICT staff 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 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. 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 be encrypted with password security applied to reduce risk of accidental distribution.

7.1.10 All suppliers or contractors that access, store or process Brasenose College information must agree to the College's Supplier Information Security Policy. Where the data accessed, stored or processed by the supplier

or contractor is either special category data (as per defined by GDPR) or of a sensitive nature that increases potential risk to the College if exposed, a Third Party Security Assessment (TPSA) must be completed by the supplier. Third Party Supplier Assessment are managed by the College's ICT team.

7.1.11 The use of approved third party cloud services for the storage, processing or handling of College data must follow the College's Cloud/3rd Party Services - Code of Practice policy laid out in Appendix 2 of this document.

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 that 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. The DPO or ICT Manager reserve the right to revoke access to Brasenose systems or information on personal devices where data contained/transmitted is deemed sensitive and 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 / passphrase 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 either key lock/password/biometrics and, where appropriate or feasible, device encryption is used. Users should understand and be able to perform the 'remote wipe' feature available in the Office 365 portal 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 to alternative physical sites. Backups should be encrypted wherever technically possible.

7.3.3 Servers must be registered with the Brasenose College ICT Staff. If the server is not being 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

- Details and information owner of any personal and special category data stored or processed on the server.

7.4 Network Security

Responsibility for management and security of the College's internal network rests with the ICT team. The ICT 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 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 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 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. 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 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.
7.6.5. 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.

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 unauthorised 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.it.ox.ac.uk/policies-and-guidelines/computer-disposal

The University policy stresses the importance of the need for all data and software on the hard disks of computers that are ready for disposal to be destroyed.

Equipment defined as hazardous waste must have its disposal handled appropriately through the ICT 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 Waste Electrical and Electronic Equipment Directive (WEEE Directive 2012) on the disposal of hazardous electrical 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

The GDPR introduces a duty on the College to report certain types of personal data breach to the Information Commissioner's Office (ICO). This must be done within 72 hours of becoming aware of the breach.

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
https://www.infosec.ox.ac.uk/services/management

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 One - 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 'special category' data. Every care is taken to protect personal data and to avoid data 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.

The GDPR introduces a duty on the College to report certain types of personal data breach to the Information Commissioner's Office (ICO). The GDPR introduces a duty on the College to report certain types of personal data breach to the Information Commissioner's Office (ICO). This must be done within 72 hours of becoming aware of the breach.

Scope

This policy applies to all personal and special category 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

Reporting a Breach (or Suspected Breach)

Anyone who discovers/receives a report of a breach (or suspected breach) must inform their line manager and the ICT Manager/ICT Infrastructure Officer immediately. The GDPR introduces a duty on the College to report certain types of personal data breach to the Information Commissioner's Office (ICO) within 72 hours of becoming aware of the breach.

Immediate Containment/Recovery

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 passphrases, 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.

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, the College must inform those individuals without undue delay

The College must also keep a record of any personal data breaches, regardless of whether the college was required to notify data subjects. 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.

The DPO's Considerations on Wider 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.

The GDPR introduces a duty on all organisations to report certain types of breaches to the Information Commissioner's Office (ICO). Every incident should be considered on a case by case basis. The following ICO guidance will help the DPO decide whether and how to notify:

> When a personal data breach has occurred, you need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it is likely that there will be a risk then you must notify the ICO; if it is unlikely then you do not have to report it. However, if you decide you do not need to report the breach, you need to be able to justify this decision, so you should document it.
>
> In assessing risk to rights and freedoms, it is important to focus on the potential negative consequences for individuals. Recital 85 of the GDPR explains that:
>
> "A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."
>
> This means that a breach can have a range of adverse effects on individuals, which include emotional distress, and physical and material damage. Some personal data breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. Other breaches can significantly affect individuals whose personal data has been compromised. You need to assess this case by case, looking at all relevant factors.
>
> If it is decided to report the incident to the ICO, the following link has details on how to do so: https://ico.org.uk/for-organisations/report-a-breach/

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 committee 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	data.protection@bnc.ox.ac.uk
ICT Department	01865 277513 computer.office@bnc.ox.ac.uk
ICT Manager	01865 615902 john.kinsey@bnc.ox.ac.uk

Annex Two – Cloud / Third Party Services - Code of Practice

1. Purpose

This document states the College Cloud/Third Party Services - Code of Practices. It includes the roles and responsibilities of users, approved Cloud/Third Party Services and the principles of Cloud/Third Party Service Provider agreements.

2. Scope

The policy applies to all staff and students of the College and all other computer, network or information users authorised by the College.

It relates to their use of any Cloud/Third Party Services for processing, storing or transmitting the College's data.

3. Responsibilities

All: Individuals who make use of the College's systems and data are responsible and liable for the data that they handle. Any member of the College who is considering or is already using Cloud/Third Party Services for College information assets needs to be aware of and abide by this code of practice. Responsibility for ensuring appropriate use of Cloud/Third Party Services in accordance with relevant legislation and College policies lies with the individual member of the College managing, procuring or using any Cloud/Third Party Service to store, process or handle College data.

ICT Manager: This role is responsible for ensuring that this policy is enacted and for undertaking assessment of any Cloud/Third Party Assurance.

DPO: This role is responsible for overall development of this policy, and monitoring of its effectiveness.

4. Policy:

Cloud/Third Party Services

Cloud service can be defined as any solution that processes, stores or transmits College information assets via an online facility not based inside the Oxford University network.

College Approved Cloud/Third Party Service Usage

4.1. Where there is use of Cloud/Third Party Services for College data, there must be a legal agreement in place between the College/Oxford University and the Cloud/Third Party Services.

4.2. In some cases, it is recognised that a number of contractual agreements may be required to provide a service. Some of these will be College-signed; others may require end users to hold the contractual agreement. An example of this is the use of a College

provided Apple iPhone, where use is predicated on the user signing up to the iCloud service.

4.3. Users may find College-approved services list in this document. Requests for additions to the approved list should be submitted to the ICT Manager. Additional requests will only be considered if the service requested is offering functionality not offered by existing approved providers.

4.4. Sharing credentials of any Cloud/Third Party Service between the College managed devices and personal devices (unmanaged by the College) is not allowed unless:

4.4.1. All devices involved in this synchronising process are at a level of security equal to College-managed devices (See Information Security Policy)

4.4.2. Multi/Two Factor Authentication is enabled

4.5. Only the following Cloud services are approved for storing, processing or handling College data:

Microsoft OneDrive & Office 365
Google – Google Docs, Apps, Google Drive
Uniware Solutions Cloud EPOS
Apple – iCloud & iDisk

Legislation and Data

4.5. Any individual considering the use of Cloud/Third Party Services must ensure compliance with applicable College policies, information security and data classification policies, regulations and government legislation, and recognised best industry practices.

4.6. Users can use College-approved and supplied Cloud/Third Party Services to process, store or transmit College data. Cloud/Third Party Services should not be used to process, store or transmit "special category" data (See GDPR regulations) unless the service contract guarantees the use of strong encryption technologies for data in transit, at rest, backups and contains other necessary security controls.

4.7. Use of the Cloud/Third Party Services and the data processed, transmitted or stored is subject to the same policies, regulations and government legislation that applicable to other data of the College. Anyone who is using Cloud/Third Party Services must ensure that all use is consistent with associated policies, regulations and government legislation.

4.8. All data generated by College users in carrying out their duties belong to the College. As such, any use of personal Cloud storage that may require persons to transfer ownership of College data (which College members are not authorised to do) is strictly forbidden.

4.9. Whilst all principles of the General Data Protection Regulations are relevant, in relation to Cloud storage, particular attention should be paid to Principle 8, which refers to sending personal data outside the European Economic Area.

https://ico.org.uk/for-organisations/guide-to-data-protection/principle-8-international/

https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/transfer-of-data/

Service Providers, Contractual Agreements and Risk

All data generated by College staff or associated members as part of their duties belongs to the College and should be managed in line with College guidance. Using a Cloud/Third Party Service may create a risk of contravening College policy or the relevant legislation as there may be few guarantees provided by Cloud storage services.

4.10. For all Cloud/Third Party Service Providers, the use of services should be considered in terms of security and risk, data management, data access, storage, deletion and retention, auditing, reliability, availability, viability of the Cloud/Third Party Service Provider, and exit conditions.

4.11. Legal agreements with Cloud/Third Party Service Providers must be approved by the College Bursar.

5. Compliance

Compliance with this policy will be checked on the following schedule.

5.1 Annual Cloud/Third Party contract review audits will be scheduled, checked and maintained.

5.2 Annual review of policy will be scheduled and reported.

5.3 Spot checks of policy compliance will be undertaken (minimum 1 per year), including review of reports and actions.

Supplier Information Security Policy

Important Note

This Policy has been produced based on current General Data Protection Regulations (GDPR) information and the Data Protection Bill (DPB). As further updates are released this Policy will be amended to reflect the changes.

Version 1.1

Version History			
Version	**Date**	**Detail**	**Author**
1.0	27/03/2018	Initial Draft	John Kinsey
1.1	28/03/2018	PP Edits Added	John Kinsey

1. Introduction

Brasenose College provides essential services and business functions which rely on IT solutions and applications contracted by third party suppliers, which may be primary or sub-contractors. The College relies on the integrity and accuracy of its information in order to carry out its business and obligations to our customers. To enable this it is essential that information is secured in line with professional best practice as well as statutory, regulatory and contractual requirements that maintain the confidentiality, integrity and availability of all information assets.

2. Purpose

The purpose of this policy is to put in place procedures so that contracts and dealings between the College and third party suppliers have acceptable levels of data protection and information security in place to protect personal data. The new General Data Protection Regulations (GDPR) places clear statutory obligations on data controllers and processors who are involved in the processing of personal data. The following are extracts from the Data Protection Bill (DPB).

54. General obligations of the controller

(1) Each controller must implement appropriate technical and organisational measures to ensure, and to be able to demonstrate, that the processing of personal data complies with the requirements of this Part.

(2) Where proportionate in relation to the processing, the measures implemented to comply with the duty under subsection (1) must include appropriate data protection policies.

(3) The technical and organisational measures implemented under subsection (1) must be reviewed and updated where necessary.

57 Processors

(1) This section applies to the use by a controller of a processor to carry out processing of personal data on behalf of the controller.
(2) The controller may use only a processor who provides guarantees to implement appropriate technical and organisational measures that are sufficient to secure that the processing will:

(a) meet the requirements of this policy, and
(b) ensure the protection of the rights of the data subject

(3) The processor used by the controller may not engage another processor ("a sub-processor") without the prior written authorisation of the controller, which may be specific or general.

In the majority of instances, the relationships between the College and its third party suppliers are ultimately governed by the contract or information sharing agreement, which is entered into between the College and the third party supplier.

3. Scope

The scope of this policy applies to contracts, service arrangements and partnership agreements that involve IT solutions or provision of services that require access to, or the processing of, personal data for the delivery and/or support of College services and business functions. The term '**processing of personal data"** within this policy refers to either: -

a) the storing, handling, processing or retention of data including personal data related to the College's information e.g. student or employee client records. Examples include, but not limited to, IT solutions for Payroll, Student Records, Educational Monitoring etc., or

b) the storing, handling, processing or retention of data - including personal data related to/associated with the services commissioned by the College. Examples of which include mailing house contracts.

4. Policy Statement

The College has procurement processes that are designed to ensure solutions and services procured are cost effective, maintain the confidentiality, availability and integrity of information and are fit for purpose. It is therefore important that throughout the procurement and subsequent contractual period the College and its providers are clear on the College's expectations in terms of data protection, information security and supplier responsibilities.

5. Third Parties – Data Protection and Information Security Obligations

The security of information is fundamental to the College's compliance with current data protection legislation and a key focus in risk assessment, procurement and management strategy.

The College uses a risk based and proportionate approach to assess how information assets should be protected. Having procurement processes which align with identified information asset risks helps to ensure that solutions are procured, which are able to provide the level and quality of information security required by the College and current data protection legislation.

To assess the level of risk, all of the College's third party partners involved in the collection, processing or storage of personal data are required to complete a Third Party Security Assessment (TPSA).

The College requires a TPSA to be completed prior to committing to any contract.

5.1 Minimum Requirements

Where the storing, handling, processing and/ or retention of personal data is incidental to the service being provided**,** suppliers will be asked to meet the minimum requirements listed at ***Appendix A***. Failure to meet these requirements may be deemed a material breach of contract, and may therefore be the basis for termination of the contract.

5.2 Contracts

All College contracts must clearly define each party's data protection and information security responsibilities toward the other by detailing the parties to the contract, effective date, functions or services being provided (e.g. defined service levels), liabilities, limitations on use of sub-contractors and other commercial/legal matters normal to any contract. Depending on the classification of the data, various additional information security controls may be incorporated within the contract in addition to those set out in either Appendix A or the College's Third Part Security Assessment (TPSA) pack dependent upon the nature of the service provision. The DPB includes details on the College's obligations in terms of contractual requirements with data processors:

The processing by the processor must be governed by a contract in writing between the controller and the processor setting out the following—

(a) the subject-matter and duration of the processing;
(b) the nature and purpose of the processing;
(c) the type of personal data and categories of data subjects involved;
(d) the obligations and rights of the controller and processor.

6. Management of Supplier Relationships

During the period of the contract or relationship term, the College will manage the arrangement with the third party supplier to ensure data protection and Information Security standards are maintained.

6.1 Sub-Contracting

The College will include appropriate contractual obligations to ensure that any sub-contractor engaged by a third party supplier is required to operate to the same data protection and Information Security standards as the primary contractor. All sub-contractors should be listed in the relevant section of TPSA and the College updated accordingly on any changes.

6.2 Supplier Access to College Information

The College will allow third party suppliers to access its information and data, where formal contracts and data sharing agreements exist in accordance with current data protection legislation, the College's ISP (Information Security Policy) and where:

- Accessing the information is an agreed part of the solution/service provided.
- The processing and viewing of information is necessary for maintenance and trouble-shooting of the solution being provided.
- Information has been provided for inclusion in the solution/service by the College.
- Information may need to be transferred to other systems or during IT solution upgrades.
- Information may need to be collected with agreement from, and on behalf of, the College.

Viewing or accessing College information is not permitted at any time by third party suppliers without the express permission of the College. College information must not be accessed under any circumstances unless formal information sharing agreements or written contractual permissions have been established between the parties which permit this to happen.

The extent of third party supplier requirements to access College information will need to be identified prior to any contractual obligations being established and entered into. The parties must also formally agree the level and type of access to College information by third party suppliers. The security requirements for each type of information will be defined within all tender and contract documentation and the security of the information must be handled in accordance with the College's Information Classification and Handling Policy.

The College is very clear that where there is a requirement for the processing of personal data of employees or customers by third parties, information must be treated in accordance with the College's data protection obligations and requirements to ensure the confidentiality, integrity and availability of all information.

6.3 Monitoring Supplier Access to the College's Network

IT solutions which are hosted on the College's network will be subject to periodic checks to ensure that any external access by third party suppliers for support and maintenance is monitored. Once required work has been undertaken by the third party, access to the account may be disabled and the password periodically changed. Each instance of support and maintenance connections required by the third party supplier will need to be formally approved by the College before being provided.

6.4 Sale of College Data by Suppliers

It is strictly prohibited for any third party to sell Brasenose College data.

7. Security Incident Management

Third party suppliers will be expected to have appropriate security incident management procedures in place, which correspond to the level of service being provided, sensitivity of the data and GDPR requirements. Third party suppliers will be required to notify the College of any significant security incidents within 24 hours of discovery.

8. Notification of a personal data breach to the Commissioner

The GDPR will introduce a duty on the College and its third party suppliers, to report certain types of data breach to the Information Commissioner's Office. A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

As a notifiable breach is required to be reported within 72 hours of an organisation becoming aware of it, any such instances must be reported to the College immediately. Failure to do so could result in significant monetary fines being levied on the College. Contracts with suppliers will usually contain indemnity by the supplier for any such fines

9. Breaches of Policy

Breaches of this policy and/or security incidents can be defined as events which could have, or have resulted in, loss or damage to College information assets, or an event which is in breach of the College's security procedures and policies. All third party suppliers contracted to provide, support or access solutions, which enable the College to carry out its business functions and deliver its services, have a responsibility to adhere to this policy and all supporting requirements as described and referenced within formal documentation and agreed contractual agreements.

All employees have a responsibility to report security incidents and breaches of this policy within 24 hours of becoming aware of the incident through the College's Data Breach Reporting Procedure

In the case of third party vendors, consultants or contractors, non-compliance could result in the immediate removal of access to IT solutions or suspension/ termination of contractual arrangements. If damage or compromise of the College's IT solutions or loss of information results from the non-compliance, the College will consider legal action against the third party. The College will take appropriate measures to remedy any breach of this policy and its associated procedures and guidelines through the relevant contractual arrangements in place or otherwise via statutory processes. In the case of an employee, infringements will be investigated under the College's disciplinary procedure and progressed as appropriate

Appendix A
Data Protection and Information Security Guidance

BACKGROUND

Individuals and organisations are integral in assisting the College to deliver a variety of essential services. To provide a number of these services, the College is required to provide access to personal data in respect of the individuals to whom services will be provided. As a responsible organisation, the College is required by law, to take reasonable steps to ensure that personal data covered by GDPR is protected against unauthorised access or loss. With this in mind, the College has produced a checklist of the basic data protection and information security standards that are required where the storing, handling, processing and/ or retention of personal data are incidental to the service being provided.

1.	**Paper Records and Confidentiality**	**In Place**
1.1	Paper records containing the College's confidential or personal data must be locked away at the end of each working day.	Yes/ No
1.2	Keys or electronic access tokens used to keep the College's information secure should only be provided to individuals who need them for their job.	Yes/ No
1.3	The College's confidential or personal data must be destroyed when no longer required.	Yes/ No
1.4	Printers and faxes used for the College's confidential or personal data should only be available to individuals who need access to undertake their role.	Yes/ No
1.5	The College's confidential or personal data should not be left on printers, faxes, photocopiers.	Yes/ No
2.	**Electronic Records and Confidentiality**	**In Place**
2.1	The College's confidential or personal data sent or accessed electronically (including spreadsheets, letters and schedules) must be protected/encrypted with a minimum of a 14-character password.	Yes/ No
2.2	The College's confidential or personal data should only be sent by fax where no other options are available.	Yes/ No
2.3	Any College access credentials (usernames or passwords) must not be transmitted via SMS, text or instant messaging services.	Yes/ No
2.4	In the event that the College's confidential or personal data is lost, stolen or accidentally given to someone who should not have it, the College must be notified within 24 hours.	Yes/ No

Brasenose College
UNIVERSITY of OXFORD

Appendix A
Data Protection and Information Security Guidance

3.	IT equipment and Confidentiality	In Place
3.1	Any laptops, USB devices, iPads etc. holding any of the College's confidential or personal data must be locked away at the end of each working day.	Yes/ No
3.2	Anti-virus software must be installed on IT equipment holding the College's confidential or personal data with the automatic update activated.	Yes/ No
3.3	Software used on laptops, PCs, and mobile devices should be constantly updated with the latest security patches.	Yes/ No
3.4	Mobile devices including phones and iPads holding the College's confidential or personal data must be secured by the use of a 'PIN'.	Yes/ No
3.5	Portable devices such as laptops, tablets or phones holding the College's confidential or personal data should be encrypted.	Yes/ No
3.6	Old laptops, USB devices, iPads, smartphones etc. used to hold the College's confidential or personal data must be disposed of securely to ensure that the data on the hard drives is destroyed.	Yes/ No
3.7	Individuals with access to the College's confidential or personal data must take all reasonable steps to ensure that the information is not accidentally or intentionally disclosed.	Yes/ No