

Safeguarding and Welfare Requirement: Information and Records

Confidentiality and client access to records

Policy statement

Our setting is committed to protecting the privacy, dignity and rights of all children and their families. We recognise that staff and managers hold a confidential relationship with families and must handle information with professionalism, integrity, and lawful practice.

We ensure that parents and carers can share information with confidence, knowing it will be used only to support their child's welfare, learning, and safety. All information is stored, processed, and shared in accordance with:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018

Data (Use and Access) Act 2025 (amending UK data-protection law)

- Human Rights Act 1998
- The EYFS Statutory Framework for group and school-based providers (effective 1 September 2026)
- Ofsted early years requirements and operating arrangements (September 2026)
- London Borough of Bromley information-sharing expectations

We maintain secure systems for managing children's records and uphold the highest standards of confidentiality, record-keeping, and information governance.

This policy has been reviewed against the EYFS statutory framework effective 1 September 2026, Working Together to Safeguard Children 2026, current Bromley Safeguarding Children Partnership/London procedures, and the UK GDPR and Data Protection Act 2018 as amended by the Data (Use and Access) Act 2025.

Confidentiality procedures

General Confidentiality Principles

- Information shared by families with the setting is treated as confidential, except where there is a legal or safeguarding requirement to share it.
- Information may be passed to other professionals (e.g., social care, health visitors, police, SEND professionals) only when necessary, lawful, and in line with our Safeguarding and Child Protection Policy and Information Sharing Policy.
- We explain how information will be used and shared through our privacy information and day-to-day practice. We do not promise absolute confidentiality where information may need to be shared lawfully to safeguard a child or another person.

Safeguarding and Welfare Requirement: Information and Records

Information Sharing

- We follow current statutory safeguarding information-sharing requirements, Working Together to Safeguard Children 2026, and Bromley Safeguarding Children Partnership/London safeguarding procedures. Staff are proactive in sharing relevant information early where this is necessary to identify, assess or respond to risks to a child.
- Information is only shared:
 - on a need-to-know basis,
 - where it supports the child's welfare, learning, or safety,
 - when consent has been obtained wherever appropriate, or
 - when there is a lawful basis for sharing without consent (e.g., safeguarding concerns).

Data protection and safeguarding principles

Personal data is processed lawfully, fairly and transparently; collected for specified purposes; limited to what is necessary; kept accurate and up to date where needed; retained no longer than necessary; and protected by appropriate security.

Safeguarding information may be shared without consent where there is a lawful basis and sharing is necessary and proportionate. Consent is not the only lawful basis for sharing. Staff record significant information-sharing decisions, including what was shared, with whom, why, and any decision not to share.

Where it is safe and appropriate, children and parents are informed about information sharing. They are not informed in advance where doing so could place a child or another person at increased risk, prejudice an investigation, or otherwise be unlawful.

Parent-to-Parent Information

- If parents choose to share personal information about themselves with other parents, the setting cannot be held responsible if those parents share that information further.
- Group discussions (e.g., workshops, support groups) have a confidentiality agreement; however, the setting cannot guarantee participants will always uphold this.

Recording Confidential Information

Parents are informed when we need to record confidential information beyond standard personal details, including:

- Injuries, disclosures or welfare concerns
- Significant changes in the child's home life
- Records relating to child protection concerns
- Correspondence or meetings with external professionals

We always explain:

- Why the information is being recorded
- How it will be used
- Who it may be shared with

Safeguarding and Welfare Requirement: Information and Records

All recording follows our Children's Records Policy and Privacy Notice.

Secure Storage of Information

- All children's records are stored securely in locked cabinets or password-protected digital systems compliant with UK GDPR.
- Staff may type reports or letters digitally; electronic drafts are deleted securely when no longer needed.
- No confidential information is stored on personal devices.
- Access to records is strictly limited to authorised staff.

Digital security, breaches and new technology

Access permissions are role-based and reviewed when staff join, change role or leave. Passwords and authentication details are not shared. Confidential information is sent only by approved secure methods and recipients are checked before sending.

Personal data breaches, including loss, misdirection, unauthorised access or disclosure, are reported immediately to the Manager/data protection lead, contained and documented. The setting assesses whether notification to the ICO and/or affected individuals is legally required and meets the applicable statutory timescale.

Personal or confidential information about children and families must not be entered into unapproved artificial-intelligence tools, personal cloud storage, messaging services or other unapproved applications. Any approved digital or AI use must have a lawful basis, appropriate security, data-minimisation controls and a documented assessment where required.

Staff Confidentiality and Information Access

- Staff discuss children's general progress in team meetings; sensitive information is restricted to the Manager, Deputy, Designated Safeguarding Lead (DSL) and the child's Key Person.
- Staff do not discuss any child with:
 - staff not involved in that child's care,
 - other parents,
 - any unauthorised individual.
- Discussions with external professionals occur in a formal, professional context only.

Managing Third-Party Information

- When third-party information is shared with us, staff check whether it is confidential and whether consent is required before further sharing.
- Third parties may include:
 - family members
 - social workers
 - health professionals
 - educational professionals

Safeguarding and Welfare Requirement: Information and Records

Client access to records procedures

A request for a child's personal information is handled as a subject access request (SAR) under the UK GDPR and Data Protection Act 2018 as amended by the Data (Use and Access) Act 2025. The child's information rights belong to the child. Where a young child is not competent to exercise those rights independently, it will usually be appropriate for a person with parental responsibility to exercise them on the child's behalf, unless disclosure would not be in the child's best interests.

Making a Request

- A SAR may be made verbally or in writing and does not need to mention data protection law or use a particular form. Requests are passed promptly to the Setting Manager/data protection lead and identity or authority is checked where reasonably necessary.
- We respond without undue delay and within the applicable one-month period. Under the Data (Use and Access) Act 2025 changes, the calculation can begin from the latest relevant point where identity, authority, a permitted fee or reasonably required clarification is needed. The period may be extended by up to two further months where necessary because of complexity or the number of requests; the requester is told within the initial period and given the reason.
- A SAR is normally free of charge. A reasonable fee may only be charged, or a request refused, where the legal threshold for a manifestly unfounded or excessive request is met, or for further copies where permitted by law. The requester is informed of the reason and their rights.

Preparing the File

The Manager and Deputy:

- Review the file to ensure it is complete, well-ordered and accurate.
- Identify all references to third parties.
- Seek advice where necessary, including legal advice for complex cases.

Third-Party Consent

- Third-party information is considered carefully. Consent may be sought where appropriate, but it is not automatically required in every case. We apply the relevant data-protection rules and exemptions, balancing the requester's right of access with the rights and freedoms of other people.
- Information supplied by another agency is not automatically withheld. We consider whether it is the child's personal data, whether disclosure is lawful, and whether any exemption or restriction applies; specialist or legal advice is sought where necessary.

Redaction and "Clean Copy" Preparation

Safeguarding and Welfare Requirement: Information and Records

- Third-party personal data is redacted or withheld only where required after applying the relevant legal test; refusal of consent by a third party does not by itself determine the outcome.
- Staff names may also be redacted if disclosure could cause risk, relates to sensitive safeguarding information, or is part of a police investigation.
- We provide the child's personal data identified through a reasonable and proportionate search, subject to any applicable exemptions or restrictions. Information is not excluded merely because it originated with another organisation.

Viewing the File

- Information is supplied securely in a clear and accessible form. A meeting may be offered where helpful, but access is not conditional on attending a meeting.
- Only individuals with parental responsibility, or their legal representative/interpreter, may attend.
- A copy of the personal data is provided securely, subject to any lawful redactions, exemptions or restrictions.

Disputes, Corrections and Complaints

- Parents may request corrections of factual inaccuracies.
- Professional opinions or observations will not be changed, but parents' views will be added to the file where appropriate.
- Complaints about the content or handling of records should follow the setting's Complaints Procedure.

Data protection complaints

From 19 June 2026, the setting maintains a process for handling complaints from data subjects about how their personal data or information-rights requests have been handled. Complaints are acknowledged within 30 days and the setting takes appropriate steps to investigate and respond without undue delay, informing the complainant of the outcome.

Individuals are told that they may complain to the Information Commissioner's Office if they remain dissatisfied. Records of data-protection complaints and the action taken are retained securely.

Safeguarding Priority

All processes above remain subject to our overriding duty to safeguard and promote the welfare of children. Information will always be shared without delay where a child's safety is at risk.

Record retention, transfer and disposal

Records relating to individual children are retained for a reasonable period after the child leaves, taking account of EYFS requirements, safeguarding needs, limitation periods, insurance

Safeguarding and Welfare Requirement: Information and Records

requirements and the setting's retention schedule. Child-protection records are kept separately and transferred securely when this is required and lawful.

When records reach the end of their retention period, paper and electronic information is securely destroyed so that personal data cannot be reconstructed. Disposal is suspended where records are needed for an ongoing safeguarding matter, complaint, investigation, legal claim or statutory inquiry.

Legal framework

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Data (Use and Access) Act 2025
- Human Rights Act 1998
- Children Act 1989 & 2004
- Working Together to Safeguard Children 2026
- EYFS Statutory Framework for group and school-based providers (effective 1 September 2026)

Further guidance

- Working Together to Safeguard Children 2026 and current statutory safeguarding information-sharing guidance
- Bromley Safeguarding Children Partnership (BSCP) policies and London Child Safeguarding Procedures
- ICO (Information Commissioner's Office) Helpline: 0303 123 1113
- ICO: Right of access / subject access guidance, updated July 2026