Safeguarding Storage and Communication Policy

This policy sets out how Gloverspiece Minifarm & School records, stores, shares, transfers and retains child safeguarding information. It supports prompt safeguarding action while restricting access to people who need the information for their role. It should be read alongside the school safeguarding and child protection policy, privacy notice, data protection procedures and retention schedule.

Policy owner	**Designated Safeguarding Lead: Jo Evans**
Safeguarding proprietor	Lynne Duffy
Reviewed	September 2026
Next review	September 2027, or sooner if guidance or systems change

1. Scope and responsibilities

This policy applies to safeguarding and child protection information held in CPOMS, paper records, secure correspondence and documents received from families, previous settings and partner agencies. It covers all pupils, including those attending alternative or off-site provision while remaining on the school roll.

The DSL is responsible for the accuracy, security and timely transfer of child protection files. A trained deputy may act on the DSL's behalf; Liam Allibone provides DSL cover on Fridays. Staff must record and report concerns promptly in accordance with the school safeguarding policy. The proprietor oversees suitable arrangements and the school's data protection lead advises on lawful processing, retention, requests and breaches.

2. Recording and access

- Record concerns on CPOMS promptly, using factual language. Separate observation, a child's account, professional opinion and historic information. Record follow-up, decisions, actions and outcomes; maintain a useful chronology and review open concerns.
- Keep child protection information in a separate, confidential file for each child, distinct from the main pupil record. CPOMS is the principal record. Any paper originals must be linked to the record and stored securely; avoid uncontrolled duplicate copies.
- Restrict full file access to the DSL and authorised deputies. The DSL may share relevant extracts with staff who need them to safeguard or support the child, including a SENCO, and must review access when roles change. Access and disclosures should be auditable.
- If CPOMS or the internet is unavailable, staff must use the school's paper concern form and give it directly to the DSL or available deputy without delay. The DSL arranges secure temporary storage and enters or attaches the record to CPOMS when access returns, retaining any original only where needed under the retention schedule.
- Store paper files in a locked cabinet with controlled keys and a sign-out log. Use secure printing, collect documents immediately, clear desks and dispose of working copies through confidential shredding. Protect electronic records through individual accounts, appropriate access controls and school-approved backups.

3. Sharing and communication

Share relevant information early when needed to identify risk, obtain help or protect a child. Consider purpose, lawful basis, necessity, accuracy and the recipient's need to know; do not let uncertainty about data protection delay urgent safeguarding action. Consent is not always required for safeguarding sharing. Record the reason, content, recipient, method and date of significant disclosures and decisions not to share. Seek advice from the DSL or data protection lead where needed.

Use a school-approved secure channel, such as encrypted email or secure transfer, for sensitive information. Verify the recipient and address before sending; use minimum necessary information in the message body, password-protect or encrypt attachments where appropriate, send passwords separately and confirm receipt. Do not use personal email or unapproved messaging. If information is misdirected, immediately follow the school's data breach procedure and inform the data protection lead and DSL.

The school must document the applicable UK GDPR Article 6 lawful basis and, where needed, Article 9 condition and Data Protection Act 2018 Schedule 1 condition in its privacy and processing records. A blanket statement that all safeguarding processing is "public task" or "vital interests" is not appropriate for every activity or recipient.

4. Transfer when a pupil leaves

When a child moves to another school or college at any stage, including an in-year move, the DSL or deputy must arrange for the complete child protection file to be transferred securely and separately from the main pupil file. This is not limited to transfer to secondary school. Transfer as soon as possible and within five days for an in-year move, or within the first five days of a new term. Verify the receiving DSL or equivalent, ensure secure transit and obtain and record confirmation of receipt.

Include a clear, structured summary of current safeguarding concerns, relevant history and context, actions, agencies involved and ongoing support or safety needs. Distinguish current risk from historic concerns. The DSL should speak to the receiving setting and share essential information before the child starts when that is needed for support or risk planning. On receipt of a file, the DSL reviews it promptly, seeks clarification of gaps and shares relevant information with key staff on a need-to-know basis.

Keep an auditable transfer record: destination, date, method, contents or file reference, sender, recipient and receipt. After confirmed transfer, do not routinely retain a duplicate child protection file or an automatically retained one-page chronology. Any retained copy or summary must have a documented safeguarding, legal or accountability purpose, a defined retention period and restricted access.

If a destination is unknown, the child is electively home educated or the child leaves education, the DSL retains the file securely pending a lawful transfer or retention review, follows children missing education and local authority notification procedures as applicable, and records attempts to identify the next setting. For dual registration or off-site/alternative provision while the pupil remains on roll, Gloverspiece retains the master file and shares relevant safeguarding information with the provider under an agreed reporting and escalation route; this is not a routine full-file transfer.

5. Retention and disposal

The school's retention schedule must identify the controller and purpose for each record. Where Gloverspiece is the last setting holding the child protection file, retain it until the child's 25th birthday. If the file relates to child sexual abuse, retain it until the child's 75th birthday, in line with DfE school record-keeping guidance. Review any litigation hold, inquiry, safeguarding review or other documented reason before disposal; do not destroy a record that remains needed.

A transfer receipt and limited audit record may be retained under the school's documented retention schedule to evidence safe handover. It does not replace the transferred file or justify keeping a full duplicate by default. Review retained records periodically, log authorised destruction and dispose of paper and digital copies securely, including relevant exports and backups according to the school's procedures.

6. Risk controls and review

Risk	Control and response
File lost or accessed without authority	Restricted permissions; locked storage and sign-out; periodic access review; report suspected loss immediately.
Wrong recipient or insecure transfer	Verify destination; approved encrypted channel; separate password if used; receipt and transfer log; initiate breach procedure immediately if misdirected.
Concern not acted on	Prompt CPOMS entry or paper fallback; direct alert to DSL/deputy; review actions, chronology and open cases.
Paper left at printer or desk	Secure printing, immediate collection, locked office/cabinet and confidential disposal.
Transition information missing or delayed	Check destination early; structured summary; deadlines, receipt and prompt review by receiving DSL; escalation if transfer stalls.
Excess retention or premature destruction	Documented schedule, annual review, disposal authorisation and legal hold check.

The DSL and data protection lead review this policy, the access arrangements and the risk controls at least annually and after a significant incident, system change or change in statutory guidance. This document describes operational controls; a separate DPIA should be completed or updated where a processing change is likely to create high risk to individuals.

Reference guidance

Department for Education, Keeping children safe in education 2026, paragraphs 140–150 and Annex B (September 2026): https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

Department for Education, Data protection in schools: Record keeping and management (child protection retention and transfer): https://www.gov.uk/guidance/data-protection-in-schools/record-keeping-and-management

Department for Education, Information sharing to safeguard children and young people (updated September 2026; information sharing duty commences 30 September 2026): https://www.gov.uk/government/publications/information-sharing-to-safeguard-children-and-young-people