|  |  |
| --- | --- |
| **Type of document** | Policy |
| **Title** | Working With Student Records |
| **Author** | Head of Student Records |
| **Document status** | Draft |
| **Next review date** | December 2022 |
| **Security level** | Public |
| **Audience** | Student Registry |

****

Contents

[Working With Student Records 2](#_Toc95290531)

[1. Introduction 2](#_Toc95290532)

[2. Policy 2](#_Toc95290533)

[a. Desks 2](#_Toc95290534)

[b. Working from home 2](#_Toc95290535)

[c. Digital filing 2](#_Toc95290536)

[d. Paper filing 3](#_Toc95290537)

[e. Emails 3](#_Toc95290538)

[f. Sharing Student Information 4](#_Toc95290539)

[g. Microsoft Teams 5](#_Toc95290540)

[h. Third Party collaboration tools 5](#_Toc95290541)

[i. Reporting Data Breaches 5](#_Toc95290542)

# Working With Student Records

# Introduction

This document is intended to provide a summary of best practice when working with student records. Following the guidelines within this document will assist Student Registry colleagues in being compliant with Data Protection legislation and the reporting of data breaches.

This document can also be shared with colleagues across the collegiate University to demonstrate best practice which other areas may also wish to adopt.

# Policy

The following points constitute Student Registry’s policy on working with student records.

# Desks

* Out of office hours, documents with identifiable student data; name, any other personal details and student number, will not be kept on desks or in desk filing trays.
* Documents currently being dealt with should be locked away overnight, either in lockable desk drawers, or a shared lockable cupboard, with responsibility for locking of desk drawers on the individual, and locking of the shared cupboard on a defined individual. Keys should be kept in a secure place with no identifiable labelling as to the drawers’/cupboard’s location.
* Staff will be responsible for collecting documents from the printers to ensure that no documents with student data are left uncollected.
* Computer screens should be locked whenever a desk is unattended (Ctrl+Alt+Delete “Lock this computer” OR Win+L).

# Working from home

* Use VPN / Remote Desktop to securely access Oxford’s network and services. Further information and guidance about how to configure this is available on the [IT Services website](https://www.it.ox.ac.uk/work-remotely).
* Do not save files to your personal computer – only save to University maintained drives
* You should still lock your computer when away from your desk (Ctrl+Alt+Delete “Lock this computer” OR Win+L).
* You should avoid printing paper documents wherever possible. If these are vital to your work you should follow the steps in [section 2.d](#_Paper_filing) below, in particular ensuring paper documents are securely destroyed when no longer needed.

# Digital filing

Digital folders on shared drives should only be accessible to those who have a need to see them. Access to shared folders should be managed centrally via IT Services, with restricted access granted by a small number of key authorisers. Access to shared drives should be reviewed regularly. Access can be maintained at <https://help.it.ox.ac.uk/connect/requests>

Agreed protocols should be in place for filing of documents containing student data, to ensure that they are:

* Only stored on secure shared access drives
* Easy to access when required
* Retained in accordance with the [Student Record Retention Policy](https://compliance.admin.ox.ac.uk/retention-schedules) i.e. not kept for longer than necessary

# Paper filing

Where possible, paper documents should be scanned and stored in digital format. Originals should then be securely destroyed. Effort should be made to reduce the amount of paper used and stored on an ongoing basis.

Where it is not possible to scan and store digitally, paper documents should be:

* Stored in a locked / restricted access area
* Agreed protocols should be in place for filing / cataloguing documents
* Easy to access when required
* Retained in accordance with [the Student Record Retention Policy](https://compliance.admin.ox.ac.uk/retention-schedules) i.e. not kept for longer than necessary
* Once no longer required, documents should be securely destroyed

# Emails

* Any email from, or relating to, a student which is received in a personal email account should be moved to an appropriate shared email account’s inbox.
* When emailing, think carefully about any information you put down in writing – would you be happy for the person concerned to read it? All information about a person is potentially disclosable to them, via a Subject Access Request.
* If you are forwarding or replying all to an email trail – carefully consider the recipients and whether everything in the included trail is appropriate to be shared with all parties.
* Where an email about/from a student leads to a wider discussion of policy or practice, this should be raised in a separate email with all student personal data removed and any discussion of the specific case kept anonymous.
* If emailing groups of people about sensitive information, think carefully about whether you should use BCC rather than CC, or set up email groups / [maillists](https://web.maillist.ox.ac.uk/admin/help). If using a mailing list, consider whether all subscribers on that list have a need to see the information. Regularly update and maintain maillist subscribers.
* You may wish to add a delay to your email send in Outlook – which would allow you to recall emails before they have been sent if they were sent in error. See this [guide to adding an email delay](https://www.ablebits.com/office-addins-blog/2019/09/25/schedule-email-delay-delivery-outlook/).
* Further guidance around email management is available on the [Compliance website](https://compliance.admin.ox.ac.uk/email-management).
* If you receive an email containing information which should not have been sent to you, it is your responsibility to demonstrate best practice by taking the following action;
  + If the underlying email trail contains sensitive information which you have no need to see, respond to the sender, deleting the sensitive information and replacing it with *\*\*This information has been deleted for Data Protection purposes\*\**, and in your email explain to them why you have done this, for example *“I have deleted the below information since it contains sensitive details about a student’s medical history which I have no need to see”*. Also cc. [data.breach@admin.ox.ac.uk](mailto:data.breach@admin.ox.ac.uk) into your response so that the Compliance Team can monitor the number of these occurrences, and forward them the original email so they can see the full details of the breach. Once you have done this, delete the original email.
  + If you are unsure of what should be redacted, or whether or not to redact something, consult your line manager.
  + If the email contains an attachment or other data which you feel has been sent to you in error, or which has not been sent via a secure means, respond to the sender and highlight this, suggesting that in future they use a different method of sharing information, as detailed in the below “sharing student information” section. It may be appropriate to share this document with them to highlight best practice. Also cc. [data.breach@admin.ox.ac.uk](mailto:data.breach@admin.ox.ac.uk) into your response so that the Compliance Team can monitor the number of these occurrences, and forward them the original email so they can see the full details of the breach. Once you have done this, delete the original email.
* If you have accidentally sent an email containing student data to the wrong recipient, report this to Information Compliance at [data.breach@admin.ox.ac.uk](mailto:data.breach@admin.ox.ac.uk) who will advise you on the appropriate action to take. You should also notify your line manager (see Reporting Data Breaches below).

# Sharing Student Information

Reports or other documents containing sensitive student data\*, e.g. spreadsheets, must be transmitted securely, by the following method (in order of preference):

* Stored on a secure shared access drive, with a hyperlink sent to shared location. You should consider who has access to the shared drive in question to determine if this is an appropriate location to store it. For example sharing via your team’s G drive might be appropriate while sharing via the P drive would not be.
* Shared via SharePoint/OneDrive/Nexus 365/Teams through the production of a secure link, with access given only to those who need to see it, requiring the recipient to access the file through their Single Sign On. See how to guide available [here](file:///\\connect.ox.ac.uk\ADMN\STUDENT\Registry%20General%20-%20All%20Staff\Working%20with%20Student%20Records\Sharing%20Files%20via%20SharePoint.docx).
* Password-protected when sent by email, if the above alternatives are not feasible.

Any files produced for sharing student data should be deleted once they no longer serve a purpose, in accordance with [the Student Record Retention Policy](https://compliance.admin.ox.ac.uk/retention-schedules).

If you are using SharePoint/OneDrive/Nexus 365/Teams to transfer student data to another person (i.e. you will not be using the report/dataset yourself) you should agree with the recipient that the document will be deleted after a set period (e.g. two weeks). If they wish to retain the document longer than this, or to share it with a wider group, they should create a local copy and take responsibility for sharing this securely themselves.

You should not use [OxFile](https://help.it.ox.ac.uk/services/oxfile/faq) to share student data; this is not a secure file sharing service:

* links generated do not require the use of Single Sign On to access files
* in the vast majority of cases emails sent to users containing the URL to access a folder are transferred over the internet with no encryption
* There is nothing to stop people forwarding an email link onto others who could then also access the file if it is not password protected

Full guidance on how to classify and handle University data securely is available on the [Information Security website](https://www.infosec.ox.ac.uk/handling-information#collapse1721931).

\*sensitive student data includes (but is not limited to): ethnicity, disability, religious belief, sexual orientation, medical background. Non-sensitive student data includes (but is not limited to): student number, name, course, college. Although not formally classified as sensitive, some data such as results and contact details should be treated carefully and in a similar way to sensitive data. If you are uncertain of whether the data you wish to share should be classified as sensitive, contact your line manager.

# Microsoft Teams

If you are using Microsoft Teams to communicate with students, the following should be taken into consideration:

* Meetings with students should not be recorded
* Take care to ensure that Teams meetings are held in a suitable place that ensures confidentiality and privacy (this includes what the student could potentially see in the background – blur or use a generic Teams background).
* If it is known in advance that that the meeting is likely to be of a sensitive or confidential nature a private meeting room/space should be booked to ensure no interruptions
* Any notes etc. written into the chat should be deleted immediately following the meeting

# Third Party collaboration tools

If you are using a third party collaboration tool such as Padlet, Trello or Miro – you should take care not to add any personal data to these sites. Even if boards are not publically available, the providers of these sites may not be on the University’s list of approved third party software. These sites can be used for generic collaboration but should not be used for any confidential or sensitive data sharing.

# Reporting Data Breaches

The University has a legal duty to report any serious breach of personal data to the Information Commissioner's Office (ICO) within 72 hours of becoming aware of it.  If the University fails to report the breach within this given timeframe it could be liable for a significant financial penalty (4% of global annual turnover or €20 million, whichever is higher).  Where there is any breach of personal data it is essential therefore to take prompt action and immediately report the breach to the Information Compliance Team ([data.breach@admin.ox.ac.uk](file:///\\connect.ox.ac.uk\ADMN\STUDENT\Registry%20General%20-%20All%20Staff\Working%20with%20Student%20Records\data.breach@admin.ox.ac.uk)) and also notify your line manager and/or head of section. The Information Compliance Team will provide guidance and support, and decide whether the breach needs to be reported to the ICO. Further information can be found on the [Compliance website](https://compliance.admin.ox.ac.uk/reporting-data-breaches).