Child Safeguarding File

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.

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 (including with Designated Safeguarding Lead/Deputy)
- 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 at least until the subject is 85 years old (currently indefinitely until further direction from the Independent Inquiry into Child Sexual Abuse)

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, check if they can be over-ridden by your IT technicians
- Tightly manage access & permissions, disable promptly when staff leave or change role
- Check that archived e-files do not have digital continuity and/or 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 relevant 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 signed for/special 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

All safeguarding files must be professionally written & respectful.
People may request access to these files or they may be used for e.g. court, case reviews, etc.
DSL/D's should regularly audit files to ensure standards are maintained.

If a parent requests access to their child's safeguarding file, this is a 'Subject Access Request' and you MUST seek Human Resources & 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-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/

Subject Access Requests

The revised legislation 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 one month. 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 the maturity/ability to understand it, or if the child does have maturity/ability 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 General Data Protection Regulation
- explain that as the information relates to the child being subject to or at risk of child abuse/ill-treatment you are lawfully permitted to refuse to release such information to parents where necessary

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 one month of receipt of the request (or up to a further two months if the request is deemed to be complex)
- Confirm to parents that not all of the information requested may be retained by the setting and that you will confirm which of their questions need to be directed to the Local Authority or other agencies
- Provided free of charge. However, a "reasonable fee" can be charged for further copies of the same information and when a request is manifestly unfounded/excessive or repetitive.

Checklists:

Preparing for subject access requests	**Complying with subject access requests**
☐ We can recognise a subject access request and we understand when the right of access applies. ☐ We have a policy for how to record requests we receive verbally. ☐ We understand when we can refuse a request and are aware of the information we need to provide to individuals when we do so. ☐ We understand the nature of the supplementary information we need to provide in response to a subject access request.	☐ We have processes in place to ensure that we respond to a subject access request without undue delay and within one month of receipt. ☐ We are aware of the circumstances when we can extend the time limit to respond to a request. ☐ We understand that there is a particular emphasis on using clear and plain language if we are disclosing information to a child. ☐ We understand what we need to consider if a request includes information about others.

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 (see details below) and arrangements can be made for a member of the Governance Team to visit the education setting to provide practical advice:

The Governance Team, Legal Services, Sheffield City Council, tel. 0114 273 6784 or Email: legalservicesgovernance@sheffield.gov.uk

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