

# Recording & File Transfer



**Documenting safeguarding concerns is vital to the effective safeguarding of children and young people.**

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

## All documents 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 actions 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 '[cloud software 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 by the DSL/D or Head with staff and other education settings. This must be done in a timely manner 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)
- Always get a receipt for any file that is passed to another setting
- You may need to keep copies of significant documents for future use, e.g. documents that originated from your agency
- 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

**Please remember: All records (on paper or electronic) must be professionally written and respectful towards the child, their family and other involved professionals. People may request access to these records or they may be used for other formal purposes, e.g. court or other reports.**



If a parent requests access to their child's safeguarding file, this is a 'Subject Access Request' and you **MUST** seek HR & legal advice from your organisation. General guidance below:

### Advice in relation to the release of a safeguarding chronology or file to e.g. a Parent

The request for safeguarding information is effectively a 'Subject Access Request (SAR)' and the Information Commissioners Office website contains useful information about the requirements to release information: <https://ico.org.uk/for-organisations/guide-to-data-protection/principle-6-rights/subject-access-request/>

### Subject Access Requests

The Data Protection Act places a duty on a data controller (in this case the education setting) to respond to a subject access request (request for personal data) within 40 days. The right of access to personal data belongs to the person the data is about (in this case the child). However, as the child is a minor the child's parents can be provided with the personal data if the child does not have capacity to understand it, or if the child does have capacity and gives express permission for it to be released to the parents.

This would be a judgment call for the setting to make and being mindful of any sanctions that may be imposed by the Information Commissioner's Officer for releasing personal data in breach of these principles.

### Education settings should:

- acknowledge receipt of the correspondence
- confirm that this is considered a subject access request under the Data Protection Act 1989
- explain that because the information relates to the child being subject to or at risk of child abuse you are legally permitted to refuse to release the information to parents

### In most cases, subject access requests would be dealt with in the following way:

- Send a holding response to acknowledge receipt of the correspondence confirming that a full response will be provided within 40 days of receipt of the written request for personal data
- Confirm to parents that not all of the information requested is retained by the setting and that you will confirm which of their questions need to be directed to the Local Authority or other agencies
- You can request that parents pay a fee of £10 (see [www.legislation.gov.uk/ukxi/2000/191/made](http://www.legislation.gov.uk/ukxi/2000/191/made)) to release the information and advise that the clock stops running until the fee has been paid

The following information **must not be released** to the pupil or parent:

- correspondence which is legally privileged
- examination marks before they are officially released
- examination scripts
- anything relating to adoption
- anything relating to court proceedings about the child
- anything relating to the child being subject to or at risk of child abuse
- anything that would be likely to cause serious harm to the physical or mental health or condition of the child or any other person

The school is prevented from disclosing information of this nature by virtue of the [Data Protection \(Subject Access Modification\) \(Education\) Order 2000 \(SI 2000/414\)](#)

If you require any assistance in preparing information for release to pupils or parents following receipt of a Subject Access Request, please make contact as soon as possible and arrangements can be made for a member of the Team to visit the education setting to provide practical advice:

**The Governance Team, Legal Services, Sheffield City Council, tel. 273 6784 or email [legalservicesgovernance@sheffield.gov.uk](mailto:legalservicesgovernance@sheffield.gov.uk)**

Any Sheffield school or college can contact the Governance Team for advice – however there will be a charge unless they have a traded service package with Legal Services. Alternatively you can contact your organisations HR advisor.