St James Infant & Pre-School

Confidentiality and Safeguarding Information-Sharing Policy

2026-27

Policy status	Non-statutory policy supporting statutory safeguarding and data protection duties
Policy lead	Headteacher / Designated Safeguarding Lead
Data controller	Inspire Multi Academy Trust (INMAT)
Information rights service	Plumsun Ltd - manages all SAR and FOI requests on behalf of the school - gdpr@inmat.org.uk
Approval route	Headteacher and Local Academy Committee
Effective from	1 September 2026
Review date	July 2027, or sooner if requirements change

Controlled document - use the current approved version.

> **Key principle:** No one can promise absolute confidentiality. Data protection law supports appropriate information sharing and must never prevent timely action to protect a child.

1. Purpose, scope and legal framework

This policy explains how St James Infant & Pre-School protects confidential information and shares it safely, lawfully and proportionately. It applies to staff, agency and supply workers, volunteers, governors, trainees, contractors and visitors, on and off site and across verbal, written, image, audio and electronic records.

It supports INMAT's data protection arrangements and the school's safeguarding, staff conduct, online safety, records, complaints, whistleblowing, acceptable use and AI policies. INMAT is the data controller.

The policy reflects the UK GDPR and Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025; Children Acts 1989 and 2004; Education Act 2002; Childcare Act 2006; Human Rights Act 1998; Freedom of Information Act 2000; common law confidentiality; Keeping Children Safe in Education 2026; Working Together to Safeguard Children 2026; the EYFS statutory framework; DfE Information Sharing Advice 2024; ICO guidance; and Northamptonshire safeguarding procedures.

2. Confidentiality principles

The child's safety, welfare and best interests come first.

Information is shared only for a clear purpose, with people who need it, and to the extent necessary.

Information must be relevant, adequate, accurate, timely, proportionate and securely handled.

Facts, observations, allegations, the child's words and professional opinions must be clearly distinguished.

Children and families are usually told what will be shared, with whom and why, unless this could increase risk, prejudice an investigation or cause harmful delay.

The child's views are heard in an age-appropriate way, but the school cannot give a child or adult control over action needed to keep someone safe.

The reasons for sharing, or deciding not to share, must be recorded.

Confidential information is information given or obtained where privacy is reasonably expected. The duty is important but not absolute. Identifiable information may need to be shared because identity, chronology and family context can be essential to understanding and managing safeguarding risk.

At the beginning of a sensitive conversation, where practicable, staff should explain that they will respect privacy but may need to tell people who can help. Staff must never promise secrecy.

3. Responsibilities

Headteacher. Ensures that the policy is implemented, staff are trained, approved systems are used, breaches are escalated and confidentiality is not used to conceal unsafe practice.

Designated Safeguarding Lead and deputies. Lead safeguarding information-sharing decisions, advise staff, maintain secure records, make and follow up referrals and ensure reliable cover when the DSL is unavailable.

Plumsun Ltd. Acts as INMAT's Data Protection Officer and information rights service. Plumsun manages all subject access requests (SARs) and Freedom of Information (FOI) requests on behalf of the school, including logging requests, confirming scope and identity, advising on exemptions and redaction, coordinating searches and issuing or overseeing responses.

> **SAR and FOI requests:** Any request received by the school must be forwarded to gdpr@inmat.org.uk and the Headteacher immediately, and no later than the same working day. A request may be verbal or written and does not need to mention SAR, FOI or legislation. Staff must not respond, disclose, redact or refuse information independently unless instructed by Plumsun.

All staff, volunteers and governors. Access only information needed for their role, follow approved systems, report safeguarding concerns promptly, maintain privacy and report any actual or suspected breach immediately.

4. Safeguarding information sharing

> **Urgent action:** Call 999 if a child is in immediate danger. Contact West Northamptonshire MASH on 0300 126 7000 for an urgent child-protection concern. Inform the DSL, but do not delay because a DSL, parent or DPO is unavailable.

Consent is not normally required where a child is at risk or there is a perceived risk of harm, provided there is a lawful basis. For safeguarding, this will most commonly be legal obligation and/or public task under Article 6 UK GDPR. Special-category information will usually rely on substantial public interest under Article 9(2)(g) and the safeguarding condition in Schedule 1, Part 2, paragraph 18 of the Data Protection Act 2018.

Staff and leaders will:

- Identify the safeguarding purpose and the possible harm from sharing or failing to share.
- Share proactively and as early as possible when this may help identify, assess or respond to risk.
- Verify the recipient's identity, role and need to know.
- Share only necessary, relevant, accurate and proportionate information, with enough context to avoid misunderstanding.
- Tell the child and, where appropriate, the parent or carer unless doing so would be unsafe or cause harmful delay.
- Use an approved secure method and protect the identity of anyone who may be endangered if identified.

Record the decision, rationale, lawful basis, information shared, recipient, method, time and follow-up. Record decisions not to share.

Staff receiving a disclosure should listen calmly, avoid leading questions, reassure the child, explain what will happen next, record the child's own words and report immediately to the DSL or deputy. The concern must be entered promptly on MyConcern. Staff must not investigate.

5. Records, security and transfer

Safeguarding concerns, decisions, referrals, professional discussions and outcomes must be recorded promptly on MyConcern. Records must be factual, dated, timed, attributable to the author and kept separately from the main pupil record. Access is limited to those who need it.

Staff must:

use school or Trust accounts, devices and approved systems;

verify recipients and attachments before sending and use secure transfer or encryption where required;

keep conversations private and avoid corridors, social media and informal messaging groups;

secure papers, screens and devices and dispose of confidential waste appropriately;

never copy school records to personal devices, email, cloud storage or unapproved systems; and

report misdirected emails, lost records, unauthorised access or overheard disclosures immediately.

Personal or safeguarding information must not be entered into unapproved AI, transcription, voice-to-text, chatbot or observation tools. Approved systems may be used only for the authorised purpose, with appropriate contracts, security, privacy information and, where required, a data protection impact assessment. Staff remain accountable for checking accuracy.

When a child leaves, the DSL transfers the child-protection file securely and separately from the main pupil file within five days of an in-year transfer or within the first five days of a new term. Receipt must be confirmed. Relevant risk or support information should be discussed with the receiving DSL before arrival where necessary.

6. Information requests, staff matters and breaches

6.1 Subject access and Freedom of Information

Plumsun manages every SAR and FOI request for the school. School staff must preserve relevant records and provide them securely when requested by Plumsun. The legal clock starts when a valid request reaches the school, so requests must be forwarded the same working day. Plumsun will coordinate the applicable deadline, normally one month for a SAR and 20 school working days for FOI.

A parent does not automatically have access to every record about their child or another person. Personal-data rights belong to the child, although a parent may exercise them where appropriate. Plumsun will consider identity and authority, third-party information, legal privilege, safeguarding

exemptions and the serious-harm test before disclosure. The school will not disclose another child's personal information when explaining an incident.

6.2 Staff information and whistleblowing

Employment, health, disciplinary, allegation and low-level concern information is handled on a strict need-to-know basis. Confidentiality does not prevent necessary sharing with INMAT, the LADO, children's social care, police, DBS, Teaching Regulation Agency or another authorised body. It does not prevent a protected disclosure, safeguarding referral, report of crime or seeking professional or trade union advice.

6.3 Personal data breaches and complaints

Any loss, unauthorised disclosure, access, alteration or destruction of personal data must be reported immediately to the Headteacher and Plumsun. Staff should take safe containment action but must not conceal the incident, delete evidence or contact affected people without direction. Plumsun and INMAT will assess the risk and make any required ICO or individual notification.

Data protection concerns should be sent to gdpr@inmat.org.uk. Complaints will be acknowledged within 30 days and answered without undue delay. A safeguarding concern will always be acted on immediately and will not be treated only as a data protection complaint.

7. Training, monitoring and review

Confidentiality, secure handling and safeguarding information sharing are included in induction and regular safeguarding updates. The Headteacher, DSL and DPO monitor practice through record quality, access controls, transfer receipts, training, complaints, breaches and new system reviews. The Local Academy Committee receives appropriate assurance without unnecessary case-identifiable information.

This policy is reviewed annually and sooner if legislation, statutory guidance, local procedures, technology or Trust requirements change.

Appendix: Quick contacts and sources

School safeguarding	Current DSL and deputies are listed in the Safeguarding Policy and on school posters. School office: 01327 702783.
Plumsun - DPO, SAR and FOI	gdpr@inmat.org.uk - www.plumsun.com. Forward every SAR and FOI request immediately.
MASH and Police	MASH: 0300 126 7000, including urgent out-of-hours concerns. Police: 999 for immediate danger; 101 for non-emergencies.
LADO and ICO	LADO: 0300 126 7000 - LADOConsultations@NCTrust.co.uk. ICO: www.ico.org.uk.