



ENSE 07

Data Protection Policy and Privacy Notice

Document Author:	Christine Williams
Approval Date (original):	2018
Authorised by:	Lorna Mclean
Review Date:	September 2026
Next Review Date:	September 2027

Contents

1. Purpose and scope
 2. Legal and regulatory framework
 3. Definitions
 4. Data controller, DPO and governance
 5. Data protection principles and accountability
 6. Lawful processing
 7. Privacy information and transparency
 8. Children's data and capacity
 9. Sharing personal data and safeguarding
 10. Individual rights and subject access requests
 11. Data protection complaints
 12. Educational records
 13. CCTV
 14. Photographs and video
 15. Data protection by design, DPIAs and EdTech
 16. Artificial intelligence and automated decision-making
 17. Information security, filtering and monitoring
 18. Retention, disposal and records management
 19. International transfers
 20. Personal data breaches
 21. Training and awareness
 22. Monitoring, assurance and review
 23. Related policies and records
- Appendix A – Personal data breach procedure
- Appendix B – Data protection complaint procedure
- Appendix C – Staff quick-response guide

1. Purpose and scope

King Edwin School is an independent special school supporting pupils with Social, Emotional and Mental Health (SEMH) needs and associated special educational needs. The school recognises that pupils' records may contain particularly sensitive information and that effective data protection is integral to safeguarding, dignity, trust and safe education.

This policy applies to all personal data processed by or on behalf of the school, in any format, about pupils, parents and carers, staff, applicants, contractors, visitors, governors/proprietors and other individuals. It applies to employees, agency staff, volunteers, governors/proprietors, contractors and processors acting on the school's behalf.

The school will protect personal data while ensuring that data protection law is not used as a barrier to appropriate safeguarding information sharing. Where a child may be at risk, the safety and welfare of the child are paramount and information will be shared lawfully, proportionately and on a need-to-know basis.

2. Legal and regulatory framework

This policy is designed to operate within the UK data protection framework in force during 2026-2027. The Data (Use and Access) Act 2025 (DUAA) does not replace the UK GDPR or Data Protection Act 2018; it amends and supplements the framework.

- UK General Data Protection Regulation (UK GDPR), as amended
- Data Protection Act 2018, as amended
- Data (Use and Access) Act 2025
- Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR), where applicable
- Freedom of Information Act 2000, where applicable to the relevant body or information
- Human Rights Act 1998 and common-law confidentiality principles, where relevant
- Children Act 1989 and 2004 and current safeguarding legislation/guidance where information sharing concerns a child's welfare
- Current Department for Education data protection in schools guidance and current Information Commissioner's Office (ICO) guidance

Where legislation, statutory guidance or ICO guidance changes during the policy period, the school will apply the current legal requirement and update this policy as necessary.

3. Definitions

Term	Meaning
Personal data	Information relating to an identified or identifiable living individual.
Special category data	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership; genetic data; biometric data used for unique identification; health data; and data concerning a person's sex life or sexual orientation.
Criminal offence data	Personal data relating to criminal convictions, offences or related security measures.
Processing	Any operation performed on personal data, including collecting, recording, organising, storing, altering, retrieving, consulting, using, sharing, restricting, erasing or destroying it.
Controller	The person or organisation that determines the purposes and means of processing.
Processor	A person or organisation processing personal data on behalf of a controller.
Personal data breach	A security breach leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
DPIA	A Data Protection Impact Assessment used to identify and reduce privacy risks in processing likely to result in high risk to individuals.

4. Data controller, DPO and governance

The school will maintain a clear written record identifying the legal entity that acts as data controller for each processing activity and will ensure that the appropriate controller is registered with the ICO and pays any required data protection fee. The school will not describe itself as the legal controller where another group entity is the controller for the relevant processing.

4.1 Data Protection Officer (DPO)

The organisation's Data Protection Officer can be contacted at Data.Protection@CareTech-uk.com. The DPO will operate with appropriate independence and access to senior decision-makers. Responsibilities include advising on obligations, monitoring compliance, advising on DPIAs, supporting information-rights requests, monitoring data incidents and acting as a contact point for the ICO and data subjects.

4.2 King Edwin School Data Protection Lead (DPL)

The school retains its local Data Protection Lead arrangement. The DPL is the Associate Principal in Operations and Safeguarding, currently Christine Williams. The DPL coordinates day-to-day implementation at school level in consultation with the DPO. If the named postholder

changes, the role transfers to the person formally appointed by the school; contact information will be updated without waiting for the annual policy review.

4.3 Principal and proprietor/governance

- The Principal is responsible for ensuring operational implementation and appropriate escalation.
- The proprietor/governing body has strategic oversight and receives assurance about data protection compliance, risks and significant incidents.
- Senior leaders will ensure appropriate resources, systems, training and contracts are in place.
- All staff are personally responsible for handling personal data in accordance with this policy and must report suspected breaches immediately.

5. Data protection principles and accountability

- lawfulness, fairness and transparency
- purpose limitation
- data minimisation
- accuracy
- storage limitation
- integrity and confidentiality (security)
- accountability: the school must be able to demonstrate compliance

The school will maintain proportionate evidence of compliance, including records of processing activities, privacy notices, data-sharing arrangements, processor contracts, DPIAs, training records, breach records, information-rights logs and retention arrangements.

6. Lawful processing

A lawful basis will be identified and documented for each processing activity. The school will not rely on consent where individuals do not have a genuine choice or where another lawful basis is more appropriate.

- consent
- contract
- legal obligation
- vital interests
- public task/official authority, where applicable to the relevant controller and function
- legitimate interests, subject to the required balancing assessment and any limitations
- recognised legitimate interests where the statutory conditions introduced by the DUAA apply

Special category data and criminal offence data will only be processed where both an Article 6 lawful basis and the additional UK GDPR/DPA 2018 condition(s) are satisfied. Where required, the controller will maintain an Appropriate Policy Document under Schedule 1 to the Data Protection Act 2018.

7. Privacy information and transparency

The school will provide privacy information at the appropriate time and in a form that is concise, transparent, intelligible and accessible. Separate or layered privacy notices may be used for pupils, parents/carers, staff, applicants, visitors, CCTV and other processing. Privacy notices will identify the controller, purposes, lawful bases, categories of data, recipients, retention information, international transfers where relevant, rights, complaint routes and DPO contact details.

Privacy information for pupils will be written in clear, age- and developmentally-appropriate language, taking account of SEND and communication needs. This policy is not a substitute for the school's operational privacy notices.

8. Children's data and capacity

Personal data about a pupil belongs to the pupil. The school will assess whether a child can understand and exercise their data protection rights on a case-by-case basis, taking account of age, maturity, understanding, communication needs and the complexity of the request. No fixed age will be treated as an automatic rule for capacity.

A person with parental responsibility may exercise rights on a child's behalf where appropriate, for example where the child lacks sufficient understanding or authorises the parent/carer to act. The school will consider the child's best interests, confidentiality and safeguarding before disclosure.

9. Sharing personal data and safeguarding

The school will share personal data only where there is a lawful basis and the sharing is necessary, proportionate and secure. Consent is not automatically required for lawful safeguarding information sharing and should not be sought where doing so would place a child at risk or prejudice a safeguarding response.

- local authorities, health and social care bodies and safeguarding partners
- police and other law-enforcement bodies where lawful
- exam bodies, education providers and other agencies supporting a pupil
- service providers and processors operating under appropriate written contracts
- emergency services where necessary to protect life or respond to an emergency
- other recipients where required or permitted by law

Before routine or high-risk sharing, the school will consider data minimisation, security, transparency, data-sharing agreements and whether a DPIA is required. Safeguarding information will be transferred securely when a pupil moves school in accordance with current safeguarding requirements.

10. Individual rights and subject access requests

Individuals have rights under data protection law, subject to applicable conditions and exemptions. These include rights to information, access, rectification, erasure in certain circumstances, restriction, objection, data portability in certain circumstances, withdrawal of consent and safeguards in relation to automated decision-making.

10.1 Subject access requests (SARs)

- A SAR can be made verbally or in writing and does not need to use the words “subject access request”.
- Any member of staff receiving a possible SAR must forward it immediately to the DPL/DPO.
- The school may request information reasonably necessary to verify identity or clarify the information sought where permitted by law.
- The school will respond without undue delay and normally within one month, subject to any lawful extension or pause permitted by the current legislation.
- Information will normally be provided free of charge. A reasonable fee may be charged, or a request refused, only where the law permits.
- Third-party information, safeguarding material, legal privilege and other exempt information will be considered carefully before disclosure.
- The school will keep a record of the request, searches undertaken, decisions, redactions, exemptions and response.

11. Data protection complaints

Any person may complain about the school's handling of their personal data. Complaints may be made by email, letter, verbally or through any electronic complaint route made available by the controller. Staff must promptly forward a data protection complaint to the DPL/DPO.

- The controller will acknowledge a data protection complaint within 30 days.
- The complaint will be investigated appropriately and the complainant will be kept informed where necessary.
- A substantive response will be provided without undue delay, explaining the outcome and any action taken.
- The complainant will be told of their right to raise the matter with the ICO and of any other applicable remedy.
- Complaint records will be retained in accordance with the retention schedule and used to identify recurring issues.

12. Educational records

Requests for pupil information will be handled under the legal route that applies to King Edwin School and the information requested. The school will not assume that the statutory 15-school-day educational-record access regime applicable to certain maintained-school records applies identically to an independent special school. Requests will therefore be assessed as SARs or under another applicable statutory right, with advice from the DPO where necessary.

13. CCTV

King Edwin School uses CCTV at appropriate locations for specified safety, safeguarding, security and property-protection purposes. CCTV footage is personal data where individuals can be identified.

- The purpose and lawful basis for CCTV will be documented.
- Cameras will be positioned proportionately and privacy risks considered before installation or material change; a DPIA will be completed where required.
- Clear signs will identify CCTV use and privacy notices will explain the processing.
- Access will be limited to trained, authorised staff and reviewed when roles change.
- Footage will be stored securely and retained only for the shortest period necessary for the documented purpose, unless required for an incident, investigation or legal claim.
- Disclosure to police or other third parties will be recorded and made only where lawful and necessary.
- SARs may include CCTV footage and will be handled under section 10.

14. Photographs and video

The school may take photographs and video for educational, safeguarding, record-keeping, communication and promotional purposes. The school will identify the correct lawful basis for each use rather than assuming that all photography requires consent.

- Where consent is the lawful basis, it will be specific, informed, recorded and capable of withdrawal.
- Pupils will be given appropriate information and their wishes considered, taking account of age, understanding and SEND.
- Images will not routinely be accompanied by unnecessary identifying information.
- External publication, social media and marketing uses will be subject to additional safeguarding and privacy controls.
- Parents/carers taking images for purely personal or household purposes are generally outside UK GDPR, but the school may impose event rules to protect safeguarding, privacy and dignity.

15. Data protection by design, DPIAs and EdTech

Data protection will be considered from the start of new projects, systems and changes to processing. A DPIA will be completed before processing likely to result in high risk, and where otherwise required by law or current ICO/DfE guidance.

- new monitoring, biometric, AI or profiling technologies
- large-scale or systematic processing of sensitive pupil information
- new EdTech/cloud systems handling personal data
- significant changes to CCTV or filtering/monitoring systems
- new high-risk data-sharing arrangements

Before procuring EdTech, the school will assess the supplier's privacy information, security, processor terms, sub-processors, data location/transfers, retention/deletion, children's privacy protections, breach support and ability to support individual rights. Contracts with processors will contain the terms required by data protection law.

16. Artificial intelligence and automated decision-making

King Edwin School recognises that approved AI tools may support learning, accessibility and administration. Staff and pupils must not enter personal, safeguarding, special category or confidential information into an AI service unless the service has been formally approved for that processing and the required safeguards are in place.

- A DPIA and procurement/privacy assessment will be completed where required before deploying AI that processes personal data.
- Only the minimum necessary data will be used; anonymised or synthetic data will be preferred where practicable.
- The school will be transparent about material AI processing affecting individuals.
- Outputs will be checked by a competent human and will not be treated as inherently accurate.
- AI will not replace professional safeguarding judgement or statutory decision-making responsibilities.
- Inappropriate disclosure of personal data through an AI tool will be treated as a potential personal data breach.

16.1 Solely automated significant decisions

Where a decision producing legal or similarly significant effects is based solely on automated processing, the school/controller will ensure that the processing is permitted under the amended UK GDPR and that the required safeguards apply. Individuals will be provided with information about the decision and enabled to make representations and obtain meaningful human intervention. Additional restrictions applying to special category data will be observed.

17. Information security, filtering and monitoring

- access to systems and records will be role-based and limited to those who need it
- strong unique passwords and multi-factor authentication will be used where available/appropriate
- school-managed devices and removable media containing personal data will be encrypted where appropriate
- confidential paper records will be secured when unattended
- personal data will only be taken off site where necessary and protected in accordance with school procedures
- personal data will not be stored on unapproved personal devices or consumer cloud services
- staff will use approved secure methods when sending sensitive information
- security patches, backups, malware protection and access reviews will be maintained through the school/organisation's IT arrangements

- staff will report phishing, misdirected emails, lost devices and other suspected incidents immediately

Filtering and monitoring systems will be operated lawfully, proportionately and transparently. Access to monitoring information will be restricted to authorised, appropriately trained staff. The school will document what is monitored, why, who can access alerts/reports and how long the information is retained. A DPIA will be undertaken before introducing a new system or making significant changes where required.

18. Retention, disposal and records management

The school will maintain and apply a records-retention schedule. Personal data will be retained only for as long as necessary for the documented purpose, legal obligations, safeguarding requirements and legitimate organisational needs. The school will review its holdings at least annually and securely dispose of information no longer required. Paper records will be confidentially destroyed and electronic records securely deleted or anonymised using appropriate methods.

19. International transfers

Personal data will only be transferred outside the UK where the transfer is lawful. The controller will use an applicable adequacy regulation, approved safeguard or statutory exception and will complete any required transfer risk assessment/data protection test. Cloud and EdTech procurement will identify data locations and onward transfers before approval.

20. Personal data breaches

All suspected or actual personal data breaches must be reported immediately to the DPL/DPO. Staff must not investigate privately, delete evidence or delay reporting while trying to resolve the issue themselves. The school will contain the incident, assess risk, document decisions and take remedial action.

Where a breach is likely to result in a risk to individuals' rights and freedoms, the controller will notify the ICO without undue delay and, where feasible, within 72 hours of becoming aware of it. Where a breach is likely to result in a high risk, affected individuals will also be informed without undue delay unless a lawful exception applies.

21. Training and awareness

All staff and relevant governors/proprietors will receive data protection training at induction and refresher training thereafter, with additional training following significant legal, technological or procedural change. Role-specific training will be provided to staff handling sensitive records, CCTV, SARs, safeguarding information, procurement, filtering/monitoring or data incidents. Training completion will be recorded.

22. Monitoring, assurance and review

- The DPL will support day-to-day monitoring and escalate significant issues to the DPO and Principal.
- The DPO will provide independent advice and appropriate assurance to senior leadership/proprietor/governance.
- The school will periodically audit access controls, processing records, privacy notices, retention, processor contracts, DPIAs, breaches and information-rights handling.
- This policy will be reviewed at least annually and earlier following significant changes in law, ICO/DfE guidance, school systems or processing activities.

23. Related policies and records

- Child Protection and Safeguarding Policy
- Online Safety / Acceptable Use arrangements
- CCTV arrangements
- Records Retention Schedule
- Privacy Notices
- Record of Processing Activities (ROPA)
- Data Breach Register
- DPIA Register
- Data Sharing Agreements
- Freedom of Information / Publication Scheme where applicable
- Complaints Policy
- Staff Code of Conduct and confidentiality requirements
- AI / EdTech procedures where maintained separately

Appendix A – Personal data breach procedure

1. Immediately report the suspected breach to the DPL/DPO using the school's normal urgent reporting route. If safeguarding information is involved, inform the DSL without delay.
2. Preserve evidence. Do not delete messages, wipe devices or contact recipients beyond immediate proportionate containment unless directed.
3. Contain the breach: for example, recall an email, disable a link/account, recover a device, change credentials or contact approved IT support.
4. The DPO/DPL will record what happened, when it occurred, when the controller became aware, categories/approximate numbers of people and records affected, data sensitivity and likely consequences.
5. Assess risk to individuals, including children's vulnerability, safeguarding implications, identity/fraud risk, confidentiality, discrimination, distress and loss of control over information.
6. Decide and document whether ICO notification is required. Where required, notify without undue delay and, where feasible, within 72 hours of awareness; provide further information in phases if necessary.
7. Where the breach is likely to result in high risk, inform affected individuals without undue delay in clear language, unless a lawful exception applies.
8. Notify other relevant bodies where necessary, such as police, local authority/safeguarding partners, insurers or IT/security providers, using the minimum necessary information.
9. Record every breach, including breaches not reported to the ICO, together with reasons, containment, remediation and lessons learned.
10. The DPO/DPL and Principal will review serious or recurring incidents and implement improvements to systems, contracts, training or procedures.

Email disclosure – immediate actions

- Attempt recall where technically possible, but do not assume recall has succeeded.
- Contact unintended recipients where appropriate and request secure deletion and no onward sharing.
- Ask for confirmation of deletion where proportionate.
- Escalate safeguarding information immediately to the DSL as well as the DPL/DPO.
- Consider whether cached, downloaded, forwarded or publicly indexed copies may remain and take proportionate removal steps.

Appendix B – Data protection complaint procedure

11. Receive and log the complaint. Any staff member may receive it and must forward it promptly to the DPL/DPO.
12. Acknowledge the complaint within 30 days and provide a contact point.
13. Clarify the complaint where necessary and identify the processing activity, controller and relevant records.
14. Investigate fairly, including reviewing systems, decisions, lawful bases, privacy information, staff actions and any relevant processor involvement.
15. Take corrective action where required, including rectification, access restriction, deletion where lawful, revised notices, training or procedural improvement.
16. Respond without undue delay in clear language, explaining findings and actions.
17. Tell the complainant that they may raise concerns with the Information Commissioner's Office and provide the current ICO contact/navigation information through the school's privacy notice or response.
18. Retain a record of the complaint, investigation, outcome and lessons learned in accordance with the retention schedule.

Appendix C – Staff quick-response guide

If this happens...	Do this immediately
You send personal data to the wrong person	Tell the DPL/DPO immediately; attempt safe containment; preserve evidence.
A laptop/phone/USB containing school data is lost or stolen	Report immediately to the DPL/DPO and IT; do not wait to see if it is found.
Someone asks for “all information you hold about me”	Treat as a possible SAR and forward immediately to the DPL/DPO.
A parent asks for their child’s records	Forward to the DPL/DPO; do not assume the parent is automatically entitled to every record.
Police or another agency asks for pupil information	Check authority/lawful basis and consult the DSL/DPL where appropriate; share only what is necessary.
You want to use a new app, EdTech or AI tool with pupil/staff data	Do not upload data until the system has been approved and any required DPIA/procurement checks are complete.
You receive a data protection complaint	Forward promptly to the DPL/DPO; do not dismiss or redirect the person unnecessarily.
You are unsure whether you can share information for safeguarding	Contact the DSL. Data protection law does not prevent necessary, proportionate safeguarding information sharing.

Reference framework

This policy was revised for the 2026-2027 academic year with reference to the Department for Education’s “Data protection in schools” guidance updated 9 July 2026, including its Data (Use and Access) Act 2025, CCTV/photos/video, EdTech, filtering/monitoring and records-management material, and to current Information Commissioner’s Office guidance on the Data (Use and Access) Act 2025 and data protection complaints. The school should use the current versions of those sources when applying this policy.