

Guidance on Managing Downloaded Copies of Student Data

1. Purpose of this guidance

Staff should avoid downloading personal data from MySIS/SITS (or, indeed other systems of record) unless there is a clear, necessary and approved business reason to do so. Where data is downloaded, it must be managed in line with QMUL's Records Retention Policy and Schedule, information security requirements and data protection obligations.

This guidance explains why unmanaged local copies of student data create risk, and what staff should do instead.

2. The problem and why it matters

SITS is the system of record for core student records. Problems arise when staff download data from that system and store copies in places such as:

- personal or shared drives, including OneDrive, and Teams or SharePoint folders with unclear ownership;
- local device folders;
- email inboxes and attachments;
- USB drives or other removable media.

These copies can quickly become unmanaged records. They may be forgotten, duplicated, out of date, accessible to the wrong people, or retained longer than permitted by the Records Retention Schedule, which applies to information regardless of format or storage medium.

QMUL's records management guidance states that records must be accurate, reliable, available and not retained for longer than necessary, and that all staff are responsible for maintaining complete and accurate records, following the Records Retention Policy, Schedule and procedures, and filing records correctly.

• **Over-retention creates compliance risk**

Keeping downloaded student data 'just in case' is not acceptable. Personal data must not be kept longer than necessary, and organisations must be able to justify how long they retain it. The Records Retention Schedule exists to standardise retention and disposal across the University. Unnecessary retention creates waste, cost and risk, including risks when responding to data protection and Freedom of Information requests. In addition, every extra copy of student data increases the risk of unauthorised access, accidental disclosure, loss, or misuse. Data protection principles require personal data to be handled securely and protected against unauthorised or unlawful processing, access, loss, destruction or damage.

• **Downloaded copies can undermine the official record**

If staff maintain separate spreadsheets or extracts, there is a risk that decisions are made using data that is incomplete, outdated or inconsistent with the central student record. This can affect students, staff, reporting, auditability and institutional accountability.

- **Downloaded data may contain more information than is needed**

Staff should only use the minimum amount of personal data required for the task. The data minimisation principle states that personal data must be adequate, relevant and limited to what is necessary. Everyone must periodically review data held and delete anything no longer needed.

3. What staff should consider

- **Before downloading student data ask:**

- i. Is the download genuinely *necessary*?
If the task can be completed in MySIS, do not download the data.
- ii. What is the specific purpose?
Do not extract data for vague, speculative or 'just in case' reasons.
- iii. What is the minimum data needed?
Only extract the fields and records required for the task.
- iv. Where will the file be stored?
It must be stored in an approved QMUL location with appropriate access controls.
- v. Who needs access?
Access should be limited to staff who need the data for the stated purpose.
- vi. When will it be deleted?
The file must have a clear retention period aligned with the Records Retention Schedule.

- **Where a download *is* necessary, staff must follow these rules:**

Do

- Use the central student records system as the primary and authoritative source of information.
- Download only the minimum information required.
- Store the extract only in an approved QMUL-managed location.
- Label the file clearly, including purpose, owner and review/deletion date.
- Restrict access to only those who need it.
- Delete the extract as soon as the business purpose has been met, unless a defined retention requirement applies.

Do not

- Keep local copies indefinitely.
- Store student data in personal drives, unmanaged folders or mailboxes.
- Create "shadow databases" or unofficial spreadsheets that duplicate the student record.
- Reuse downloaded data for a new purpose without checking whether that use is appropriate.
- Share extracts by email where a secure shared location or system access would be more appropriate.
- Retain downloaded data simply because it might be useful in future.
- Assume that because data came from the central system it can be stored anywhere.

4. Practical examples

Example	Scenario	Correct approach	Incorrect approach
1: One-off reporting task	A staff member downloads some student data to prepare a one-off report	Download only the required fields, store the file in an approved restricted-access location, use it for the report, and delete it once the report has been completed and checked	Keep the data in a personal folder for future reference
2: Local tracking spreadsheet	A team maintains a spreadsheet of student information because it is more convenient than checking the student records system	Review whether the tracking activity can be carried out in SITS or another approved system. If a local tracker is genuinely required, agree ownership, access controls, retention, review dates and deletion arrangements	Allow multiple versions of the spreadsheet to develop across SharePoint folders, Teams channels and email attachments
3: Annual exercise	A team downloads student data each year for an annual process	Create a documented process setting out what data is downloaded, why, where it is stored, who owns it, who has access, and when it is deleted after the annual exercise	Keep each year's downloaded files indefinitely in a legacy folder

5. More information

- Records Retention Schedule: <https://www.qmul.ac.uk/governance-and-legal-services/governance/information-governance/records-management/records-retention-schedule/>
- Information Classification Policy: <https://www.qmul.ac.uk/its/media/its/documents/governance/sops/Information-Classification-Policy.pdf>