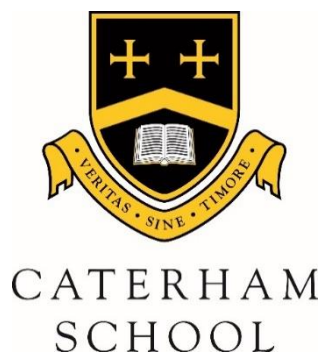


Information Sharing Policy



Policy Author:	DPO
Date reviewed by Author:	November 2025
Next review due:	November 2026

This policy is reviewed annually

Introduction

The school's information sharing policy underscores the crucial role of sharing data to address potential abuse, support children's welfare, and aid educational progress. Safeguarding partners must transparently outline local action criteria, including early help assessments and referrals for social care. Governing bodies must facilitate information sharing within schools and with relevant agencies, emphasising timely sharing to address risks. Adherence to Data Protection laws is essential, permitting sensitive data sharing for safeguarding purposes. This Policy covers data sharing within the Family of Schools -Caterham School (Senior & Prep), Copthorne Prep School and Hawthorns School.

1. Purpose and Scope

- This policy integrates and supports existing policies of Caterham School and other schools within the Family of schools, including the Safeguarding Policy and the IT Acceptable Use Policy suite.
- Ensures compliance with the GDPR and KCSIE, emphasising personal data protection and child safety.
- Applies to all staff, students, parents, and third parties involved in data processing or student interaction.

This policy should be read in conjunction with the following documents:

- *Schools Safeguarding Policy (2025)*
- *Schools Online Safety Policy (2025)*
- *School Complaints Policy (2025)*
- *School Curriculum Policy (2025)*
- *Keeping Children Safe in Education (2025)*

2. Data Protection Principles (Referencing GDPR)

- **Compliance with GDPR and KCSIE:** As outlined in KCSIE 2025, information sharing is vital for the effective identification, assessment, and provision of services, especially in safeguarding contexts. All information sharing must respect data privacy as mandated by GDPR and the child protection principles of KCSIE.
- **Lawfulness, Fairness, and Transparency:** Processing of personal data will comply with legal obligations and be transparent to data subjects.
- **Purpose Limitation:** Data collected will align with the school's Privacy Notice, ensuring clarity on data usage.
- **Data Minimization and Accuracy:** In line with the school's Record Management Policy, only necessary data will be collected and maintained accurately.

- **Storage Limitation:** Ensure that all personal data is stored securely, whether in electronic or paper format, as per GDPR guidelines. Data retention will follow the GDPR guidelines and the school's Staff Code of Conduct. -
- **Access Control:** Information is shared strictly on a need-to-know basis. Staff should only access and share personal information necessary for the intended purpose. Access to sensitive information should be restricted to authorised personnel only.
- **Integrity and Confidentiality:** Data will be processed in accordance with the Online Safety Policy and Staff Code of Conduct, ensuring confidentiality and security. A high level of confidentiality must be maintained. Discussions about pupils and parents should be held in private settings and only with relevant parties.

3. Child Safety (Incorporating KCSIE Guidelines)

- **Designated Safeguarding Lead (DSL):** The DSL will be responsible for handling all safeguarding concerns, in alignment with the Safeguarding Policy.
- **Training and Awareness:** Staff will receive annual training on child protection, referencing KCSIE, online safety and the school's Staff Code of Conduct.
- **Safe Recruitment Practices:** As per the Recruitment Policy, all staff will undergo thorough checks, including DBS, to ensure child safety.
- **Online Safety:** The Online Safety Policy will guide measures to protect children from online risks.

4. Information Sharing in Meetings

- **In-person Meetings with Parents and Pupils:** Discussions should be held in private and confidential spaces. Information shared in these meetings should be documented and stored securely.
- **Remote Meetings:** Similar to in-person meetings, remote meetings must ensure confidentiality. Use secure, school-approved platforms and avoid sharing sensitive information in unsecured environments.
- **Staff Meetings:** When discussing pupils or parents, staff should ensure the information is relevant to the educational or welfare needs of the pupil. Minutes of these meetings should be recorded and stored in compliance with GDPR.

5. Reporting and Compliance

- **Data Breaches:** To be reported to the Data Protection Officer, as per the Data Breach Response Plan.
- **Safeguarding Concerns:** Immediate reporting to the DSL, following procedures outlined in the Safeguarding Policy.
- **Review and Audit:** Annual review of this policy, ensuring alignment with current GDPR, KCSIE standards, and school policies.

6. Policy Enforcement

- Violation of this policy will be addressed as per the Staff Code of Conduct, with potential legal implications under GDPR and child protection laws.

7. Contact Information

- Questions or concerns related to data protection or sharing of data :
DPO's at the relevant school
- Safeguarding inquiries: DSL at the relevant schools