Brasenose College Information Classification and Handling Scheme v4 (June 2024)

Overview

This scheme is designed to help College members determine best how to process College data easily and securely. The scheme is a balance between security and usability. Any scheme that is to be effective, must be achievable. Over complication of methodology is often counterproductive in the goal of information security. The overview is to minimise the number of platforms that store College data and to maximise processing on University/College hosted systems, or approved cloud-based systems that have been scrutinised with suitable data agreements (e.g. Office365).

Data Breach Rules

A data breach is a security incident in which internal or confidential data is copied, transmitted, viewed, stolen, destroyed, or used by an individual unauthorized to do so. This document defines internal and confidential classifications.

Examples include sending a file (regardless of encryption) containing names and addresses to the wrong email recipient or leaving sensitive hard copies of documents in a public meeting room. It is important every data breach (or significant near miss) in college is reported, no matter how big, as this is a critical element in monitoring and improving the college's approach to data security. Anyone can make a mistake, especially under time pressure, and the College should employ a culture of open reporting without fear of recrimination.

All data breaches, regardless of perceived size or risk, should be reported immediately to your line manager. In the absence of a line manager, the *ICT Director, or Infrastructure Officer*. Failure to declare a data breach may result in disciplinary action. All incidents should be logged centrally by the College (data.protection@bnc.ox.ac.uk).

Help Encrypting and Sending Documents Securely

The College Staff website has a number of guides to help with encrypting and protecting common file types (e.g., Word, Excel or PDF) as well as safe use of removable/portable storage devices.

https://staff.bnc.ox.ac.uk/guides/

There are also guides for use of secure file transfer tools/platforms such as OneDrive.

Common Data Definitions

Brasenose College data can be classified according to the following scheme. The following definitions may help in understanding terms mentioned in it:

Public data: Information should be classified as "**Public**" when unauthorised disclosure has no potential to cause any damage or distress to the interests, employees or reputation of the College, its affiliates or data subjects. This classification should be used for information for the public domain and does not carry appreciable confidentiality risk.

Internal data: Information should be classified as ''**Internal**'' when unauthorised disclosure has a potential to cause some damage or distress to the interests, employees or reputation of the College, its affiliates or data subjects. This classification should be used for information for a defined audience but is not particularly sensitive.

Confidential data: Information should be classified as **"Confidential"** when unauthorised disclosure has a potential to cause serious damage or distress (including severe or long-term impact) to the interests, employees or reputation of the College, its affiliates, or data subjects. In GDPR terms, any special category (see below) data should always be considered **"Confidential"** data.

General Data Protection Regulation & Other Terms Used in this Scheme

Personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special category personal data is personal data (of a living individual) which the GDPR says is more sensitive, and so needs more protection. Loosely, it can be defined as anything that can be used to discriminate against an individual. Examples are: Race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life or sexual orientation. However, one common exception to this loose definition is 'age' – a person's age is not classed as special category data even though it can be a common discriminatory agent.

Basic Personal data in this document refers to information that whilst can be defined as personal data, can already be considered in the public domain. E.g. Names of published Academics, University email addresses and internal phones numbers for College or University staff - Any data that is already publicly published about an individual.

How to identify what class of data you are accessing/storing/sending.

Classification Level	Information		Rationale
Confidential	**Teaching and research** • Special Category Personal Data relating to students and participants • Mass (>100 records) Personal Data relating to students or participants • Patient identifiable data • Confidential College data • Intellectual Property • Examination papers (under preparation)	**Development and Fundraising** • Special Category Personal Data relating to alumni and donors • Mass (>100 records) Personal Data relating to alumni and donors • Major Donations	The need for confidentiality will far outweigh requirements for availability. Unauthorised disclosure may result in: • Severe financial harm • Long-term reputational damage • Severe regulatory action • Interruption of critical business system/processes • Research contracts revoked Risks to the safety or wellbeing of staff, students, alumni, donors, applicants or visitors
	Operations: **e.g.HR/Finance/Conference/IT** • Special Category Personal Data relating to staff, visitors or guests. • Unpublished financial accounts • Payment cards and bank details • Passwords • Mass (>100 records) Personal Data • Details on storage of hazardous materials • Details on storage of high value assets	**Admissions and Outreach** • Special Category Personal Data relating to applicants or the public. • Mass (>100 records) Personal Data relating to applicants or general public • Any Personal Data relating to Under 16s	
Internal (Default)	**Teaching and research** • Personal Data relating to students other than basic student data (see Below) • >50 basic data student records • Any Personal Data relating to participants • Research/Teaching contracts • Marks, prizes, appeals and complaints • Unpublished research papers • Course and exam information • Student discipline information	**Development and Fundraising** • Any Personal data relating to alumni and donors. • Project research and analysis • Gift administration and donations	Unauthorised disclosure may result in: • Financial harm • Reputational damage • Regulatory action • Distress to personnel • Impact on business systems/processes
	Operations: **e.g.HR/Finance/Conference/IT** • Personal Data relating to staff other than basic staff data (see below) • >50 basic data records • Any Personal Data relating to visitors • Staff performance and discipline information • Financial records and transactions • Information on Intranets, network shares or SharePoint • Internal governance documents or reports • Meeting agendas & minutes • IT system and infrastructure information • Usernames and IDs • Supplier contracts • CCTV	**Admissions and Outreach** • Any Personal Data relating to applicants or general public. • Applications, aptitude tests, interview notes, outcomes • Funding assessment information • Information relating to commercial activities	

Public	• Names, email addresses and phones numbers for staff, <50 records (basic staff data) • Names, email addresses and phones numbers for students, <50 records (basic student data) • Public internet information • Brochures • Prospectuses • Published financial reports • Published academic & research reports • Press releases	• Unauthorised disclosure causes no harm • Information likely already in the public domain • Information is routinely published.

Data Handling Rules

Action	Public	Internal	Confidential
Marking	• Information should be identifiable as originating from Brasenose College • Information published publicly such as web site content or College brochures should have a record of the decision to release the information noted.	• Information should be identifiable as from Brasenose College. • It is good practice to mark "INTERNAL" on the front page of each document and on front of folders, binders.	• Information should be identifiable as from Brasenose College. • It is good practice to mark "CONFIDENTIAL" on all pages of the document and on front of folders, binders as well is in the subject line and body of all emails. • The same rule applies to removable electronic and optical media, such as USBs, CD-ROMs, microfilms, photographs, and removable hard drives.
Dissemination	• Widely available. • May be viewed by anyone, anywhere in the world subject to restrictions in law.	• Dissemination only to members of the College or organisations and individuals within the University of Oxford. • Access to the information should require an individual to authenticate themselves by password or similar. E.g. A personal email account secured by a password (and potentially two factor authentication). • Dissemination should be on a "need to know" basis.	• Dissemination only to recipients authorised by the information owner on the basis of genuine and justified 'need to know'. In accordance with appropriate retention schedule • Appropriate access control measures to be taken by depending on method of dissemination and storage. • It is good practice to advice the recipient if and when they should delete the information sent.
Termination of employment	• No restrictions.	• Prior to termination ensure return of all internal information held and full revocation of access rights and permissions granted to systems and data stores holding internal information.	• Prior to termination ensure return of all confidential information held and full revocation of access rights and permissions granted to systems and data stores holding confidential information.
Document Creation	• No restrictions.	• Depending on the sensitivity and confidentiality of the information, consider protecting document through: *Marking as final* (let reader know the document is final and make it read-only). *Restricting permissions* (grant people access while removing their ability to edit, copy or print).	• Protect document by: *Restricting permissions* (grant people access only on a justified ''need to know'' basis). *Marking as final* (let reader know the document is final and make it read-only). • Depending on the sensitivity and confidentiality of the information, consider initially protecting document through encrypting with password to prevent leakage of 'sensitive work in progress'. Guides on how to encrypt common file types can be found here: https://staff.bnc.ox.ac.uk/guides/
Digital Storage	• No restrictions.	• Information should be stored on College or University approved systems on monitored and restricted access mediums managed by either local College IT or central IT Services where possible. • Storage on external system may be possible subject to a Risk Assessment approval. Please consult IT for more information. • Depending on the sensitivity and confidentiality of the information, consider restricting access by: *Amending default folder permissions* (full control, modify, read only) *Amending permissions inherited from parent folder*, *Regularly monitoring users* (adding or deleting), *Password protection* for sensitive files at document level.	• Information should be stored on College or University approved systems in monitored and restricted access drives managed by either local College IT or central IT Services. • Storage on external systems may be possible subject to Third Party Risk Assessment approval by the Bursar. • Restrict access by: *Amending default folder permissions* (full control, read only) *Amending permissions inherited from parent folder*, *Regularly monitoring users* (adding or deleting), *Password protection* for sensitive files at document level.

Paper Storage	• No restrictions.	• Information should be created in a secure environment and stored in a locked filing cabinet or equivalent.	• Information should be created only in a secure environment and stored in locked filing cabinet or equivalent or in an office which is locked or attended only by authorised staff. • In open access offices, documents should not be left unattended on desks, printers, or photocopiers. • Locks should conform to an appropriate standard of security. • In open access offices, documents shall not be left unattended. • Ideally, rooms containing confidential paper storage should have SALTO door entry access control installed to log access.
Taking Off-site	• No restrictions.	• Documents can be taken off site but should be kept securely in a document holder. • Internal data taken off-site by portable data storage devices (e.g. USB memory stick) must be encrypted. Please consult with IT if you are doing this.	• Documents can be taken off site only exceptionally for shortest time possible, and only with *authorisation from the data owner or Bursar*. • Confidential data taken off-site by portable data storage devices (e.g. USB memory stick) *must be encrypted and with the express permission of the Bursar*. • Documents should not be left unattended.
Faxing	• No restrictions.	• Ensure fax number is entered correctly.	• Not permitted, you should not fax anything confidential.
Posting	• No restrictions.	• Sealed envelope. • Normal internal and external mail services can be used.	• Sealed in a sturdy envelope marked as ''confidential''. • Originals and copies should be delivered by hand where possible. • If delivery by hand not possible, use recorded delivery or courier delivery with the confirmation of receipt. • Depending on the recipient, or who may open their mail, consider: *Sealed double envelope* with inner envelope marked as "confidential".
Printing	• No restrictions.	• Print only what you really need to hold as hard copy. • Use College managed or provided printers where possible.	• Print only what you really need to hold as hard-copy and dispose of securely as soon as possible. • Use only College managed or provided printers
College Owned Devices & Portable Media	• No restrictions.	• Data may be accessed and stored on College PCs, laptops and portable media providing Sophos endpoint protection is in place and the Operating System (OS) is in-support and up to date on security patches. • Access to the device should be controlled in accordance with the College's security policy. • Full disk encryption should be deployed where possible. • Laptops should be always kept secure and locked away overnight when left in the office. If travelling by car, laptops must only be stored out of site (e.g. In the boot)	• Data may be accessed and stored on College PCs, laptops and portable media providing Sophos endpoint protection is in place and the Operating System (OS) is in-support and up to date on security patches. • Access to the device should be controlled in accordance with the College's security policy. • Full disk encryption must be deployed to any device taken off site (including mobile phones). • Avoid downloading files to laptops and portable media but where this is not possible, files should be retained only on a temporary basis and erased as soon as possible. • Laptops should be always kept secure and locked away overnight when left in the office. If travelling by car, laptops must only be stored out of site (e.g. In the boot)

Personally, Owned Devices	• No restrictions.	• Data may be accessed and stored on personal PCs and mobile devices only when those devices are setup in accordance with the University's guidance on protecting personally owned devices. https://www.infosec.ox.ac.uk/protect-my-computer	• *Only with specific Bursar or IT Director (in Bursar's absence) approval* and in accordance with the University's guidance on protecting personally owned devices. https://www.infosec.ox.ac.uk/protect-my-computer No-one should be accessing (remotely or otherwise) or storing confidential information on personal devices without permission. This includes personal phones.
University SharePoint & O365 SharePoint	• No restrictions.	• Depending on the sensitivity and confidentiality of the information, consider assigning specific permissions. • Use the simple standard three permission groups for each SharePoint site: Owner, Member and Visitor. • By default, all sites, lists, and libraries in a site collection inherit permissions settings from the site that is directly above them in the site hierarchy. Owners can assign unique permissions to a list, library, or survey, through first breaking permissions inheritance, then assigning unique permissions. Permissions can be altered down to the document level.	• Assign specific named permissions - MANDATORY. • By default, all sites, lists, and libraries in a site collection inherit permissions settings from the site that is directly above them in the site hierarchy. *If in doubt, ask the College IT team* to check permissions before granting wider access to a site or dissemination. • Owners can assign unique permissions to a list, library, or survey, through first breaking permissions inheritance, then assigning unique permissions. Permissions can be altered down to the individual document level. • Consider using ''ALERT ME'' function to be informed about changes to the site is made by others.
University OxFile	• N/A	• Retired Service – Do Not Use • Use OneDrive instead.	• Retired Service – Do Not Use • Use OneDrive instead.
University O365 OneDrive	• No restrictions.	• By default, access to OneDrive for Business documents are restricted only to the OneDrive owner, until sharing options are enabled. Permissions can be altered down to the document level. • Storage on O365 OneDrive is permissible.	• By default, access to OneDrive for Business documents are restricted only to the OneDrive owner, until sharing options are enabled. Permissions can be altered down to the document level. Sharing confidential information by this route is approved and encouraged. • The user should ensure that access rights are set up on a ''need to know'' basis and removed when no longer required.
University O365 MS Teams Platform	• No restrictions.	• When using specific 'Teams', owners should ensure that access rights are set up based on need to know and maintained. When uploading data bear in mind that the content is visible to all the members of that 'Team' including Guests until access removed. • Organisers of MS Team meetings should ensure that access rights are set up based on need to know and guest access is removed after their requirement for access is ended. • Sharing internal information on MS Teams is considered a secure method. • After a meeting(s) or projects are over, the owner should consider removing files from the Teams storage medium.	• When using specific 'Teams', owners should ensure that access rights are set up based on need to know and maintained. When uploading data bear in mind that the content is visible to all the members of that 'Team' including Guests until access removed. • Organisers of MS Team meetings should ensure that access rights are set up based on need to know. When uploading data to meeting file space, bear in mind that the content is visible to all the participants of that meeting, including 'guests'. • Sharing confidential information on MS Teams is considered a secure method. • After a meeting(s) or projects are over, the owner should consider removing files from the Teams storage medium.
University O365 Email	• No restrictions.	• Distributing internal level information 'as is' via University O365 email accounts and to other University O365 email addresses is fine. • When distributing to non-University O365 email accounts, consider: *Using encryption and passwords* to protect specific files / attachments.	• Where transmitted via Outlook client or Outlook web service, the internal transmission of confidential data between University email accounts is automatically encrypted in transit and at rest. So: a. Personal University email accounts are protected by a password and two factor authentication. As such, when sending any information to personal University email account, **no** further security action is required. The setting of passwords on files for internal distribution is discouraged.

		Always consider. *Double-checking the 'To'/'CC'/'BCC' address* before sending the email. Using blind copy (bcc) when emailing multiple recipients. *Whether recipient may have delegated authority* to others. *Restricting permissions from forwarding the email* (Recipients can read the message but cannot forward, print or copy). *Requesting a delivery and read receipt* for the message.	b. Generic University email accounts can be accessed by several individuals. Users should consider sending confidential information directly to personal accounts instead. Where this is not possible, password protecting attachments and only letting those intended to know the password by another authenticated means (e.g., MS Teams message) is acceptable. • Subject of the email should indicate CONFIDENTIAL. • Where confidential data is transmitted via Outlook 365 (local client or webmail version) to external email recipients, use Outlook 365 PROTECT function for encrypting. https://docs.microsoft.com/en-us/microsoft-365/admin/security-and-compliance/secure-your-business-data?view=o365-worldwide#encryption • When sending from University hosted email account to external email account (from @ox.ac.uk to @xx.xx.xx), confidential attachments should be encrypted and password protected at a document level. Passwords for protected email attachments must never be sent in the same email as the attachment and should be communicated via another mechanism such as by separate email, Team message, SMS text message or phone. • Do not email confidential information to individual's 'personal' (non-University) email accounts (e.g. Gmail / Hotmail etc.) unless permission has been granted by the Bursar or data owner to use that address.
Telephony	• No restrictions.	• No restrictions.	• Telephone systems do not always offer a high level of security unless both the voice of the recipient and the telephone number dialed is known to you. • In receiving a call, anyone can pretend to be any number when dialing. Do not trust the number identified by caller ID on a received call. No-one is required to enter a password to authenticate themselves when making a traditional phone call – Therefore assume any received caller could be anyone until you have authenticated them. Consider an alternative method of authenticated voice communication, such as MS Teams for the call.
Disposal	• No restrictions.	• Use bins or shredders located in your building. • Ensure all copies of information are erased when no longer needed or according to your data retention policy. Remember to empty the trash bin. • If hardware is to be disposed of, contact the College IT team for secure destruction computer.office@bnc.ox.ac.uk .	• Use confidential waste bins or shredders located in your building. • Ensure all copies of information are erased when no longer needed or according to your data retention policy. Remember to empty the trash bin. • If hardware is to be disposed of, contact your local IT support for secure destruction computer.office@bnc.ox.ac.uk .