



Recording & File Transfer

Recording safeguarding concerns is vital to the effective safeguarding of children/young people.

Safeguarding records are kept for many years & must be fully understood even after they have left your education setting.

All records should:

- Be factual, evidenced, concise, complete, accurate and objective
- Include full names, dates, role/relationship to student
- Be securely stored (physically or electronically)

A safeguarding file should be set up for each student when a safeguarding concern is identified.

The file should be in date order & have a:

- Front sheet with basic details of the student
- Chronology of the contents
- Record of all discussions and meetings relating to the student and their family
- Copy of any other documents e.g. assessments, minutes of conferences, core groups etc.
- Letter of confirmation if a student is made or is no longer, subject to a Child Protection Plan

Each file record should include:

- Date and time of:
 - writing the record
 - when an incident and/or concern began
- Details of your concerns, what gave rise to them, and any discussions about this
- All action you have taken
- The extent and nature of any involvement by other professionals, and their full details

Storage:

- All individual hardcopy safeguarding files should be stored in a locked cabinet
- Access to child protection information is only via the Head Teacher, Designated Safeguarding Lead or Deputy (DSL or DSD)
- Early intervention information should be securely archived until 25 years after last action
- Child protection information should be securely archived until the subject person reaches 85 years old

E-storage:

- **Always seek specialist advice**
- Encryption of files is strongly advised
- If using password protection, ensure the Head, DSL & DSD all have the password, **but do not share it with others**
- Passwords should use a standard formula that is **strong** and **memorable**
- If using 'restricted access' folders, this can be over-ridden by your IT technicians
- Tightly manage access & permissions, disable promptly when staff leave or change role
- Archived e-files may have digital continuity & password protection limitations
- If using [on-line storage](#) ensure that it is secure, subject to UK law and meets all data protection requirements & handling standards

Sharing information:

Appropriate levels of information **must** be shared appropriately by the DSL/D or Head with staff and other settings so they can respond effectively to the child or young person's needs.

Transferring files:

- All safeguarding files must be securely transferred **immediately**, in person or by recorded delivery, to the DSL/D of the new setting (including 16+ provisions) and a receipt obtained
- You may need to keep copies of significant documents for future use
- If the new establishment is out of city consider if a copy of the whole file should be retained
- Any copying of documents must be subject to personal & sensitive [data processing conditions](#)
- E-transfers **must** be secure, e.g. encrypted, for both the sending and receiving IT systems
- Documents may be copied to the file of another child **only** if appropriate
- All DSL's receiving files must **not** dispose of any of the original contents