Brasenose College Information Security Policy (ISP v1.8) & Annexes

1. Introduction

Brasenose College seeks to maintain the appropriate level of confidentiality, integrity, and availability (CIA) of all the information it owns or processes. 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 to keep information appropriately secure, accurate and available.

In support of this objective all users of data assets, whether they are manual or electronic, have roles and responsibilities in ensuring information is protected by:

- Treating information security seriously
- Maintaining an awareness of security issues
- Adhering to applicable security policies / following applicable guidance
- Reporting issues and incidents as they arise to either a line manager or the data protection team (data.protection@bnc.ox.ac.uk).

Sensitive 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 UK Data Protection Act (2018), 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 any individual.
- 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 additional information that can indirectly identify a person, e.g. photography or IP 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, relevant contractors, 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 (CIA) of all data it holds in systems. This includes the protection of any device that can carry or access

College 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 so that the College can continue to operate if employees and members are not able to access systems due to IT problems or loss of loss physical access.
- Prohibit unauthorised use of the College's information and systems.
- Communicate this and other related Information Security Policies to all persons processing or handling college data.
- Provide information security training to all persons appropriate to their role.
- Report any breaches of information security, actual or suspected to the Data Protection Officer (DPO) as soon as they occur or are observed.

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 is a process of risk assessment 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. The College has a **Data Classification & Handling Scheme** that all college members should be aware of. It can be found within the College's GDPR Framework documentation found here: https://www.bnc.ox.ac.uk/privacypolicies

5.5 Data Protection Impact Assessments (DPIAs) must be completed before any new (or planned significant change to existing) data processing activities commence that could result in a higher risk to either data subjects or college sensitive data.

5.6 Personal data must be handled in accordance with the UK Data Protection Act (2018) and in accordance with this policy.

5.7 The UK Data Protection Act (2018) 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 UK Data Protection Act (2018) 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 ensuring an appropriate and effective Information Security framework is in place. This responsibility extends to the facilitation and encouragement of healthy organisation wide cultures and values that support safe and supportive environments for the reporting of issues, concerns, and breaches.

Governing Body requires **all system owners and process owners** to be accountable for implementing an appropriate level of security control for the system & information held and processed by their systems and processes. Any reviews or amendments to systems or process should include a review of the information handling implications by appropriately qualified members of staff.

Each person is accountable to the system or process owner for operating an appropriate level of security control over the information and systems they use to perform their duties.

The **Data Protection Officer** is responsible for overseeing and reviewing the College's obligations and ensuring compliance with all relevant data protection / information security legislation, and approving all subject access requests and responses to data breaches.

The **IT Director** is responsible for ensuring the College prepares appropriate information security policies, reviewing / monitoring whether they are being followed, and as a first responder to information security incidents.

The IT Director also assists the DPO by coordinating the day-to-day management of information security, logging of incidents, maintaining this Information Security Policy as well as the college's data protection framework documents e.g. Privacy notices and ROPAs) and providing advice and guidance on its implementation and training.

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, but the College also recognises the importance of transparency and openness, and the avoidance of a "blame culture". The College therefore encourages its members to be open about concerns and such openness will reduce the likelihood of disciplinary action; conversely secrecy about mistakes or concerns will increase the likelihood of disciplinary action.

7. 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.
- Effective 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. Where systematically possible, multifactor

authentication should be enforced. It should be noted that the University SSO (Microsoft) identity has multi-factor authentication built in & should be the identity management tool of choice for accessing web-based systems where it is technically possible to do so. Future system developments should look to utilise this credential.

Passphrases shall follow good security practices and use the following techniques:

- All administrator level passphrases (e.g., root, enable, admin, application administration accounts, etc.) should be changed regularly. Root / system administrative level passphrases should be changed on at least a yearly basis.
- The use of strong authentication (minimum 16-character length, non-reusable passphrases) will be used when accessing Brasenose information.
- Users should have the ability to change their passphrases at any time.
- Permanent Passphrases protecting Brasenose information or systems must not be inserted into email messages, electronic or physical letters. One-time temporary passphrases or codes may be sent by MS Teams or to a personal University Nexus365 email account.
- Any exception to these provisions must be subject to a specific risk assessment and is only permitted where approval is given by the IT Director.
- Each user of any ICT system that stores, accesses or processes Brasenose Information is responsible for the security of their own passphrase and maintenance of any multi-factor authentication methods required to access it. 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 use that compromised passphrase.
- Access privileges to specific systems 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. Where a system owner is unsure as to the required level of access for a user, they should seek advice from the IT Director.
- All shared computer systems will require users to authenticate before use (unless authenticated network access controls are already in place) and will enable activities to be traced to an authenticated individual.
- To allow for potential investigations, network logs should be kept in the University SAVANT cloud & for a minimum of six months, or for longer, where considered appropriate.

External access to the College's administered networks and systems.

7.1.3. College ICT staff shall review all external 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 the College's

assets in their possession upon termination of their employment, contract or agreement. Department heads or other relevant roles are responsible for completing leavers' checklists and communicating those lists to appropriate sections of college.

7.1.6. Most 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". https://governance.admin.ox.ac.uk/legislation/it-regulations-1-of-2002. Where any additional monitoring falls outside the defined scope of the University regulations, the IT Director and Bursar must agree scope and duration of the additional monitoring.

7.1.7. Domain administrator privileges – those that can override system and application controls on multiple devices and services college wide – shall be restricted to those persons who are authorised and qualified to perform multi-system administration only. Such privileges shall be authorised by the IT Director 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 electronic documents that contain personal or sensitive information should be internally distributed via a permission-based share-link as opposed to actual copies of the file disseminated (e.g. attached to emails). If whole file copies must be attached or electronically disseminated, then methods that ensure the information is encrypted during transit & 'at rest' must be used. It should be noted the University Nexus365 email system encrypts emails in transit and at rest and so for internal (OU Wide) distribution of sensitive material there is no need of further encryption (e.g., Passwords on files). University Microsoft Teams and SharePoint also satisfy the encryption requirement.

7.1.10 All suppliers or contractors that access or process Brasenose College information must either demonstrate suitable information security standards (as defined in points A, B, C & D below) or agree to the College's Supplier Information Security Policy (Supplier ISP - Appendix three). If processing special category or particularly sensitive data, the supplier will be required to undertake a Third-Party Security Assessment (TPSA) by the college IT team unless sufficient security standards (as defined in points A, B, C & D below) are satisfied. If all the requirements below are met by the supplier, there is no requirement for the Supplier ISP or a TPSA:

- A. Actively certified to information security standard IS027001.
- B. If a Cloud service provider, additionally certified to cloud information security standard ISO27017.
- C. Data is processed, accessed, and backed up solely inside the UK or within the European Economic Area (EEA).
- D. The Data Protection Officer is satisfied that any stipulated maximum financial liabilities with regards data protection in the supplier engagement contract is within the college's risk tolerance.

  Any required Third-Party Supplier Assessments (TPSA) are managed by the College 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. If a service is not on the

approved Cloud / third party list (Appendix 2), then members of college must not use that provider to process college information.

7.1.12 No third-party supplier or service provider should be engaged to process college information without permission of the DPO.

7.2. Use of Personal Computer Equipment and Removable Storage

7.2.1. The college must ensure all devices provided for the purposes of processing or storing college data 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 college members need to use their own computing equipment to access information (including personal data and emails). Users should ensure such devices are, with support of the college ICT department:

- Protected with a suitable strong passphrase (minimum 16 character) or biometric feature.
- Running an in-support operating system that is patched to the latest version.
- Protected (where possible) with active and up to date anti-virus.
- Encrypted.
- Utilise either University or Brasenose VPN services to enable encryption of traffic over unsecured networks.
- The DPO or ICT Director reserve the right to revoke access to 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 required that:

- If the DPO allows College information containing personal data to be saved onto non-encrypted removable storage, it shall be encrypted before being transferred to the storage device. 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, their operating systems are in-support and up to date, and where appropriate or feasible device encryption is used.
- Users should understand that if they setup their university email address on personal devices, there is a remote wipe feature that can be activated by college IT staff that could potentially wipe the personal device completely if the account is suspected of being compromised. Users put their university email accounts on their personal devices at their own risk.
- 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 applies to server & network equipment owned and/or operated by Brasenose College. No server grade or capable services should be run on the College's internal networks without authorisation and administrative access being given to the College IT team.

7.3.1 All servers must be physically located in an access and environment-controlled rooms.

7.3.2 Servers should be backed up incrementally to at least one alternative physical site. Backups should be encrypted. In addition to standard incremental backups, all college servers must have an offline cold backup no older than 10 days.

7.3.3 The university information security baseline assessment lists all the technical controls that should be applied (where appropriate) across the whole college IT estate. These controls, listed in Annex 4, will apply (where appropriate) to all servers and services administered by college.

7.4 Network Security

Responsibility for management and security of the College's internal network rests with the Infrastructure Manager and IT Director. These responsibilities extend to:

- Ensuring all ICT Staff [network administrators] are suitably trained in modern network architecture, security methods and the ICT staff policy and procedures manual is kept up to date.
- Network Logs are kept in accordance with the University OxCert technical policies.
- Protect the network and the information transmitted across it. The university information security baseline assessment lists all the technical controls that should be applied (where appropriate) across the whole college IT estate. These controls, listed in Annex 4, will apply (where appropriate) to the networks operated by college and services run across them.
- Restrict unauthorised traffic using firewalls or equivalent devices.
- 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 & exported to the University cloud SAVANT service. It is currently recommended that at least 60 days of logs be kept, and longer if possible. Logs must include identifiable data to enable traces back to specific events, computer systems, and specific users. Timestamps, MAC addresses, IP Addresses, and where possible usernames should be included in logging systems.

7.5. Email and Internet Use

Policy for the use of electronic mail is covered by the University's ICTC regulations of 2002 (with subsequent amendments) and available at https://governance.admin.ox.ac.uk/legislation/it-regulations-1-of-2002

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. Mass mailing functionality provided by the College is for work-related information only. This therefore excludes the use of the email system for personal business.

7.6. Software Compliance

7.6.1. College will provide appropriately licensed and authentic installations of software or cloud service access 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 device (including mobile equipment). The ICT Director (or Infrastructure Manager in absence) 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 external contacts, including alumni/students, without express permission of the IT Director.

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

7.6.5 Any further software usage policies should be included in the Staff Handbook.

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. 'Home offices' must also satisfy this criteria. 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 communal 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. In the case of virtual meetings, organisers must ensure 'meeting chats' are deleted appropriately.

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 https://help.it.ox.ac.uk/equipment-disposal-stone
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 Director.

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”.

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. Batteries will be disposed of in line with The Waste Electrical and Electronic Equipment Directive (WEEE Directive 2012 & Waste Directives 2023) on the disposal of hazardous electrical waste.

8.1.5. Hard Disks must be secure wiped using a tool such as PGP or DBAN, or physically destroyed.

9.0 Data Breach/Loss

The College has a duty to report certain types of personal data breach to the Information Commissioner's Office (ICO). Where required to do so, 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 suspected data breach incidents. Reportable incidents 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.
- Use of cc instead of bcc on email use.
- Loss of password / decryption key for encrypted files.

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 University InfoSec Toolkit https://www.it.ox.ac.uk/information-security

10.0 Governance

This Policy will be reviewed regularly by the Bursar and IT Director. Any changes will be approved by the Governing Body.

11.0 Enforcement

11.1 Breaches of this 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. However, any individual reporting their own breach of the policy (data.protection@bnc.ox.ac.uk) would substantially reduce any actions in this regard.

12.0 Payment of 'Ransoms'

Brasenose College is committed to safeguarding the confidentiality, integrity, and availability of our information assets. As part of our comprehensive approach to information security, the College establishes the following default position with respect to ransomware attacks:
We do not pay ransoms.
Paying ransoms in response to ransomware attacks not only poses significant financial risks but also contributes to the perpetuation of criminal activities. The College acknowledges that paying ransoms does not guarantee the retrieval or confidentiality of data, does not address the root causes of the attack, and may encourage further attacks. Therefore, the default stance is to resist ransom payments.

13.0 Official College Social Media Accounts

There is nothing to stop individuals, internal or external, creating social media and using the college name or crest. It is imperative that official college social media accounts:

13.1 Are registered with college IT team and added to the list of official account on the college website. https://www.bnc.ox.ac.uk/socialmedia

13.2 Protected by Multi-Factor authentication.

13.3 Where applicable, additional recovery email addresses on accounts should be generic college addresses.

13.4 A named college member is assigned to the account and responsible for its handover on leaving.

Annex One

BRASENOSE DATA PROTECTION BREACH POLICY

This policy is part of the Information Security Policy.

Policy Statement

Brasenose College processes personal, special category, and confidential data. Every care is taken to protect the confidentiality, integrity and availability of this data as well as ensuring it is only processed for the purposes communicated to data subjects in the relevant College privacy notice(s) & records of processing activities (ROPAs). However, whether accidental or by the actions of a malicious actor, loss of confidentiality, integrity or availability of data can occur. It is imperative that when such situations arise or are suspected that they are reported and investigated as soon as possible. The college acknowledges that reporting a data breach, especially if accidental, can be distressing to individuals concerned – as such, the college tries to operate a 'blame free' and open culture to the reporting of data breaches.

Purpose

This policy sets out the procedure to be followed by all college members if a data protection breach is suspected.

The Data Protection Act 2018 introduces a duty on the College to report certain types of personal data breach to the Information Commissioner's Office (ICO) within 72 hours - all actions must be taken promptly.

Scope

This policy applies to all college members that process personal, special category, and confidential data owned by Brasenose College.

Types of Reportable Breach

Data protection breaches refer to any occasion where either the confidentiality, integrity or availability of college data is, or was nearly, compromised. If in doubt, report it. Some examples are:

- Loss or theft of data or equipment on which data is stored.
- Inappropriate access controls reducing the confidentiality of data.
- Equipment failure resulting in the loss, destruction, integrity, or availability of data.
- Human Error. For example, use of cc instead of bcc in email usage.
- Unforeseen circumstances such as fire or flood
- Hacking or other malicious online activities.
- Loss of password / decryption key for encrypted files.
- Incidents where information (or access to information) is obtained by deception or blackmail.
- Incidents where only a 'last minute' nonprocedural check prevented a breach.

Reporting a Breach (or Suspected Breach)

Anyone who discovers, receives a report of or thinks they may have enabled a data breach (or suspected breach) must inform the data protection team immediately. Relevant contact details are at the end of this policy. The Data Protection Act 2018 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 and so reporting quickly is essential.

Immediate Containment/Recovery

The data protection team and system/process owner 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 immediately.

The Data Protection Officer (or IT Director in their absence) must also consider whether the University emergency response team (OxCert) or 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. If the Police are to be informed, evidence must be preserved which may delay recovery. If OxCert are informed, they will give advice on how to proceed.

The Data Protection Office must ensure that the appropriate steps are taken quickly to recover any losses and limit the damage. Steps might include:

Attempting to recover lost equipment.

Contacting any affected individuals or departments so that they are prepared for any potentially inappropriate enquiries 'phishing' for further information on the individual(s) concerned. Consideration should be given to a global email.

Contacting the relevant teams so that they can be prepared to handle any press or other enquiries that may result.

The use of back-ups to restore lost/damaged/stolen data.

If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use.

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(s) 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 Director and the relevant line manager, system or process owner.

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 regulatory bodies may need to be notified as part of the initial incident.

The Data Protection Officer should, after seeking advice, decide whether any such regulatory bodies should be notified of the breach. The DPO maybe required to liaise with the College Accountant about potentially informing the insurers in some cases.

The UK Data Protection Act (2018) 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.
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, 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. The DPO needs 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 investigation 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.
If systemic or ongoing problems are identified, then an action plan must be drawn up to put this 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 DPO.

Useful Contacts

Data Protection Team	data.protection@bnc.ox.ac.uk
ICT Department	01865 277513 computer.office@bnc.ox.ac.uk
ICT Director	01865 615902 ict.manager@bnc.ox.ac.uk
Oxford University OxCert	01865 282222 oxcert@infosec.ox.ac.uk

Annex Two

Cloud / Third Party Services - Code of Practice

Purpose

This document states the College Cloud/Third Party Service - Code of Practices. It includes:

a. The roles and responsibilities of college users of such services
b. List of approved Cloud/Third Party Services
c. Requirements and principles of Cloud/Third Party Service Provider agreements.

Scope

The policy applies to any Cloud or third-party service provider that any college member intends to processes, access or store Brasenose College data.

Responsibilities

Everyone: Individuals who process or store College's 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 need 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 Director: 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.

Policy:

Cloud/Third Party Service Definitions

Cloud services are defined applications, services or infrastructure resources that are accessible via the Internet but are not hosted inside the college or wider Oxford University network.

Third Party Services are defined as either:

a. Applications, services, or infrastructure deployed inside the college or wider Oxford University network but are not under the direct control of the college or alternative Oxford University unit (e.g. Some Telethon service providers).
   OR
b. Any unaffiliated person, company, or entity that performs services involving the processing of Brasenose College data offsite.

College Approved Cloud/Third Party Service Usage

4.1. Where there is use of Cloud/Third Party Services processing College data, there must be a legal agreement in place between the College/Oxford University and the Cloud/Third Party Services. If not already on the approved Cloud/Third Party Service list, any such legal agreements must be

assessed by the data protection team and signed off by the DPO before the service(s) can be used. This includes any trial periods of a service.

4.2. In some cases, it is recognised that several 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 data protection team (data.protection@bnc.ox.ac.uk). 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 must have at least the minimum level of security as stipulated in the Information Security Policy)

4.4.2. Multi/Two Factor Authentication is enabled wherever technically possible.

4.5. Only the following Cloud services are currently approved for storing, processing, or handling College data (University hosted services are exempt):

Provider	**Related Services Covered**	**Approval / Last Assessment Date**
Apple	iCloud & iDisk	August 2021
Atlassian	Confluence Cloud IT Wiki	January 2022
Blackbaud	Raiser's Edge NXT, NetCommunity	September 2021
Cintra	Payroll and HR Cloud	October 2021
Heimdall	Cloud patch and control management	October 2023
Metadatis	Cloud Archiving Solutions	May 2023

Nexus Microsoft O365 Platform	OneDrive, SharePoint, MS Teams, Nexus365 Email, MS Bookings + Other 365 Apps	June 2023
Oracle	Oracle NetSuite (Member Database)	July 2023
Ruckus	CloudPath Wireless Management	June 2021
Snipe IT	Asset Management	July 2023
Uniware / Upay Services	Uniware Cloud EPOS, Upay.co.uk, Order Ahead	June 2022
Xibo	Xibo Display Cloud	June 2022

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 utilise 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 UK Data Protection 2018 regulations) unless the service contract guarantees security controls equivalent to ISO 27017.

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, ROPAs 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 forbidden without the express authorisation of the data protection officer (DPO).

4.9. Only cloud / third party services that process and backup data within UK or EEA based datacentres should be considered for processing of Brasenose College information.

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.

Compliance

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

5.1 Cloud/Third Party contract review audits will be scheduled, checked and Maintained every two years.

5.2 Review of this policy will be scheduled and reported every two years.

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

Annex Three

Brasenose College Supplier Information Security Policy

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-contracted. The College relies on the confidentiality, integrity and availability of its systems and data 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 stipulate the minimum-security requirements expected by Brasenose College of third-party suppliers to have acceptable levels of data protection and information security in place to protect personal data. The UK 2018 Data Protection Act (DPA) places clear statutory obligations on data controllers and processors who are involved in the processing of personal data.

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 Brasenose College of a processor to carry out processing of personal data on behalf of the College.

(2) The College 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) Processors engaged by the College may not engage another processor ("a sub-processor") without the prior written authorisation of the College, which may be specific or general.

The relationships between the College and its third-party supplier will ultimately be 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 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 the College's third-party partners involved in the collection, processing or storage of special category data are required to complete a Third-Party Security Assessment (TPSA) unless they satisfy all three criteria below:

- 1. Active certification to information security standard IS027001.
- 2. If a Cloud service provider, additionally certified to cloud information security standard ISO27017.
- 3. Data is processed, accessed, and backed up solely inside the UK or within the European Economic Area (EEA).

Where required, the College would require a completed TPSA 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

Any authorised sub-contractors engaged by a third-party supplier are required to operate to the same data protection and Information Security standards as the primary contractor. All sub-contractors should be listed by the processor and reviewed by the College before a contract is signed.

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. 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 UK Data Protection Act 2018 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 UK Data Protection Act 2018 requires 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.

9.0 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.

10.0 Minimum Controls

As a responsible organisation, the College is required by law, to take reasonable steps to ensure that personal data covered by 2018 UK Data Protection Act is protected against unauthorised access or loss. 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 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 in transit and at rest.	Yes/ No
2.2	Any College access credentials (usernames or passwords) must not be transmitted via SMS, hardcopy, email, or unencrypted instant messaging services.	Yes/ No
2.3	If 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
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 in support and 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 have screens secured using a 'PIN', biometric or password.	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

Annex Four

University Baseline Security Controls

These are the core technical controls that must be applied throughout the entire IT estate where it is technically possible to do so. Where it is not possible to apply a specific control, appropriate mitigations should be in place.

As of 2023 (v4) there are 109 technical controls in the areas of:

- Access Controls: Accounts & Privileges
- Access Controls: Authentication
- Access Controls: Network
- Incident Management
- Monitoring & Logging
- Network Management
- Operations
- System Acquisition & Maintenance
- Vulnerability Management

A detailed list of each control can be found here: