Information Security Procedure

The following Information Security Procedure has been approved by Balliol College. Any amendments to the document requires College's approval. Each department within Balliol College is required to comply with this set of procedures. Support and guidance for departments is offered by Balliol College's ICT Team which in turn is supported by the central information security team, "InfoSec". Information Security is not a new requirement, and to a large extent the Data Protection Policy and these accompanying procedures formalise and regularise existing good practice within the college and wider university.

Balliol College is required by its Governing Body to review this document every three years to ensure any new developments are covered and protected.

Policy was approved by Executive Committee: November 2025
Next review: MT 2028
Author: Christopher Thompson – ICT Director

Contents

Information Security Procedure 0
Access to Information and Information systems 2
Access Control and Passwords 2
UK GDPR and Data Protection 4
Monitoring 4
Use of Personal Computer Equipment and Removable Storage 5
Data Movement 5
Servers 6
Network Security & Logging 6
Email and Internet Use 7
Mobile Computing 8
Mobile Device Security 8
Software Compliance 9
Clear Desk/Clear Screen 9
Information Backup 10
Non-University Cloud Storage and Services 10
Homeworking 10
Working at Home Equipment 11
Working at Home: Data Security and Confidentiality 11
Computer Equipment Disposal 11
Exceptions 12
UK GDPR - Data Breach/Loss & Incident Management 12
How to Recognise a Personal Data Breach 13
Do We Have to Make a Notification? 13
Notification – The College's Obligation 14
Notification - Your Obligation 14
Notifications to Individuals 15
Appendix 1 Key Data Systems 16
Appendix 2 Characteristics of a strong password 16
Appendix 3 Recommended practices for password protection 16
Appendix 4 Recommended end user practices to prevent virus problems: 17
Appendix 5 Server General Configuration Guidelines: 18
Appendix 6 Using BYOD or Self-Managed Computing Devices: 18
Appendix 7: Glossary 19

Access to Information and Information systems

- Information assets shall be 'owned' by a named officer within College. A list of information assets, and their owners, shall be maintained by the Data protection Coordinator(DPC). An information asset is any data, record, or system that holds value to the College and must therefore be managed and protected appropriately. In the context of data protection, information assets include all forms of information—digital or physical—that the college creates, collects, stores, processes, or transmits, and that have importance to its operations, decision-making, or legal obligations.
- Access to information shall be restricted to authorised users and shall be protected by appropriate practical physical and/or logical controls.
- Physical controls for information and information processing assets shall include:
    - Locked storage facilities (supported by effective management of keys)
    - Locks on rooms which contain computer facilities. Electronic locks should have their database systems reviewed at frequent intervals to ensure user access control is up-to-date.
    - 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.
    - "Clean desk" working
    - Encryption of data either transmitted or taken outside College's properties. Encryption of data should be appropriate to the level of risk assessment of the data.
    - Logical controls for information and information processing assets shall include passwords for systems access, unique "per-user" accounts, role-based access control mechanisms, and multi-factor authentication (where available and practical)

Access Control and Passwords

- Passwords and password management systems shall follow good practice on all systems including stand-alone systems on a single host for security and use the following techniques:
    - All system-level passwords (e.g., root, enable, admin, application administration accounts, etc.) must be changed from default manufacturer values, kept in a secure password vault with appropriate role-based access controller and with enforced MFA/2FA where possible.
    - All domain-attached computers where there are local accounts with administrator privileges must have passwords that are specific to that computer-the same password must not be used across all domain computers.

- The use of strong authentication (minimum length, high complexity, non-reusable passwords). Refer to Appendix 2 & 3 for Password Construction Guidelines.
- Users to have the ability to change their own passwords at any time
- Passwords to be changed at regular intervals appropriate to the information and resources being secured. Usually this is on an annual basis in line with the Universities guidance. A password expiry or account lock-out system to be in place to automate and enforce this process
- Passwords must not be inserted into email messages or other forms of electronic communication. If a password must be shared with others in order to open secure documents or zip files, then please follow these guidelines:
  - Passwords for secure documents **must never be shared via the same channel** as the document itself.
  - Passwords must not be sent **in clear text by email** or **written on/in the document**.
  - Staff must use **university-approved secure methods** for transmitting passwords. This could be the use of a person to person Teams Chat, text message, or WhatsApp secure message.
  - Passwords must be **unique, strong, and changed** if there is any suspicion of compromise.
  - Responsibility for safeguarding shared passwords lies with both sender and recipient.
- 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 ICT team immediately and change passwords on other systems that may have also been compromised. For further standards on password protection refer to Appendix 3.

- Access privileges shall be allocated based on the minimum privileges required to fulfil that member of staff's duties. Access privileges shall be authorised by the appropriate information owner or someone with authority to act on their behalf.
- All shared computer systems, with the exception of open access kiosk-style browser-only systems, will require users to authenticate before use, and will enable activities to be traced to an authenticated individual.
- Access to the College's administered networks via remote access must require a login to get access to any system on the internal network.
- Information owners shall review access permissions on an annual basis.
- 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.
- 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. College Officers or other relevant roles are responsible for completing leavers checklists and communicating those lists to appropriate sections of the College. ICT Department are responsible for ensuring accounts and access are closed in a timely manner for all access to systems that the leaver had.

- 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 restricted to those persons who are authorised to perform systems administration or management functions. Such privileges shall be authorised by the Director of ICT 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.
- 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.

UK GDPR and Data Protection

- Users must take particular care when sharing or disclosing personal data to any third party, to ensure compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. Before releasing any personal or special category data, users must seek authorisation from the relevant Information Asset Owner (IAO) and the Data Protection Coordinator (DPC) to confirm that the disclosure is lawful, necessary, and proportionate.

  In certain circumstances—such as requests from law enforcement or other statutory bodies—information may be disclosed without consent where there is a legal requirement or lawful basis to do so. In such cases, users must verify the legitimacy of the request, ensure that only the minimum necessary information is shared, and record the decision and rationale for disclosure. All of these special circumstance disclosures must also be approved by the DPC.

- To allow for potential investigations & traceability, electronic access logs (where available) should be kept for a minimum of six months, or for longer, Logs could include user and group memberships, authentication details, access activity, systems events, and audit trails. Logs are owned and managed by the ICT Department.
- Further information on UK GDPR and Data Protection is included as a further section of this procedure

Monitoring

- 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 -

https://www.ox.ac.uk/about/how-we-are-run/governance-finance/legislation/it-regulations-1-of-2002 ".

- Any exception to these provisions must be subject to a specific risk assessment and is only permitted where approval is given by the DPC. In certain circumstances the Head of House must authorise further invasive monitoring, such a the content of email.

Use of Personal Computer Equipment and Removable Storage

- Privately owned computing equipment will not be allowed to connect to the College managed network. All connections to the College Administration networks will be from college managed devices.

There may be times where the transfer of information outside the college is required. Appropriate safeguards must be put in place to protect the data based on its risk and category rating.

It is the responsibility of all members of the college to ensure that the data they process, store, or transport have the required protection in line with the mode of transport and the sensitivity of the data. Before moving any data specified as Special Category Data, permission from the DPC must be obtained.

Data Movement

Personal data is defined as "Any information that relates to an identified or identifiable natural person who is or can be identified, directly or indirectly, in particular by reference to an identifier such as a name, ID number or identifier or one or more factors specific to that individual such as health information." Emails and contacts stored in an email system count as personal data, as do most CVs, references, and job applications.

- Information containing personal data concerning pupils, students, alumni or staff that is to be saved onto removable storage shall be encrypted before storage. Training is available via the ICT Department.
- Special category data (covered by the UK GDPR) must only be stored on removable storage devices temporarily and must be protected from loss and/or theft. Removable storage devices must have encryption enabled, or software installed to encrypt data that is on the device. Other means of transferring the data should be explored before using removable storage devices.
- College information shall not be retained on removable storage devices longer than necessary (i.e. once information that has been updated on a computer owned by a member of staff is uploaded onto College systems, it shall be securely deleted from the removable storage device).

It is the responsibility of all members of the college to ensure that the data they process, store, or transport have the required protection in line with the mode of transport and

the sensitivity of the data. Before moving any data specified as Special Category Data, permission from the DPC must be obtained.

Servers

These procedures specifically apply to server equipment owned and/or operated by the College, and to servers registered under any College-administered network.

- All internal servers deployed in the College must be administered by an operational group that is responsible for system administration. The operational group at Balliol is the ICT department. 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 includes peer review and approval.
- Physical servers must be housed in a location where physical access and the server environment (power, temperature, and humidity) can be controlled.
- Servers should be backed up to offsite storage, such as the University HFS.
- Servers must be registered with the College ICT team. As a minimum, the following information is required to positively identify the point of contact:
    - Server contact(s) and location, and a backup contact
    - Hardware and Operating System/Version
    - Main functions and applications, if applicable

Balliol College ICT Staff will police its own policies in this area but will seek regular review and audit from the University IT Services and the wider IT support community in the University.

Network Security & Logging

- Responsibility for management and security of the College's internal network rests with the ICT team. The ICT team for the College must:
    - Ensure network/systems administrators are suitably trained in security
    - Proper logs are kept in accordance with University IT Services policies.
    - Review file system security to ensure users have only the access they need
    - Protect physical network from interception/damage/interference
    - Restrict unauthorised traffic using a firewall or equivalent device
    - Regularly review and maintain network security controls and device configurations
    - Remove permissive firewall rules once there is no longer a business requirement
    - Permit remote access to firewalls (e.g. for configuration or monitoring) only when there is a clear, documented business requirement and appropriate authorisation, subject to periodic review.

    - 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 University IT Services policy. It is currently recommended that at least 60 days of logs be kept, and longer if possible, to allow for any post-incident review. Logs must include identifiable data to enable traces back to specific events, computer systems, and specific users. Timestamps, MAC addresses, IP Addresses, and where possible usernames should be included in logging systems. These logs should be proactively monitored and reviewed as an early warning system for hacking or any other form of unauthorised activity.

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

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://www.ox.ac.uk/about/how-we-are-run/governance-finance/legislation/it-regulations-1-of-2002

Where email systems are hosted locally, it should be checked by the College's ICT Services Department on a regular basis to ensure that it is being appropriately updated in regard 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 "blacklist" of banned email addresses. For centrally hosted email by University IT Services (Office365), their information policy will take precedence.

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

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

Mobile Computing

Applies to any mobile hardware that is used to access College resources, whether the device is owned by the user or by the College. Persons with laptop computers and other mobile computing devices including mobile phones shall take all sensible and reasonable steps to protect them from damage, loss or theft. Such steps may include:

- Securing laptops and removable media whether in college or while travelling.
- 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
- Persons using computing equipment in public places shall ensure that confidential information cannot be viewed by unauthorised persons (e.g. stations, airports, trains, etc.)
- Use of external wireless access points shall be permitted provided that the firewall software provided with the mobile computer is activated.
- 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.

Use of any mobile computing device owned by the College, or that is used to access College data (including email) must be in accordance with these procedures and for non-academic staff, the relevant section of the Staff Handbook.

Mobile Device Security

- Anyone using mobile devices and related software for network and data access will, without exception, use secure data management procedures. All mobile devices must be protected by a strong password of 12 characters or more, or PIN, or biometrics, and must never be shared with anyone.
- Any mobile device that is used to access College resources should have the remote wipe capability of the device turned on to protect against potential loss or theft.
- It is prohibited to connect to the College network any mobile device that has undergone a 'jailbreak' procedure. A **jailbroken device** is a smartphone, tablet, or other electronic device whose manufacturer-imposed operating system restrictions have been deliberately removed or bypassed. This is usually done by exploiting security vulnerabilities to gain "root" or administrator-level access.
- Mobile devices should not be used to carry sensitive College data for any longer then absolutely necessary and should be encrypted to protect any data that is on the device.

ANY COLLEGE PROVIDED MOBILE DEVICE THAT IS STOLEN OR LOST MUST BE REPORTED TO THE ICT TEAM IMMEDIATELY, REGARDLESS OF DATE/TIME. USE THE OUT OF HOURS ICT SUPPORT NUMBER (LODGE HAVE THIS NUMBER) WHEN NEEDED. LOST PERSONALLY OWNED DEVICES SHOULD BE REMOTELY WIPED AS SOON AS POSSIBLE.

Software Compliance

- College will provide properly licensed and authentic installations of software to all users who require it in the course of their duties.
- Users of College computer equipment and software shall not copy software or load unauthorised/unapproved software onto a College computer including mobile equipment. The ICT Director is responsible for giving authority and approval for software suitable for loading on College equipment
- College's software shall only be distributed and used as licenced.
- The ICT team shall maintain a register of authorised software, including the licence information. All licences and media shall be held securely in the ICT team.
- Licensed software shall be removed from any computer that is to be disposed of outside of the College.

Clear Desk/Clear Screen

- 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.
- 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.
- Documents shall be immediately retrieved from printers, photocopiers and fax machines. Secure print should be enabled where possible.
- All desktop computers must be logged off or locked automatically after a suitable period* (unless required to remain on for operational purposes) to ensure that unattended computer systems do not become a potential means to gain unauthorised access to the network. It is suggested that 15 minutes is a suitable time.
- Unattended laptop computers, mobile telephones and other portable assets and keys shall be secured e.g. in a locked office, within a lockable desk, or by a lockable cable.
- Those in charge of meetings shall ensure that no confidential information is left in the room at the end of the meeting.
- The College shall ensure that members of staff have suitable storage facilities to enable them to comply with these procedures and the Data Protection Policy.

Information Backup

- 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.
- The ICT team shall be responsible for ensuring that systems and information are backed up in accordance with the defined requirements.
- Accurate and complete records of the back-up copies shall be produced and maintained.
- The back-ups shall be stored in a remote location which must:
    - 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
    - scan backups as they are being created to avoid backing up malware
    - be immutable and "air-gapped" to reduce risk of cyber/malware attacks.
    - scan backups using up-to-date systems to detect previously undetectable malware
- Back-up media shall be regularly tested to ensure that they can be relied upon for emergency use when necessary.
- Restoration procedures shall be regularly checked and tested to ensure that they are effective and that they can be completed within the time allotted in the operational procedures for recovery.
- Backup for physical information assets - for example printed paper documents, and media containing information – shall be governed as appropriate by the same principles as above.

Non-University Cloud Storage and Services

- The use of cloud services for the processing and/or storage of personal or sensitive information should be risk assessed and adhere to all other sections of these procedures. Individuals must ensure they do not make use of personal cloud services for the processing and/or storage of personal or sensitive information unless those services have also been risk assessed and adhere to all other sections of this these procedures.
- All cloud services/resources other than those provided by the college and/or the university must be protected by Multi-Factor Authentication.

Homeworking

We support homeworking in appropriate circumstances either occasionally (to respond to specific circumstances or to complete particular tasks) and in some cases on a regular (full or part-time basis). In addition, occasional or permanent homeworking can, in certain circumstances, be a means of accommodating a disability and can be requested as a means of flexible working.

These procedures sets out how we will deal with requests for homeworking, and conditions on which homeworking will be allowed. If you are allowed to work from home you must comply with these procedures and the Data Protection Policy.

These procedures do not form part of any employee's contract of employment, and we may amend it at any time.

Working at Home Equipment

- Home working / remote working electronic equipment will be provided by the college once proper authorisation has been given by the head of department.
- College is not responsible for associated costs of you working from home including the costs of heating, lighting, electricity or telephone calls.

Working at Home: Data Security and Confidentiality

- You confirm that you have read and understood our policies relating to computer use, electronic communications, password security and data security and that you will regularly keep yourself informed of the most current version of these policies
- All College related communications must be made through your College email address.
- If you discover or suspect that there has been an incident involving the security of information relating to the College, students or anyone working with us, you must report it immediately to the DPC. At Balliol College, the role of the DPC is fulfilled by the Domestic Bursar.

Computer Equipment Disposal

- Balliol College responsibly recycles all IT equipment and operates a **zero-landfill policy** for IT waste.
- The College 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.

- Equipment that has residual value may be sold, either to University/College members or outside bodies once all data has been completely removed from devices.
- 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.

Disks that have contained information classed as confidential or sensitive must be secure wiped using a tool such as PGP or DBAN, physically destroyed, or recycled by a registered third-party who can supply data-destruction certificates for each recycled disk.

Exceptions

An exception to a published policy or procedure may be granted in any of the following situations:

- Temporary exception, where immediate compliance would disrupt critical operations.
- Another acceptable solution with equivalent protection is available.
- A superior solution is available. An exception will be granted until the solution can be reviewed, and standards or procedures can be updated to allow the better solution.
- A legacy system is being retired (utilize a process to manage risk).
- Lack of resources,
- All exceptions to this policy must be approved by the DPC/DPO.
- All requests for exceptions must include:
    - Description of the non-compliance
    - Anticipated length of non-compliance
    - Assessment of risk associated with non-compliance
    - System(s) associated (for example, host names or IP addresses)
    - Data Classification Category(s) of associated system(s)
    - Plan for alternate means of risk management
    - Metrics to evaluate success of risk management (if risk is significant)
    - Review date to evaluate progress toward compliance

UK GDPR - Data Breach/Loss & Incident Management

Balliol College has appointed MooreClear Ltd as its Data Protection Officer (DPO). The Domestic Bursar of Balliol College is appointed internally as Data Protection Coordinator (DPC) and will manage the College's relationship with the DPO.

- If you know or suspect that a personal data breach has occurred, do not attempt to investigate or resolve the matter yourself. Please inform the DPC, immediately. You must also preserve all evidence relating to the potential personal data breach. Failure to comply with these procedures may result in disciplinary action being taken against you.

- We must make our formal notification to the ICO (Information Commissioner's Office) within 72 hours of becoming aware of a breach if the personal data breach is serious and there is a high risk of harm or damage arising. It is therefore crucial that you notify the DPC immediately so that we are able to comply with the law.
- We may also need to inform the individual(s) whose data has been subject to the breach. Our DPC (with advice from the DPO if required) shall make the final determination in respect of any notifications to individuals. You are not permitted to notify individuals without prior consultation with or instruction from the DPC.
- Regardless of whether we are required to make a notification to the ICO or individuals, all personal data breaches must be notified to our DPO via the DPC who shall maintain a record of the incidents.
- We shall document, with your mandatory cooperation, details of all breaches, their effects and the remedial action taken. We shall investigate whether or not each breach has occurred as a result of human error or a systemic issue and see how a recurrence can be prevented, whether this is through better processes, further training or other corrective steps. Failing to notify a breach when required to do so can result in Balliol College incurring a significant fine and publicity of the failure may cause irreparable reputation damage. Please note that failure to abide by our policies and procedures may result in disciplinary action.

How to Recognise a Personal Data Breach

- A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data whether unintentional or deliberate.
- Whenever any personal data is lost, destroyed, corrupted or disclosed, a personal data breach will have occurred. This includes circumstances where someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.
- If in any doubt, notify our DPO via the DPC, who shall make the final determination of whether a breach has occurred.

Do We Have to Make a Notification?

Our DPO shall determine the need to notify the ICO and/ or the individual(s) affected. We may also need to notify organisations that regulate our activity and the University of Oxford or other third parties.

In determining whether we must notify the ICO, our DPC (with advice from the DPO) shall establish the likelihood and severity of the resulting risk to people's rights and freedoms including consideration of the possible emotional distress and physical, material or non-material damage to the person such as but not limited to:

- loss of control over their personal data;

- 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.

Where it is likely that there will be a risk then we must notify the ICO, where it is unlikely then we need not. Where our DPO determines that a notification is not required, a record shall be kept of the reasons for that decision.

We do not always have to notify individuals of a personal data breach having occurred, only where the breach is likely to result in a high risk to the individual(s) concerned.

Notification – The College's Obligation

- Our DPO shall submit our formal notification to the ICO (or, in the case of individuals outside the UK, the relevant supervisory authority) as soon as possible and in any event within 72 hours of being made aware of the breach. Time runs from the time at which the organisation becomes aware of the breach, i.e. that you become aware of the breach and not the time at which our DPO or the DPC is made aware.
- Notification must be made notwithstanding whether or not we are in possession of full details of the breach, damage caused or individuals affected.
- In the event that we are not able to make our notification within 72 hours we must give notification immediately thereafter and give reasons for our delay.

Notification - Your Obligation

On notifying the DPC (who shall notify our DPO of the breach identified), you must assist in providing information as above, to the best of your knowledge. If you were not the individual to identify the breach but you are able to assist in providing relevant information you must cooperate in providing this information so that we are able to make our notification promptly and in any event within the time limit. When reporting a breach, we must provide:

- a description of the nature of the personal data breach including, where possible:
- the categories and approximate number of individuals concerned; and
- the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

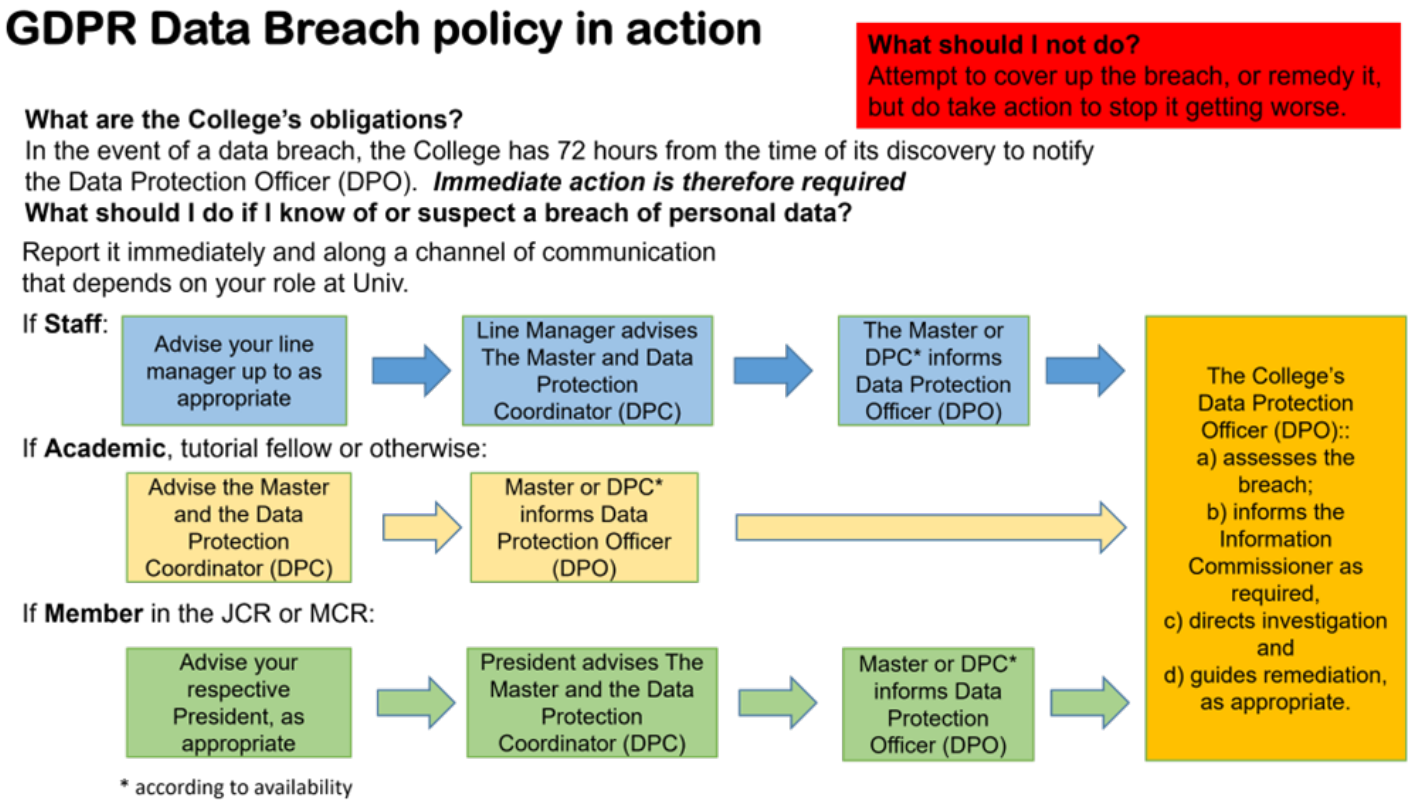
Where not all information is immediately available, you must provide the information to our DPO via the DPC as it becomes available and in any event without undue delay. Our DPO shall update the ICO and any other notifiable person with corresponding promptness. Our DPO shall keep the ICO updated of any anticipated or actual delay.

Notifications to Individuals

Where our DPC (with advice from the DPO) has determined that we must notify the individual(s) concerned, we will set out, in clear and plain language, the nature of the personal data breach and, at least provide:

- the name and contact details of your data protection officer so that the individual(s) can request any further information they may require;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects.

Guidance on handling a data breach



Appendix 1 Key Data Systems

The below table includes a list of the key data systems within the College and their location. This is not an exclusive list as other, sometimes more specialised, data systems are used within College.

Data Systems	**Location/'Owner'**
Payroll	Bursary
Accounts	Bursary
Members	Bursary / HR
Alumni	Development Office
Admissions (u/g)	Academic Office
Admissions (p/g)	Academic Office
Book Usage	Library
GB & Cttee minutes & agendas	Master's Office

Appendix 2 Characteristics of a strong password

- Contains both upper and lower case characters (e.g., a-z, A-Z)
- Digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- At least 16 alphanumeric characters long and is a passphrase (Ohmy1stubbedmyt0e).
- Is not a single word in any language, slang, dialect, jargon, etc.
- Is not based on personal information, names of family, etc.
- Is never written down or stored on-line in the clear / unless encrypted.
- Passwords should be easily remembered but still complex and difficult to guess.

One way to do this is create a password based on a song title, affirmation, or other phrase personal to you. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

Appendix 3 Recommended practices for password protection

- 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.).
- 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 College ICT systems.

- Do not share passwords with anyone, including personal administrative assistants or secretaries.
- Do not reveal a password over the phone to ANYONE
- Do not reveal a password in an email message
- Do not reveal a password to a manager, unless exceptional circumstances make this an absolute requirement.
- Do not talk about a password in front of others
- Do not hint at the format of a password (e.g., "my family name")
- Do not reveal a password on questionnaires or security forms.
- Do not share a password with family members
- Do not reveal a password to co-workers while on holiday
- If someone demands a password, refer them to this document or have them call the local ICT Staff
- Do not use the "Remember Password" feature of applications (e.g., Outlook, Firefox, Safari)
- Do not write passwords down and store them anywhere in your office.
- Do not store passwords in a file on ANY computer system (including mobile phones, tablets, or similar devices) without encryption.
- Change passwords at intervals in line with the specific system requirements or password policies.
- Use a password manager to securely store passwords. Reputable and widely-used options like LastPass, 1Password, KeePassXC, and Bitwarden are good options.

Appendix 4 Recommended practices to prevent virus problems:

- Always run the standard, supported anti-virus software which is available from the University.
- 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 frequently, and that a licence is renewed annually.
- 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.
- Delete spam, chain, and other junk email without forwarding.
- Never download files from unknown or suspicious sources.
- Always scan a USB key or other removable media from an unknown source for viruses before using it.
- Back-up critical data and system configurations on a regular basis and store the data in a safe place.

Appendix 5 Server General Configuration Guidelines

- Operating System configuration should be in accordance with approved University guidelines.
- Services and applications that will not be used must be disabled where practical.
- Access to services should be logged and/or protected through access-control methods such as physical and application firewalls, if possible.
- 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.
- 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.
- 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.
- 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).
- All security related logs will be kept online for a minimum of 1 week.
- Security-related events will be reported to OxCERT, who will review logs and report incidents to ICT Services management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
- Port-scan attacks
- Evidence of unauthorised access to privileged accounts
- Anomalous occurrences that are not related to specific applications on the host.

Appendix 6 Using BYOD or Self-Managed Computing Devices

Guidance when using a "bring-your-own-device" at work, or when you manage the configuration of a computer yourself: Using BYOD or Self-managed Computing Devices

Your Responsibilities

If you are using a self-managed computer, you have a responsibility to configure it securely.

Self-managed computers

Any computer or device you use that has not been configured by the University Supported Desktop or is not automatically configured by a service in your College counts as "self-managed". For the most part this applies to all Academic staff computers and devices.

This "automatic configuration" needs to be of the kind that keeps your computer up-to-date on a regular basis. If the computer is configured once, at the time it is allocated to you, it is quite likely to count as self-managed and you need to take responsibility to keep it securely configured.

Many laptops and many desktops are not configured using Supported Desktop. You still have a responsibility to protect all the information they your devices may carry. With a self-managed computer you have the responsibility to configure it as strongly and safely as practical. Follow the link to “Protect my Computer" above.

Department/College-managed computers

Some Departments have their own methods for managing the configuration of computers for staff, for their labs, and in some cases for students. Check with your Department computer support team if you are not sure if a computer you are using counts as self-managed.

BYOD

A BYOD (Bring Your Own Device) is any computer or device that you own, that is used for any kind of University business. If you do University work on it, you are responsible for ensuring it is configured securely.

Further information can be found at the Universities page on protecting your computer

https://www.ox.ac.uk/students/life/it/training-and-skills/information-security-and-data-protection

Appendix 7: Glossary

- DPA The Data Protection Act 1998
- DPO Data Protection Officer
- DPC Data Protection Coordinator
- UK GDPR UK 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 ICT Services