Name of Policy: Information Security

RESPONSIBLE COMMITTEE: Academic Services

RESPONSIBLE OFFICER: Data Protection Officer

LINKED DOCUMENTS: College: IT Policy; College Regulations Relating to the Use of Information Technology Facilities; Data Sharing on *Prevent* Policy; Physical Security Policy; *Prevent* Team Reporting Procedure.

LINKED DOCUMENTS: Other: n/a

Annual Review date: First meeting of Hilary term

POLICY HISTORY

Date of GB approval	***Brief summary of changes***	***Confirmation that linked documents have updated if necessary***	***College policy register updated***
March 2014	Original document	na	na
June 2016	Approval including revision for *Prevent* documentation	na	Yes (Sandra Campbell)
March 2017	Committee Review	na	Yes (Sandra Campbell)
March 2018	Web links updated. Policy reviewed by Committee and subsequently approved by GB	na	Yes (Sandra Campbell)
May 2018	Updated for GDPR and reviewed by GB	Yes	Yes (Sandra Campbell)

Information Security Policy

The following policy has been approved by the Governing Body of St John's College for College information assets. Any amendment to the policy requires The Governing Body's approval. All Fellows, staff, students, visitors and others handling information assets related to St John's College are required to comply with this policy. Support and guidance for compliance with this policy is provided by St John's College's IT Officers. This Information Security policy and accompanying procedures formalise and regularise existing good practice within the College and wider University.

The Governing Body intends to review this policy annually to ensure any new developments are covered and protected.

Overview

Users of ICT within the University are subject in the first instance to the University ICTC regulations (2002) with subsequent amendments and available for review at: http://www.admin.ox.ac.uk/statutes/regulations/196-052.shtml

The ICTC regulations alone do not fully provide for all the needs of a security policy covering ICT services within St John's College. This security policy provides additional policies and guidelines which apply to its services and users of information assets within St John's College. Effective security is a team effort involving the participation and support of every College Fellow, staff, student, visitor and others handling information assets related to St John's College. It is the responsibility of every individual handling information assets to know these policies and guidelines, and to conduct their activities accordingly.

To avoid ambiguities, particular terminology is used when explaining the policies:

- **MUST** This word, or the terms **"REQUIRED"** or **"SHALL"**, mean that the item is an absolute requirement.
- **MUST NOT** This phrase, or the phrase **"SHALL NOT"**, mean that the item is absolutely prohibited.
- **SHOULD** This word, or the adjective **"RECOMMENDED"**, mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.**SHOULD NOT** This phrase, or the phrase **"NOT RECOMMENDED"** mean that there may exist valid reasons in particular circumstances when the particular behaviour is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.

1. Introduction

St John's 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 St John's 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 St John's College and demonstrates management direction and support for information security across St John's College. This policy is meant to keep information secure and highlights the risks of unauthorized access or loss of data.

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

(a) Treating information security seriously

(b) Maintaining an awareness of security issues

(c) Adhering to applicable security policies / following applicable guidance

Information relating to living individuals (such as may be found in Personnel, Payrolls, and Student Record Systems) should only be stored in the appropriate secure systems and is subject to legal protection. All users of the ICT system are obliged, under the terms of the General Data Protection Regulation (GDPR), 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 St John's College's information and its operational activities including but not limited to:

(a) Records relating to applicants, students and staff, alumni, visitors, conference guests and external contractors where applicable
(b) Operational plans, accounting records, and minutes
(c) All processing facilities used in support of St John's College's operational activities to store, process and transmit information
(d) 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 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 supported staff as applicable.

4. Policy

St John's College aims, as far as reasonably practicable, to:

(a) Protect the confidentiality, integrity and availability of all data it holds in its systems. This includes the protection of any device that can carry data or access data, as well as protecting physical paper copy of data wherever possible,
(b) Meet legislative and contractual obligations,
(c) Protect St John's College's intellectual property rights and commercial interests,
(d) Produce, maintain and test business continuity plans in regards to data backup and recovery,
(e) Prohibit unauthorised use of St John's College's information and systems,
(f) Communicate this Information Security Policy to all persons potentially accessing data,
(g) Provide information security training to all persons appropriate to their role,
(h) Report any breaches of information security, actual or suspected in accordance with Appendix 1.

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 appropriate degree of control therefore is determined by 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 St John's College's information assets; identify the responsible Officer for those assets; and classify the information assets, according to their sensitivity and/or criticality to St John's College or the University as a whole. In assessing risk, St John's 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 implemented. Users of College resources must be aware of the University's Regulations and Policies applying to all users of University ICT facilities. Further information is 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 St John's College's infrastructure, systems and processes.

5.6 Personal data must be handled in accordance with the General Data Protection Regulation (GDPR) and in accordance with this policy and the College's Data Protection 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. A higher level of security should be provided for 'sensitive personal data'.

6. Responsibilities

The Governing Body is responsible for establishing the framework and for issuing and reviewing policy statements and procedures to support St John's College and the University's Ordinances and Regulations with which members of the University must comply.

Governing Body requires the College Officers in St John's College to be accountable for implementing an appropriate level of security control for the information under their responsibility and processed by persons accessing that data on behalf of College.

Each member of staff is accountable to their head of department for operating an appropriate level of security control over the information and systems they use to perform their duties. Fellows and Tutors and Lecturers are responsible to the Senior Tutor, Junior Members are responsible to the Senior Dean, academic visitors are responsible to their host and Conference and other visitors are responsible to the Domestic Bursar.

The Data Protection Officer is responsible for co-ordinating the management of information security, maintaining this Information Security Policy and ensuring availability of 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 GDPR. This includes infringements relating to:

- Integrating data protection 'by design and by default'
- Records of processing activities
- Co-operation 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 GDPR.

The includes infringements relating to:

- The basis 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. Detailed Policies and Guidance

The following shall be complied with throughout St John's College.

7.1. Access to Information and Information systems

7.1.1. Information assets shall be under the responsibility of a named officer within St John's College. A list of information assets and the responsible officer shall be maintained by the DPO.

7.1.2. Access to information shall be restricted to authorised users and shall be protected by appropriate practical physical and/or logical controls.

(a) Physical controls for information and information processing assets shall include:

(i) Locked storage facilities (supported by effective management of keys)

(ii) 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.

(iii) Securing of mobile computers and other devices to prevent theft, where other physical controls such as locked doors or available secure storage cabinets are not available.

(iv) "Clean desk" policies (refer to section 7.8 of this policy)

(v) Encryption of sensitive data either transmitted or taken outside St John's College's properties. Encryption of data should be appropriate to the level of risk assessment of the data.

(b) Logical controls for information and information processing assets shall include passwords for systems access.

(c) Passwords and password management systems shall follow good practice for security which may include the following techniques:

(i) All system-level passwords (e.g., root, enable, admin, application administration accounts, etc.) should be changed periodically, and an expiry policy should be configured to enforce this where possible,

(ii) The use of strong authentication (minimum length, high complexity, non-reusable passwords). Refer to **Appendix 3** for Password Construction Guidelines,

(iii) Users where possible to have the ability to change their own passwords at any time,

(iv) Passwords to be changed at regular intervals appropriate to the information and resources being secured. A password expiry or account lock-out system to be in place to automate and enforce this process,

(v) Passwords should not be inserted into email messages or other forms of electronic communication except if it is necessary to issue a 'single use' password electronically,

(vi) Any exception to these provisions must be subject to a specific risk assessment and is only permitted where approval is given by the DPO,

(vii) Specific exemption from a requirement for individual passwords applies to hardware where there is no capacity for individual passwords, such as BIOS protection, and to externally required single institutional passwords, such as from HMRC where College has a legal obligation to report data. All such group passwords must be restricted to only those College staff or external maintenance staff who need to use such passwords in the course of their work for College.

(d) Each user of the ICT system is responsible for the security of their own password. If a password of an account is suspected to have been compromised, the user must report the relevant incident to the IT team immediately and change all passwords on all system. For further standards on password protection refer to **Appendix 3**.

(e) Access privileges shall be allocated based on the minimum privileges required. Access privileges shall be authorised by the appropriate information owner or someone with authority to act on their behalf.

(f) Shared computers will require users to authenticate before use in order to enable activities to be traced to an authenticated individual. A specific exemption to this is the Main Lodge central console where working practice make signing on and off impractical and where rotas and video surveillance of the console can identify users.

(g) To allow for potential investigations & traceability, access records should be kept for a minimum of six months, or for longer, where considered appropriate.

(h) Access to the St John's College's administered network via remote access must require a login in order to get access to any system on the internal network.

7.1.3. Officers responsible for information assets shall review access permissions on an annual basis.

7.1.4. Access to physical information assets – for example printed paper documents, and media containing information – shall be governed as appropriate by the same principles as above.

7.1.5. Processes shall be in place to ensure that all employees, contractors and third party users have appropriate information and physical access permissions granted on joining the organisation, expediently revoked on leaving the organisation, and updated on changes in role. Leavers will also be required to delete or return all of St John's College's information assets in their possession upon termination of their employment, contract or agreement. College Officers or other relevant staff are responsible for completing leavers checklists and communicating those lists to appropriate sections of College.

7.1.6. The circumstances under which the College may monitor use of its ICT systems, and the levels of authorisation required for this to be done form part of the University's "Regulations Relating to the use of Information Technology Facilities".

7.1.7. Access to operating system commands and the use of system utilities - such as administrator privilege - that might be capable of overriding system and application controls, shall be appropriately restricted to those persons who are authorised to perform systems administration or management functions. Such privileges shall be authorised by the DPO once they have been reviewed and appropriate risk assessments made as to the validity of requirements and the skill levels of those requesting increased privileges.

7.1.8. Visitors to St John's College should be provided with specifically assigned credentials and should be appropriately authenticated and automatically disabled at the end of their term with St John's College.

7.2. **Use of Personal Computer Equipment and Removable Storage**

7.2.1. St John's College recognises that there may be occasions when staff need to use their own computing equipment to process information (including personal data). Point 7.1.2 addresses this where information is to be transferred outside of the college property/ICT system. Appropriate levels of control should be put in place for information which is held on a staff members' own computing equipment or on removable storage.

7.2.2. It is good practice and required that:

(a) Privately owned computing equipment used to process St John's College information or connect to St John's College's network must have up-to-date anti-virus software installed and, if the computer is to be connected to the Internet, a firewall. Anti-virus software provided by a site-license and can be used on all systems connected to the administered network and installed via the University's IT Services website. Refer to **Appendix 5** for further recommended end user practices to prevent Virus problems.

(b) The information on removable storage devices holding personal data should be protected from loss and/or theft. Information containing personal data that is to be saved onto removable storage or privately owned computing equipment shall be encrypted before storage. Appropriate encrypted storage devices or software needed for College purposes can be requested from the IT Officers.

(c) St John's College information shall not be retained on removable storage devices longer than necessary (i.e. once information that has been updated on a computer owned by a member of staff is uploaded onto St John's College systems, it shall be deleted from the removable storage device).

7.3. **Servers**

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

All internal servers deployed in St John's College must be the responsibility of an operational group that is responsible for system administration. Approved server configuration guides must be established and maintained by each operational group. Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a process for changing the configuration guides, which may include peer review and approval.

7.3.1. Physical servers must be housed in a location where physical access and the server environment (power, temperature, and humidity) can be controlled.

7.3.2. Servers should be backed up to offsite storage, such as the University HFS. (Refer to section 7.9 of this policy for further information)

7.3.3. Servers must be registered with the St John's College IT team. As a minimum, the following information is required to positively identify the point of contact:

(a) Server contact(s) and location, and a backup contact
(b) Hardware and Operating System/Version
(c) Main functions and applications, if applicable

Refer to **Appendix 6** for Server General Configuration Guidelines.

St John's College IT Staff will police their own policies in this area but will seek to follow policies that are regularly reviewed and audited by the University IT Services and the wider IT support community in the University.

7.4. Network Security

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

(a) Ensure IT Officers are suitably trained in information security.
(b) Proper logs are kept in accordance with OxCERT policies.
(c) Protect physical network from interception/damage/interference.
(d) Restrict unauthorized traffic using a firewall or equivalent device.
(e) Regularly review and maintain network security controls and device configurations.
(f) Identify security features, service levels and management requirements and include them in any network service agreements whether they be in-house or outsourced.
(g) Use secure network connections for making any transfers of non-public information.

7.4.2 All St John's College's networks must be monitored at all times. Monitoring must detect and log at least the following activities, as comprehensively as reasonably possible:

(a) Unauthorized access attempts on firewalls, systems, and network devices (only authorized systems and users should have access to the network)
(b) Port scanning
(c) System intrusion originating from a protected system behind a firewall
(d) System intrusion originating from outside the firewall
(e) Network intrusion
(f) Denial of services
(g) Any other relevant security events

7.4.3 All network activity should be logged in accordance with OxCERT policy. It is currently recommended that at least 60 days of logs be kept, and longer if possible. Logs must include identifiable data to enable traces back to specific events, computer systems, and specific users. Timestamps, MAC addresses, IP Addresses, and where possible usernames should be included in logging systems.

Further information on good IT security practice can be found on the University's Information Security site https://www.infosec.ox.ac.uk/.

7.5. Email and Internet Use

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

Where email systems are hosted locally, they should be checked by St John's College's ICT Services Department on a regular basis to ensure that they are being appropriately updated in regards to spam/virus filters. All email that passes through the email system shall be content checked and scanned for viruses and inappropriate content and cross-checked against an internet "black list" of banned email addresses. For centrally hosted email by ITSS, their information policy will take precedence.

7.5.1. St John's College policy and procedure on staff use of email and the Internet should be included in the Staff Handbooks.

7.5.2. Virus or other malware warnings should be forwarded to IT staff for checking and distribution rather than sent to other users. Mass mailing users of address groups

provided by St John's College is for work-related information only. This therefore excludes the use of the email system for advertising personal items for sale.

7.6. **Mobile Computing.**

This applies to any mobile hardware that is used to access St John's College resources, whether the device is owned by the user or by St John's College.

7.6.1. Persons with laptop computers and other mobile computing devices including mobile phones shall take all sensible and reasonable steps to protect them from damage, loss or theft. Such steps may include:

(a) Securing laptops and removable media whether in college or while travelling.

(b) Avoiding taking laptops into areas with a high risk of theft and locking such equipment in the boot of a vehicle when leaving it unattended

7.6.2. Persons using computing equipment in public places shall ensure that confidential information cannot be viewed by unauthorised persons (e.g. stations, airports, trains, etc.)

7.6.3. Use of external wireless access points shall be permitted provided that the firewall software provided with the mobile computer is activated.

7.6.4. Mobile computer and smart phone users are required to ensure that software controls and updates are installed and regularly updated to protect the mobile computers and smart phones from viruses, spyware and similar malicious programmes. Regular updates of anti-malicious software files should occur automatically on connection to the Internet.

7.6.5. Use of any mobile computing device owned by St John's College, or that is used to access St John's College data (including email) must be in accordance with this Policy and the relevant section of the Staff Handbooks.

7.6.6. Mobile Device Security

(a) Any mobile device that is used to process or store St John's College sensitive data should have any remote wipe capability of the device turned on to protect against potential loss or theft.

(b) It is prohibited to connect to the St John's College network any illegal mobile device

(c) Mobile devices should not be used to carry St John's College sensitive data for any longer then absolutely necessary and should be encrypted if possible to protect any data that is on the device.

7.6.7. **ANY MOBILE DEVICE HOLDING ST JOHN'S COLLEGE SENSITIVE DATA THAT IS STOLEN OR LOST MUST BE REPORTED TO THE LODGE IMMEDIATELY, REGARDLESS OF DATE/TIME.**

7.7. **Software Compliance**

7.7.1. College will provide staff properly licensed and authentic installations of software required for their role, and will ensure the necessary authorisation has been obtained.

7.7.2. Users of St John's College computer equipment and software shall not copy software or load unauthorised/unapproved software onto a St John's College computer including mobile equipment. The Senior IT Officer is responsible for giving authority and approval for software suitable for loading on St John's College equipment

7.7.3. St John's College's software shall not be given to any outsiders, including pupils/students.

7.7.4. The IT team shall maintain a register of authorised software, including the licence information. All licences and media shall be held securely in the IT team.

7.7.5. Licensed software shall be removed from any computer that is to be disposed of outside of St John's College.

7.7.6 Further Software Usage Policies should be included in the Staff Handbook.

7.8. Clear Desk/Clear Screen

7.8.1. Outside normal working hours, all confidential information, whether marked up as such or not, shall be secured; this may include within a locked office or in a locked desk. During normal office hours, such information shall be concealed or secured if desks are to be left unattended in unlocked/open access offices.

7.8.2. Confidential printed information to be discarded shall be kept secure until it can be placed in an approved confidential waste container for disposal.

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

7.8.4. All desktop computers must be logged off or locked automatically after a suitable period (unless required to remain on for operational purposes) to ensure that unattended computer systems do not become a potential means to gain unauthorized access to the network.

7.8.5. Unattended laptop computers, mobile telephones and other portable information assets and keys shall be secured e.g. in a locked office, within a lockable desk, or by a lockable cable.

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

7.8.7. St John's College shall ensure that members of staff have suitable storage facilities to enable them to comply with this Policy.

7.9. Information Backup

7.9.1. The requirements for backing-up information shall be defined based upon how often it changes and the ease with which lost data can be recovered and re-entered.

7.9.2. The IT Officers shall be responsible for ensuring that electronic systems and information are backed up in accordance with the defined requirements.

(a) Accurate and complete records of the back-up copies shall be produced and maintained.

(b) The back-ups shall be stored in a remote location which must:

(i) be at a sufficient distance to escape any damage from a physical disaster at St John's College

(ii) be accessible

(iii) afford an appropriate level of protection to the back-up media in terms of its storage and transportation to and from the remote location

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

(d) Restoration procedures shall be regularly checked and tested to ensure that they are effective and that they can be completed within the time allotted in the operational procedures for recovery.

8. Computer Equipment Disposal

St John's College subscribes to the University policy for disposal of equipment that is surplus to the requirements of the unit that originally purchased it. This policy may be found at http://www.ict.ox.ac.uk/oxford/disposal/.

The University policy stresses the importance of the need to remove sensitive and confidential data from the hard disks of computers that are ready for disposal.

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 use of surplus equipment can be made to further the College's charitable objectives,
8.1.2. Equipment that has residual value may be sold, either to College members or outside bodies, subject to the College's financial guidelines.
8.1.3. If the equipment cannot be reused or sold, then it should be recycled or disposed of in accordance with waste disposal regulations.
8.1.4. 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. Data Breach/Loss

Proper logs must be kept in order to allow traceability of security events involving cases of data breach or loss using particular IP addresses on either St John's College's network or the University backbone. Section *7.4 Network Security* details logging requirements in order to comply with this policy.

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's Data Protection Breach Policy (Appendix 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:

(a) data breach/loss/theft
(b) loss of equipment due to theft
(c) inappropriate access controls allowing unauthorised access
(d) equipment failure
(e) human error
(f) unforeseen circumstances such as fire and flood
(g) hacking
(h) '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 (Appendix 1). All investigations should be carried out urgently and reviewed once the issue has been resolved.

Further information on good IT security practice can be found on the University's Information Security site https://www.infosec.ox.ac.uk/.

10. Governance

This Policy will be reviewed regularly by the Data Protection Officer. Any changes will be approved by the Governing Body.

11. Enforcement

11.1 Breaches of data protection legislation could lead to civil or criminal actions against the individual or the College.

11.2 Non-compliance with this policy may lead to disciplinary action being taken up to and including dismissal.

The Governing Body of St John's College has approved this policy on 12th March 2014

Appendix 1 – 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

The 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 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 the 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 IT Officer immediately (within 30 minutes of becoming aware of the possible breach). The supervisor or line manager or equivalent must let the Data Protection Officer (DPO) know of the possible breach immediately (within 30 minutes of when it is brought to their attention). Information provided by the user about the possible breach should be made available to the DPO as soon as possible.

Immediate Containment/Recovery

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 College IT staff.

The line manager must inform the DPO as soon as possible. In the DPO's absence, inform the Bursar, Bursary Manager or President.

The DPO must 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.

The line manager, IT staff or DPO 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 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 DPO.
- 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 passwords, then these codes must be changed immediately, and the relevant agencies and members of staff informed.

Investigation

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

If the breach involves University data then the DPO must contact the University's Information Compliance Team or Data Protection Officer. The DPO should also contact the University where the breach may result in reputational/financial risk, whether or not this relates to University data. The University Information Security Team should also be contacted when the breach relates to IT infrastructure.

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.

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 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 is relevant:

"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 the DPO decides 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 DPO should fully review both the causes of the breach and the effectiveness of the response to it. A report should be written and considered by relevant committees and Governing Body.

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.

Implementation

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

Useful Contacts

Data Protection Officer: data.protection@sjc.ox.ac.uk

Appendix 2

Data Systems	**Responsible Officer**
Finance	Finance Bursar
Bursary	Principal Bursar
College Office, academic staff	Senior Tutor
Domestic Office, non-academic staff, conferences	Domestic Bursar
Student Welfare	Senior Dean
College Archive	Principal Bursar
Alumni records	Fellow for Alumni
Admissions (u/g)	Tutor for Admissions
Admissions (p/g)	Tutor for Graduates
Library	Fellow Librarian
College Buildings	Establishment Bursar
College Estate	Estates Bursar
GB & Committee minutes & agendas	President

The College Data Protection Officer is appointed by the Governing Body from time to time. Names of current College Officers are available from the President's Secretary (presidents.secretary@sjc.ox.ac.uk).

Appendix 3 – Password Protection Guidelines

Password strength is increased by the following characteristics:

(a) Contains both upper and lower case characters (e.g., a-z, A-Z) ,
(b) Digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./) ,
(c) A larger number of alphanumeric characters,
(d) Is not a single word in any language, slang, dialect, jargon, etc,
(e) Is not based on personal information, names of family, etc,
(f) Is never written down or stored on-line in the clear / unless encrypted,
(g) Passwords should be easily remembered but still complex and difficult to guess.

Appendix 4 Recommended end user practices for password protection:

(a) Do not use the same password for University accounts as for other non-University access (e.g., personal ISP account, MRC Portal, option trading, banking, etc.).
(b) Do not use the same password for various University access needs. Select one password for the IT Services and University Administration systems using the SSO and a separate password for St John's College IT systems.
(c) Do not share personal passwords with anyone, including personal administrative assistants or secretaries.
(d) Do not reveal a password over the phone
(e) Do not reveal a password in an email message
(f) Do not reveal a password to a manager, unless exceptional circumstances make this an absolute requirement.
(g) Do not talk about a password in front of others
(h) Do not hint at the format of a password
(i) Do not reveal a password on questionnaires or security forms.
(j) Do not share a password with family members
(k) Do not reveal a password to co-workers while on holiday
(l) If someone demands a password, refer them to this document or have them call the local IT Staff
(m) Do not use the "Remember Password" feature of applications (e.g., Outlook, Firefox, Safari)
(n) Do not write passwords down and store them anywhere in your office.
(o) Do not store passwords in a file on ANY computer system (including Blackberries, iPhones, Palm Pilots or similar devices) without encryption.
(p) Change passwords regularly in line with the password policies.

Appendix 5 Recommended end user practices to prevent virus problems:

(a) Always run a supported anti-virus software which is updated automatically with the latest anti-virus definitions. Sophos is available from the University via a site license.
(b) St John's College installed anti-virus software will be configured to update automatically. On personally owned or remote systems, the user should ensure that updates are performed automatically, and that a licence is renewed annually.
(c) NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then empty your Trash/Wastebasket.
(d) Delete spam, chain, and other junk email without forwarding.
(e) Never download files from unknown or suspicious sources.
(f) Always scan a USB key or other removable media from an unknown source for viruses before use and periodically on your own.
(g) Back-up critical data and system configurations on a regular basis and store the data in a safe place.

Appendix 6 Server General Configuration Guidelines:

(a) Operating System configuration should be in accordance with approved University guidelines.
(b) Services and applications that will not be used must be disabled where practical.
(c) Access to services should be logged and/or protected through access-control methods such as TCP Wrappers, if possible.
(d) The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.

(e) Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication will do.
(f) Always use standard security principles of "least required access" to perform a function. Do not use privileged accounts when a non-privileged account will do.
(g) If a method for secure channel connection is available, privileged access must be performed over secure channels, (eg. encrypted network connections using SSH or IPsec).
(h) All security related logs will be kept online for a minimum of 1 week.
(i) Security-related events will be reported to OxCERT, who will review logs and report incidents to IT Services management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
    - Port-scan attacks
    - Evidence of unauthorized access to privileged accounts
    - Anomalous occurrences that are not related to specific applications on the host.

Glossary

GDPR	General Data Protection Regulation
HFS	Hierarchical File Store
ICT	Information, Communications & Technology
ICTC	University of Oxford Information, Communications & Technology Committee (http://www.admin.ox.ac.uk/ictc/)
OxCERT	The University of Oxford's Computer Emergency Response Team
SSO	The University of Oxford Single Sign-On username.
VPN	Virtual Private Network as supplied by IT Services