Brasenose College Information Classification and Handling Scheme v1.2 (May 2018)

Data Breach Rules

The College has a Data Breach Policy – It is 'Annex One' of the College's Information Security Policy located with all other staff polices here: https://staff.bnc.ox.ac.uk/policies/

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

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.

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 Manager or Infrastructure Officer. Failure to declare a data breach may result in disciplinary action.

Help Encrypting and Sending Documents Securely

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

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

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

Common Data Definitions

Brasenose College data (information) has been classified according to the following scheme. The following definitions may help in understanding terms mentioned in it:

Public data is information that can be freely used, reused and redistributed by anyone with no existing local, national or international legal restrictions on access or usage.

Personal Data is 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 data is personal data 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

Confidential Data is any sensitive data about the College (as opposed to individuals) that the college does not make public.

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

<table>
<tr><th>Classification Level</th><th colspan="2">Information</th><th>Rationale</th></tr>
<tr><td rowspan="2">Highly Protected</td><td>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)</td><td>Development and Fundraising
Special Category Personal Data relating to alumni and donors
Mass (>100 records) Personal Data relating to alumni and donors
Major Donations</td><td rowspan="2">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</td></tr>
<tr><td>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</td><td>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</td></tr>
<tr><td rowspan="2">Protected (Default)</td><td>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</td><td>Development and Fundraising
Any Personal data relating to alumni and donors.
Project research and analysis
Gift administration and donations</td><td rowspan="2">Unauthorised disclosure may result in:
Financial harm
Reputational damage
Regulatory action
Distress to personnel
Impact on business systems/processes</td></tr>
<tr><td>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</td><td>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</td></tr>
<tr><td>Public</td><td colspan="2">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</td><td>Unauthorised disclosure causes no harm
Information likely already in the public domain
Information is routinely published.</td></tr>
</table>

Information Handling Rules

Departments are responsible for the implementation of the Information Handling Rules per each classification level presented below.

Store, Process, Share …	Highly Protected	Protected	Public
Where	• College/University premises, ICT Infrastructure or approved third parties as defined in ISP • College issued/controlled devices only	• College/University premises, ICT Infrastructure or approved third parties as defined in ISP • Can be transported in encrypted form with Bursar's permission • Can be accessed on personal devices that satisfy College ISP security requirements	• Anywhere
How	• Approved methods only (see below) • High levels of physical security with monitored access • 'Off-Site' usage must be explicitly authorised by the Bursar. • Minimal number of copies permitted with full audit trail • 2-factor authentication for remote access • Explicitly approved third parties with appropriate contractual agreements and TPSA. • Strict policies and procedures for secure disposal/deletion • All data sharing must be explicitly authorised and files encrypted using appropriate password protection before being sent • Passwords for decrypting documents are sent via alternative means • Physical copies kept in locked drawers, filing cabinets or equivalent • Physical copies only sent via recorded delivery or courier • In accordance with appropriate GDPR retention schedule	• In accordance with baseline security standards as per College's ISP • Secured (e.g. in a locked cabinet) when out of the office • Remote access permitted • Contractual agreements for third party access as per College's Supplier ISP • In accordance with appropriate retention schedule	• Any method • In accordance with appropriate retention schedule
Who	• Tightly restricted groups of authorised persons only • Approved and assured third parties only	• Authorised personnel (including third parties) only	• Anyone

User Practices

To comply with the Information Handling Rules users must adhere to the following practices.

	Highly Protected	Protected	Public
Using email	Double-check recipient address Use blind copy (bcc) when mailing large numbers of recipients Encrypt attachments (See Staff Guides) with Password or encrypt the email. Share passwords separately via trusted means.	Double-check recipient address Use blind copy (bcc) when mailing large numbers of recipients Encrypt attachments (See Staff Guides) with Password or encrypt the email. Share passwords separately via trusted means.	Double-check recipient address
File transfer	Internal College or University tools permitted (e.g. SharePoint or OxFile). Encrypt files (e.g. Microsoft Encrypt with Password or 7-zip) and share passwords separately via trusted means	Internal College or University tools permitted (e.g. SharePoint or OxFile).	Any tool permitted
Post	Permission from Bursar required Sealed envelope with sender details Sent by recorded delivery or courier University Mail Service not permitted	Sealed envelope with sender details Normal external mail and University Mail service permitted	Any method permitted
Cloud Storage	University OneDrive storage allowed Explicitly authorised providers according to College ISP and that provide adequate security assurances	University OneDrive storage allowed Any other approved College 3rd Party Provider (Google Drive & iCloud)	Any tool permitted
Paper Storage	Locked drawers, filing cabinets or equivalent in restricted-access College premises.	Desks and offices in restricted-access College premises Locked draws, filing cabinets or equivalent in unrestricted-access College premises or off site.	Anywhere
Networked Storage	Within restricted-access drives/folders. Encrypt files with Passwords Share passwords separately via trusted means	Within restricted-access drives/folders. Encrypt files with Passwords	No restrictions
Portable storage	Permission from Bursar required Encrypt either specific files or the whole device. Share passwords separately via trusted means Kept in locked drawers, filing cabinets or equivalent when not in use	Permission from Bursar required Encrypt either specific files or the whole device.	No restrictions
College Managed Devices	Permitted	Permitted	Permitted
Personally Managed Devices	Only via Remote Access	Only via Remote Access	Permitted