

Evidence Handling Checklist

Reporting an incident and evidence

If you witness an incident, come across evidence relating to an incident, or are asked to gather or retain evidence:

- Do not alter or amend the evidence in any way.
- If collecting the evidence from the site will alter or damage the evidence, then take photographs of the original location before collection.
- Preserve any documentation in its original form (e.g., do not edit, redact, or convert formats).
- If you are directly involved in the incident, or your involvement in collection or storage of evidence is likely to give rise to a conflict of interest, ask a colleague to handle and store the evidence on your behalf.
- Hand the evidence to the investigating office as soon as possible, along with a short statement confirming how and when you obtained it, and confirmation that the evidence has not been changed or tampered with.
- If you need to share a copy of physical evidence via a digital communication for expediency of reporting, the original physical evidence should be retained unaltered and handed to the investigating office as soon as practicable. Digital copies in these circumstances should be relied on for initial reporting and triage only.

Once handed over, the investigating office will take responsibility for secure storage, and any necessary processing in line with QMUL procedures.

Before Investigation

- Assign a clear and descriptive document title for each piece of digital evidence.
- Log receipt details for any physical evidence: date, source, and description in the Decision Log.

Redaction

- Remove personal or sensitive information not relevant to the case before sharing files.
- Verify that redaction does not alter meaning or context.

- Always retain unredacted original versions.

Storage

- Use QMUL-approved systems only: secure SharePoint (preferred) or approved other system eg AskQM.
- Do not store on personal drives or unapproved cloud services.
- Create clearly labelled folders for Originals and Redacted/modified versions.
- Apply consistent file naming conventions (e.g., Original_[CaseID], Redacted_[CaseID]).

Modifications

- Record any changes (digitally enhanced images, file format changes etc) in Decision Log: date, reason for modification, method/software used, person responsible.
- Always retain both original and modified versions.

Sharing Evidence

- Do not grant access to original secure storage.
- Share via secure share link (copy only) or password-protected email attachments.
- Send password via separate communication.

Data Protection

- Minimise unnecessary data storage beyond QMUL retention schedule requirements.
- Share only with those who have a legitimate need-to-know.

Translation

- Use professional translation for sensitive or crucial evidence.
- If machine translation is used: ensure no personal data is shared with third-party, record the program/software used, allow parties to comment on the translations if no independent professional review was conducted.
- If translation provided by party to the case: request original unaltered version of the evidence and arrange independent verification and translation.

Audit Trail

- Record all decisions and actions in the case Decision Log.

- For physical evidence: maintain chain of custody records, and specify the storage location in digital case notes.

Disposal

- Dispose securely after retention period (shredding or secure deletion).