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 policies 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>
<thead>
<tr>
<th>Classification Level</th>
<th>Information</th>
<th>Rationale</th>
</tr>
</thead>
<tbody>
<tr>
<td>Highly Protected</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| 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 |
| Operations:          |             |           |
|                      | • 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 | Risks to the safety or wellbeing of staff, students, alumni, donors, applicants or visitors |
| Protected (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 | |
| Operations:          |             |           |
|                      | • 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 | Unauthorised disclosure may result in:  
• Financial harm  
• Reputational damage  
• Regulatory action  
• Distress to personnel  
• Impact on business systems/processes |
| 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.
# Information Handling Rules

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

<table>
<thead>
<tr>
<th></th>
<th>Highly Protected</th>
<th>Protected</th>
<th>Public</th>
</tr>
</thead>
</table>
| **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              | • Anywhere     |
|                      | • College/University premises, ICT Infrastructure or approved third parties as defined in ISP  
                      | • College issued/controlled devices only                                          | • Can be accessed on personal devices that satisfy College ISP security requirements  
                      |                                    | • Can be transported in encrypted form with Bursar’s permission              |                |
|                      | • 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                                     | • 2-factor authentication for remote access                               |                |
|                      | • Explicitly approved third parties with appropriate contractual agreements and TPSA. | • Explicitly approved third parties with appropriate contractual agreements and TPSA. |                |
|                      | • Strict policies and procedures for secure disposal/deletion                    | • Secured (e.g. in a locked cabinet) when out of the office               |                |
|                      | • All data sharing must be explicitly authorised and files encrypted using appropriate password protection before being sent | • Remote access permitted                                                 |                |
|                      | • Passwords for decrypting documents are sent via alternative means             | • Contractual agreements for third party access as per College’s Supplier ISP |                |
|                      | • Physical copies kept in locked drawers, filing cabinets or equivalent         | • In accordance with appropriate retention schedule                        |                |
|                      | • Physical copies only sent via recorded delivery or courier                     |                                                                             |                |
|                      | • In accordance with appropriate GDPR retention schedule                        |                                                                             |                |
|                      |                                                                             |                                                                             |                |
| **Who**              | • Tightly restricted groups of authorised persons only                           | • Authorised personnel (including third parties) only                      | • Anyone       |
|                      | • Approved and assured third parties only                                      |                                                                             |                |
**User Practices**

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

<table>
<thead>
<tr>
<th></th>
<th>Highly Protected</th>
<th>Protected</th>
<th>Public</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Using email</strong></td>
<td>Double-check recipient address</td>
<td>Double-check recipient address</td>
<td>Double-check recipient address</td>
</tr>
<tr>
<td></td>
<td>Use blind copy (bcc) when mailing large numbers of recipients</td>
<td>Use blind copy (bcc) when mailing large numbers of recipients</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Encrypt attachments (See Staff Guides) with Password or encrypt the email. Share passwords separately via trusted means.</td>
<td>Encrypt attachments (See Staff Guides) with Password or encrypt the email. Share passwords separately via trusted means.</td>
<td></td>
</tr>
<tr>
<td><strong>File transfer</strong></td>
<td>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.</td>
<td>Internal College or University tools permitted (e.g. SharePoint or OxFile).</td>
<td>Any tool permitted</td>
</tr>
<tr>
<td><strong>Post</strong></td>
<td>Permission from Bursar required Sealed envelope with sender details Sent by recorded delivery or courier</td>
<td>Normal external mail and University Mail service permitted</td>
<td>Any method permitted</td>
</tr>
<tr>
<td><strong>Cloud Storage</strong></td>
<td>University OneDrive storage allowed Explicitly authorised providers according to College ISP and that provide adequate security assurances</td>
<td>University OneDrive storage allowed Any other approved College 3rd Party Provider (Google Drive &amp; iCloud)</td>
<td>Any tool permitted</td>
</tr>
<tr>
<td><strong>Paper Storage</strong></td>
<td>Locked drawers, filing cabinets or equivalent in restricted-access College premises.</td>
<td>Desks and offices in restricted-access College premises Locked draws, filing cabinets or equivalent in unrestricted-access College premises or off site.</td>
<td>Anywhere</td>
</tr>
<tr>
<td><strong>Networked Storage</strong></td>
<td>Within restricted-access drives/folders. Encrypt files with Passwords Share passwords separately via trusted means</td>
<td>Within restricted-access drives/folders. Encrypt files with Passwords</td>
<td>No restrictions</td>
</tr>
<tr>
<td><strong>Portable storage</strong></td>
<td>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</td>
<td>Permission from Bursar required Encrypt either specific files or the whole device.</td>
<td>No restrictions</td>
</tr>
<tr>
<td><strong>College Managed Devices</strong></td>
<td>Permitted</td>
<td>Permitted</td>
<td>Permitted</td>
</tr>
<tr>
<td><strong>Personally Managed Devices</strong></td>
<td>Only via Remote Access</td>
<td>Only via Remote Access</td>
<td>Permitted</td>
</tr>
</tbody>
</table>