

DATA PROTECTION, CONFIDENTIALITY, INFORMATION SHARING AND RECORDS POLICY

POLICY STATEMENT

St Eval Preschool is committed to protecting the privacy, confidentiality and personal information of children, parents, carers, staff and other individuals connected with the setting.

We recognise that accurate and appropriate recording, secure storage and lawful information sharing are essential to:

- safeguard and promote children's welfare;
- support children's learning, development and individual needs;
- meet statutory and regulatory requirements;
- manage the setting effectively;
- work appropriately with parents, carers and other professionals;
- enable effective multi-agency safeguarding.

The setting will comply with applicable UK data protection legislation and statutory guidance, including the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 as amended, the Data (Use and Access) Act 2025, the Human Rights Act 1998, and the current EYFS Statutory Framework for group and school-based providers.

The current EYFS framework requires providers to maintain records and obtain and share relevant information with parents/carers, professionals, police, social services and Ofsted where appropriate. Confidential records about children and staff must be held securely and only be accessible to those who have a right or professional need to see them.

RECORD KEEPING

St Eval Preschool maintains records that are necessary for the safe and efficient management of the setting and to meet the individual needs of children.

Records will be:

- accurate and factual;
- relevant and proportionate;
- recorded as soon as reasonably practicable;
- kept securely;
- accessible only to authorised persons with an appropriate professional need;
- retained only for as long as necessary and in accordance with applicable retention requirements;
- securely destroyed when the relevant retention period has expired.

Records must not be altered, removed or destroyed because their contents may be uncomfortable, controversial or potentially viewed by a parent, Ofsted or another professional.

Where an error is identified, the original record must remain identifiable and any correction should be made transparently, dated and attributable to the person making the amendment.

Records held by the setting

Records may include, where applicable:

- children's registration and contact details;
- parent/carer and parental responsibility information;
- emergency contact information;
- attendance records;
- key-person information;

- consent and permissions;
- health and medical information relevant to the child's care;
- allergy and medication records;
- accident, injury and incident records;
- safeguarding and child protection records;
- records of concerns and actions taken;
- SEND information and support plans;
- Early Help, Child in Need or Child Protection information where applicable;
- correspondence with parents/carers;
- correspondence with other professionals and agencies;
- records of meetings and professional discussions;
- complaints and responses;
- risk assessments;
- learning and development records;
- funding information;
- photographs and videos taken for legitimate setting purposes;
- information required by Ofsted, the local authority or other statutory bodies.

The setting will only collect and retain information that is necessary, relevant and proportionate to the purpose for which it is being processed.

DATA PROTECTION PRINCIPLES

Personal data must be processed in accordance with the principles of applicable data protection law.

In particular, personal data must be:

1. processed lawfully, fairly and transparently;
2. collected for specified, explicit and legitimate purposes;
3. adequate, relevant and limited to what is necessary;
4. accurate and, where necessary, kept up to date;
5. retained only for as long as necessary;
6. processed securely, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

St Eval Preschool will maintain appropriate technical and organisational measures to protect personal information.

LAWFUL PROCESSING

The setting will identify an appropriate lawful basis for processing personal information.

Depending on the circumstances, this may include:

- compliance with a legal obligation;
- performance of a contract;
- performance of a task carried out in the public interest or in the exercise of official authority, where applicable;
- legitimate interests, where applicable and appropriate;
- protection of vital interests;
- consent, where consent is the appropriate lawful basis.

Where special category data is processed, the setting will identify an appropriate additional condition under UK data protection law.

Consent is therefore not the legal basis for all information held by the setting.

Parents and carers will be informed through the setting's Privacy Notice about how their information and their child's information is collected, used, stored and shared.

SAFEGUARDING RECORDING

Safeguarding concerns must be recorded accurately and promptly.

Records should:

- distinguish clearly between fact, observation, information provided by another person and professional interpretation;
- avoid speculation, assumptions or judgemental language;
- include dates and times where relevant;
- record the exact words of a child where appropriate;
- describe injuries accurately, including their location and appearance where relevant;
- record what action was taken;
- record advice sought and from whom;
- record decisions to share or not share information and the reasons for those decisions;
- record relevant communication with parents/carers and other professionals;
- record the outcome of referrals where this information is known to the setting.

Where an injury or safeguarding concern is recorded, staff should describe what they observed rather than attempting to diagnose the cause.

For example, staff should record:

"A bruise approximately [description] was observed on the child's [location]."

rather than:

"The child was deliberately hurt."

unless the latter is a direct allegation made by the child or another person, in which case the source and exact wording should be recorded.

Safeguarding records should be completed as soon as reasonably practicable. There is no universal statutory requirement that every safeguarding record must be completed within a fixed five-working-day period; the setting expects significant safeguarding information to be recorded promptly and without unnecessary delay.

CONFIDENTIALITY

Information relating to children, families and staff will be treated as confidential where appropriate.

Confidential information will only be disclosed where:

- the individual has given valid consent, where consent is the appropriate basis;
- there is a lawful basis for disclosure;
- disclosure is required by law;
- disclosure is necessary to safeguard a child or another person;
- disclosure is necessary for another legitimate statutory or professional purpose.

Confidentiality does not mean that information can never be shared.

Staff must understand that information given to them in confidence may need to be shared with the DSL, manager or other appropriate professional where necessary to safeguard a child.

Staff must never promise a child, parent or another person that information will be kept secret where there is a possibility that it may need to be shared for safeguarding purposes.

INFORMATION SHARING FOR SAFEGUARDING

St Eval Preschool recognises that effective safeguarding depends upon appropriate information sharing.

The current statutory *Working Together to Safeguard Children 2026* guidance makes clear that data protection legislation is not a barrier to appropriate safeguarding information sharing. Consent is not necessarily required to share information for safeguarding purposes where there is a lawful basis for processing the information.

The setting may therefore share relevant information with appropriate professionals, including:

- Cornwall Children's Social Care/MASSH;
- social workers;
- the police;



- health professionals;
- other early years settings or schools;
- the local authority;
- Ofsted;
- other safeguarding partners or agencies where appropriate.

Where safeguarding concerns exist, the DSL or another appropriate member of staff will consider:

- what information is relevant;
- why it needs to be shared;
- who needs to receive it;
- the appropriate lawful basis;
- whether consent is appropriate or required;
- whether informing the parent/carer at that point could increase risk or prejudice safeguarding enquiries;
- how the decision will be recorded.

The decision to share or not share safeguarding information must be recorded, including the rationale.

SHARING INFORMATION WITHOUT PARENTAL CONSENT

Parental consent is not always required before information is shared for safeguarding purposes.

Where a child may be at risk of harm, practitioners must not allow uncertainty about consent to prevent necessary safeguarding action.

The setting may share information without parental consent where there is an appropriate lawful basis and where seeking consent is not appropriate, for example where:

- seeking consent could place the child or another person at increased risk of harm;
- seeking consent could prejudice a safeguarding or criminal investigation;
- there is another lawful requirement or basis for disclosure;
- the information needs to be shared urgently to protect a child or another person.

The current government safeguarding guidance states that consent is not necessary for safeguarding information sharing where there is a lawful basis.

Where practicable and safe, the reasons for not seeking consent or for sharing information despite a refusal should be explained to the parent/carer and recorded.

INFORMATION SHARING AND SAFEGUARDING REFERRALS

Where a safeguarding concern meets the threshold for referral, the setting will follow Cornwall's local safeguarding procedures and make a referral to the appropriate safeguarding service.

The setting's role is to:

- recognise concerns;
- record relevant facts;
- seek appropriate advice;
- provide relevant information to the appropriate safeguarding professionals;
- cooperate with any subsequent safeguarding assessment or enquiry.

The setting does not determine whether a child has suffered significant harm or whether a Section 47 enquiry should be undertaken. Such decisions are made by the appropriate statutory safeguarding authority.

Once information has been referred, the setting will cooperate with Children's Social Care, the police and other relevant professionals as required.

DECISIONS ABOUT INFORMING PARENTS

St Eval Preschool recognises the importance of working openly and honestly with parents and carers.

Parents will normally be informed about concerns relating to their child and involved in safeguarding processes where it is appropriate and safe to do so.

However, there may be circumstances in which the setting does not immediately inform a parent/carer that a safeguarding referral has been made.

This decision must be considered on a case-by-case basis, taking account of:

- the nature and seriousness of the concern;
- the child's safety and welfare;
- advice from the DSL, manager or safeguarding professionals;
- whether informing the parent could increase risk;
- whether disclosure could prejudice or interfere with safeguarding enquiries;
- any instructions or advice from Children's Social Care, the police or another relevant agency.

Where information is not shared with a parent/carer immediately, the reason for the decision should be recorded.

This is not intended to exclude or deceive parents/carers. It is a safeguarding decision based upon the circumstances and professional advice available at the time.

PHOTOGRAPHS, VIDEO AND DIGITAL RECORDS

Photographs and videos of children may only be taken for legitimate setting purposes and in accordance with the setting's privacy arrangements.

St Eval Preschool uses preschool-owned digital devices for professional purposes, including photographs used for children's learning records and the Tapestry online learning platform.

Staff must not use personal mobile phones or personal devices to photograph children for preschool purposes unless specifically authorised under an emergency procedure and in accordance with the setting's safeguarding and data protection arrangements.

Photographs taken for safeguarding purposes must only be taken where necessary and proportionate to the safeguarding concern.

Where a photograph of an injury is required to accurately record or communicate a safeguarding concern, it may be taken using an authorised preschool device and shared securely with the appropriate safeguarding professionals where there is a lawful basis for doing so.

Parental consent is not necessarily required for the processing or sharing of an image where it is necessary and lawful for safeguarding purposes.

Safeguarding photographs must:

- be limited to what is necessary;
- be stored securely;
- not be shared through personal messaging or social media;
- not be circulated unnecessarily;
- only be shared with appropriate professionals;
- be retained and deleted in accordance with the setting's retention requirements and any ongoing safeguarding requirements.

CHILDREN'S PERSONAL FILES

Children's personal files may contain:

Personal information

- registration information;
- contact details;
- parental responsibility information;
- emergency contacts;
- relevant court orders.

Health and welfare

- health information relevant to the child's care;
- allergies;
- medication information;

- accident and injury records.

Learning and development

- assessments;
- observations;
- learning records;
- progress information;
- transition information.

SEND

- identified additional needs;
- support plans;
- relevant professional reports;
- EHCP information where applicable.

Safeguarding

- records of concerns;
- safeguarding forms;
- records of actions taken;
- correspondence with parents;
- referrals;
- relevant professional correspondence;
- information received from safeguarding agencies.

Children's files must be kept securely, with access restricted to authorised individuals who have a legitimate professional need to access them.

ACCESS TO RECORDS AND SUBJECT ACCESS REQUESTS

The current EYFS framework states that parents/carers must be given access to records about their child, subject to any relevant exemptions under data protection law.

A parent/carer may make a Subject Access Request (SAR) for personal information held about themselves or, where appropriate, on behalf of their child.

A SAR does not need to use a prescribed form or particular wording. It may be made verbally or in writing.

The setting will:

1. identify and verify the requester where reasonably necessary;
2. establish whether the request is for the adult's information, the child's information, or both;
3. establish parental responsibility or other appropriate authority where the request is made on behalf of a child;
4. conduct a reasonable and proportionate search of relevant records;
5. consider whether any exemptions or restrictions apply;
6. redact information where necessary;
7. provide the information securely.

The normal response period is one month, subject to the applicable rules concerning clarification or additional information required from the requester. The Data (Use and Access) Act 2025 has amended the operation of subject access time limits, including a "stop the clock" provision where further information is reasonably required from the requester.

Where a request is complex or involves multiple requests, the applicable legislation may allow the response period to be extended by up to two further months. The requester must be informed where an extension is being used.

Information relating to other people will not automatically be disclosed. The setting will consider third-party privacy and any applicable safeguarding or other legal exemptions before disclosure.

Where records contain information supplied by or relating to Children's Social Care, the police, health professionals or another agency, the setting will consider whether that information should be disclosed by the setting or whether the requester should be directed to the agency that holds the relevant information.



Where disclosure may create a safeguarding risk, the setting will seek appropriate advice before releasing the information.

Records must never be altered, destroyed or withheld simply because a parent or other person has requested access to them.

CORRECTION OF INFORMATION

Individuals have rights in relation to inaccurate personal information.

If a parent/carers identifies a factual inaccuracy, the setting will consider the request for rectification. Where the information represents a professional opinion, assessment or account of an event rather than a demonstrably inaccurate fact, the setting will not necessarily amend the original record. Where appropriate, the individual's differing view may be recorded alongside the original information.

Original safeguarding records must not be rewritten retrospectively.

PRIVACY NOTICE

St Eval Preschool maintains a separate Privacy Notice explaining:

- what personal information is collected;
- why it is collected;
- the lawful bases for processing;
- how information is used;
- who information may be shared with;
- how information is protected;
- retention arrangements;
- individual data protection rights;
- how to raise a data protection concern.

The Privacy Notice will be provided to parents/carers and kept available for inspection.

The Privacy Notice will be reviewed whenever there are significant changes to the setting's processing activities or relevant data protection law.

WHO WE MAY SHARE INFORMATION WITH

Where there is an appropriate lawful basis, information may be shared with:

- Ofsted;
- Cornwall Council;
- Cornwall Children's Social Care/MASSH;
- the police;
- health professionals;
- social workers;
- other early years settings;
- schools;
- safeguarding partners;
- funding authorities;
- professional advisers;
- insurers where necessary;
- other statutory or regulatory bodies where legally required or permitted.

Information will only be shared where it is necessary, relevant and proportionate to the purpose.

The setting will not sell children's or families' personal information or provide it to organisations for their own unrelated marketing purposes.

SECURITY OF INFORMATION

Paper records will be stored in secure, locked storage when not in use.

Electronic information will be protected by appropriate technical and organisational measures, including secure passwords, access controls and appropriate security settings.



Staff must:

- keep passwords confidential;
- lock devices when unattended;
- avoid accessing confidential information in inappropriate public places;
- not send confidential information through personal email or messaging accounts;
- not store setting information on personal devices unless expressly authorised;
- report suspected data breaches immediately to the manager/Data Protection Lead.

Any suspected personal data breach must be assessed promptly and managed in accordance with the setting's data breach procedure.

Where a breach is likely to result in a risk to individuals' rights and freedoms, the setting will consider whether notification to the Information Commissioner's Office is required within the applicable statutory timeframe.

EMAIL AND ELECTRONIC COMMUNICATION

Staff must take appropriate care when sending personal or confidential information electronically.

Before sending confidential information, staff should:

- check the recipient carefully;
- ensure the information is necessary to send;
- use secure systems where available;
- avoid copying unnecessary individuals into communications;
- use appropriate password protection/encryption where required.

Confidential safeguarding information must not be sent through personal email accounts or informal messaging applications unless there is an authorised emergency procedure and an appropriate lawful basis.

Tapestry

St Eval Preschool uses Tapestry as a professional communication and learning-record system.

Information uploaded to Tapestry must:

- relate to the child and their learning, development, welfare or relevant setting communication;
- be appropriate and proportionate;
- be accessed only by authorised users;
- comply with the setting's privacy and safeguarding procedures.

Photographs uploaded to Tapestry must only be taken using authorised preschool equipment in accordance with the setting's mobile phone/device policy.

RETENTION AND DESTRUCTION

Personal information will not be retained indefinitely.

The setting will maintain a retention schedule identifying appropriate retention periods for different categories of records.

Retention periods will take account of:

- statutory requirements;
- EYFS requirements;
- Ofsted requirements;
- safeguarding requirements;
- local safeguarding arrangements;
- insurance requirements;
- legal claims;
- the nature and sensitivity of the information.

Where safeguarding or child protection concerns have been referred to Children's Social Care, records may need to be retained for longer than ordinary childcare records where this is necessary and lawful.

Records must be securely destroyed when the applicable retention period has expired and there is no continuing lawful reason to retain them.

TRANSFER OF CHILDREN'S RECORDS

When a child moves to another early years setting or school, relevant information will be transferred securely to support continuity of care, learning and safeguarding.

Developmental and educational information will be shared as appropriate.

Where there are current or significant safeguarding concerns, relevant safeguarding information will be shared with the receiving setting in accordance with safeguarding procedures and data protection law.

Where appropriate, the receiving setting's DSL will be contacted directly to ensure that important safeguarding information is received securely and understood.

Parental consent is not necessarily required for safeguarding information sharing where there is a lawful basis to share the information.

The decision about what safeguarding information should be transferred will be made on a case-by-case basis, ensuring that information is:

- accurate;
- relevant;
- necessary;
- proportionate;
- securely transferred.

The setting will not routinely transfer an entire child's personal file unless there is a lawful and appropriate reason to do so.

STAFF RESPONSIBILITIES

All staff are responsible for protecting confidential information.

Staff must:

- follow this policy;
- complete required safeguarding and data protection training;
- maintain confidentiality;
- record information accurately;
- only access information they have a legitimate professional reason to access;
- share safeguarding information appropriately;
- report concerns to the DSL;
- report suspected data breaches immediately;
- never use personal devices or accounts to store or share confidential setting information unless specifically authorised.

Failure to follow these requirements may result in disciplinary action and, where appropriate, referral to relevant authorities.

SAFEGUARDING AND DATA PROTECTION DECISION-MAKING

Where staff are uncertain about whether information should be recorded, shared, retained or disclosed, they should seek advice from:

1. the DSL;
2. the DDSL/Manager;
3. the relevant safeguarding professionals;
4. the setting's data protection adviser/DPO;
5. legal advice, where necessary.

Staff should not allow uncertainty about data protection to prevent necessary safeguarding action.

Similarly, safeguarding responsibilities do not remove the need to comply with data protection law. Information must be shared lawfully, securely and proportionately.

LEGAL AND STATUTORY REFERENCES

This policy should be read alongside the current versions of:

- Early Years Foundation Stage (EYFS) Statutory Framework for Group and School-Based Providers – effective 1 September 2026. (GOV.UK)
- Working Together to Safeguard Children 2026 – statutory guidance. (GOV.UK)
- Information Sharing: Advice for Practitioners Providing Safeguarding Services to Children, Young People, Parents and Carers – current statutory guidance. (GOV.UK)
- UK General Data Protection Regulation (UK GDPR), as amended.
- Data Protection Act 2018, as amended.
- Data (Use and Access) Act 2025. (GOV.UK)
- Human Rights Act 1998.
- Children Act 1989.
- Children Act 2004, including applicable information-sharing provisions.
- Freedom of Information Act 2000, where applicable.
- Relevant Cornwall safeguarding partnership procedures and information-sharing arrangements.

REVIEW

This policy will be reviewed at least annually and sooner where:

- legislation changes;
- statutory guidance changes;
- local safeguarding procedures change;
- there is a significant data protection incident;
- Ofsted identifies an issue;
- the setting's systems or technology change;
- the setting identifies a need to strengthen its procedures.

