Secure Storage, Subject Access Requests and Recording Guidelines

Introduction:

- Documenting safeguarding concerns effectively is vital to the effective safeguarding of children and young people.
- A safeguarding file should be set up for each student when a safeguarding concern is identified.
- Safeguarding records are retained for significant time periods and therefore must be fully understood even after they have left your education setting.

Key recording principles:

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)

The file should be in date order and have a:

- Front sheet with basic details of the student (e-storage systems generate this)
- Chronology of the contents
- Record of all discussions (including phone calls) and meetings relating to the student and their family
- Copy of any other relevant documents e.g., assessments, minutes of conferences, core groups etc.

Each file record should include:

- Date and time of writing the record and when an incident and/or concern began (e-storage systems have time stamps)
- Clear and comprehensive summary of concern
- How the concern was followed up and resolved
- Any action taken, decisions reached and outcome.
- All discussions and decisions made (including with Designated Safeguarding Lead/Deputy)
- It is **essential** that the rationales behind decisions are recorded.
- The extent and nature of any involvement by other professionals, and their full details

Storage:

E-Storage systems

Many education settings choose to purchase an e-storage system for safeguarding files.
There is no expectation that e-storage systems are used.
The choice to use an e-storage system is for an education setting to make.
Any support around functionality of an e-storage system would need to be sought from the provider.

Top tips for e-storage systems:

- Know about the level of encryption and type of authentication needed to keep information secure.
- Carefully manage who has access to what information (permissions)
- Know how to disable permissions/remove access when someone leaves or needs access withdrawn.
- Think carefully about who is receiving notifications.
- Manage ‘tags’ very carefully so information can be filtered effectively.

Secure Storage, Subject Access Requests and Recording Guidelines

- Understand the archiving protocols for the e-storage system. It is the responsibility of the setting to ensure that the correct information retention periods are adhered to.

Clouds, shared folders and drives:

- If using internal IT systems for file storage ensure 'restricted access' folders and drives are password protected and that the correct people have access (e.g., Head, DSL/Ds)
- Use best practice for setting passwords that cannot be broken/guessed.
- Ensure password protected and restricted access drives and folders cannot be overridden by IT technicians.
- Check archived e-files don't have digital continuity or password protection limitations and that retention is set appropriately.
- If using cloud software storage ensure it is secure, subject to UK law and meets all data protection requirements and handling standards.

Paper files:

If paper storage is used for safeguarding files then;

- 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)

Retention periods and transfer of safeguarding information between settings:

Retention periods;

- Early Help information retained should be securely archived until 25 years after last action.
- Child protection information retained should be securely archived at least until the subject is 85 years old.
- If using an e-storage system please check the retention periods are set correctly.

- **Transfer;**
- When a child leaves a setting their safeguarding information needs to be transferred from the setting to the new setting **securely** at both ends of the transfer. This may take the form of an e-transfer or an in-person/signed for transfer.
- Transfers must be prompt.
- The DSL receiving a safeguarding file must not dispose of any of the original contents.
- Keep a clear transfer record for files transferred/files received.
- Copies of safeguarding files should not be retained by the setting transferring the information unless there is a specific reason for doing so;
- 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. If the decision is to retain a copy then mark this clearly in the transfer record. Best practice would be to have written confirmation from the out of city setting that the safeguarding file has been received. This confirmation must be kept with the transfer record. This would mean that the copied file can be disposed of by the transferring setting in Sheffield.
- Please be aware that any copying of documents must be subject to personal and sensitive **data processing conditions** and current retention/archiving requirements
- If the education setting is the last setting that will be attended by a young person (e.g., a secondary school or 6th Form College) then the retention periods need to be understood and strictly adhered to for when that information must be securely disposed of.

Secure Storage, Subject Access Requests and Recording Guidelines

Information sharing:

- Appropriate 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 to respond effectively to the child or young person's needs.
- Your setting should have a process for sharing information about a pupil after they have left.

Subject Access Requests:

- If a parent requests access to their child's safeguarding file, this is a 'Subject Access Request' (SAR), and you must seek Human Resources and legal advice from your organisation.
- The Information Commissioners Office, Rights of Access webpage can advise you about the requirements to release information.

Overview;

- The duty is on a data controller (e.g., the education setting) to respond to a request for personal data (SAR) within one month.
- The right of access to personal data belongs to the person the data is about (e.g., the child). However, as the child is a minor, their 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 decision 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.

If a SAR is received;

- 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 considered 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.

SAR checklist for education settings;

- ✓ We can recognise a SAR and we understand when the right of access applies.
- ✓ We have a policy for how to record SAR's we receive verbally.
- ✓ We understand when we can refuse a SAR.
- ✓ We 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 SAR.
- ✓ We have a process to ensure that we respond to a SAR without undue delay & within one month of receipt.
- ✓ We are aware of the circumstances of when we can extend the time limit to respond to a SAR.
- ✓ We understand the particular emphasis on using clear, plain language if we disclose information to a child.
- ✓ We understand what we need to consider if a SAR includes information about others

Secure Storage, Subject Access Requests and Recording Guidelines

Where to go for support with a SAR;

- If you require assistance in preparing information for release to pupils or parents following receipt of a SAR, please contact The Governance Team quickly for advice:

The Governance Team, Legal Services, Sheffield City Council

Email: legalservicesgovernance@sheffield.gov.uk

- Any Sheffield school/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.

Recording guidelines:

Key principles;

- All safeguarding files must be professionally written & respectful.
- Remember that 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.
- Secure storage in an individual file is required without exception.
- The author of the safeguarding record must be clear, including their role and relationship to the child.
- Rationale for decisions must be recorded.

Safeguarding records must be;

1. Factual
2. Evidenced
3. Concise
4. Complete
5. Accurate
6. Objective

Records must include include (where known) details of:

- The correct biographical details of the Child/young person
- Others in household
- Involved practitioners.
- Your concerns
- Any incident
- Any action taken