Central Schools Trust

INCORPORATING BALSALL COMMON PRIMARY SCHOOL AND DAMSON WOOD NURSERY AND INFANT SCHOOL

Data Protection Policy

Document Control

Date of Policy	Policy Version	Approving Body	Approval Date	Review Period
September 2022	1.2	MAT Board	4 October 2022	Autumn Term 2023
May 2023	1.2	MAT Board	23 May 2023	Summer Term 2024
June 2024	2.0	MAT Board	2 July 2024	Summer Term 2025
June 2025	2.0	MAT Board	1 July 2025	Summer Term 2026
May 2026	2.1	MAT Board	12 May 2026	Autumn Term 2027
September 2026	2.2	MAT Board	6 October 2026	Autumn Term 2027

1. Purpose and scope

This policy explains how Central Schools Trust (the Trust) protects personal data and complies with data-protection law. It applies to trustees, local governors, employees, agency staff, volunteers, contractors and others processing personal data for or on behalf of the Trust. It covers personal data in any format and on any system, whether processed on Trust premises or remotely.

The Trust is normally the controller where it determines why and how personal data is processed. In some arrangements it may act as a joint controller, processor or separate controller; the applicable role and responsibilities will be documented.

Deliberate, reckless or repeated breach of this policy may be managed under the Trust's disciplinary, capability, contractual or other appropriate procedures. Nothing in this policy prevents lawful and necessary information sharing for safeguarding or other public-interest purposes.

2. Legal and regulatory framework

The Trust will comply with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, the Data (Use and Access) Act 2025 and, where relevant, the Privacy and Electronic Communications Regulations 2003, the Protection of Freedoms Act 2012, the Freedom of Information Act 2000, the Environmental Information Regulations 2004, education legislation and statutory safeguarding duties.

The Trust will take account of current guidance from the Information Commissioner's Office (ICO), the Department for Education and other relevant regulators. Where legislation or binding guidance changes, the Trust will apply the current requirement and update this policy as soon as practicable.

3. Data-protection principles

Personal data must be:

- processed lawfully, fairly and transparently;
- collected for specified, explicit and legitimate purposes and not further processed incompatibly with those purposes;
- adequate, relevant and limited to what is necessary;
- accurate and, where necessary, kept up to date;
- kept in identifiable form for no longer than necessary;
- processed with appropriate security; and
- managed so that the Trust can demonstrate accountability.

Privacy by design and by default will be built into projects, services, procurement, systems and working practices.

4. Roles and responsibilities

Board of trustees

- Retains overall accountability for compliance and approves this policy.
- Ensures adequate resources, oversight and assurance arrangements.
- Receives reports on significant risks, breaches, complaints, audit findings and improvement plans.

Data Protection Officer

The Trust will appoint a suitably qualified DPO, publish their contact details and notify the ICO. (Insert DPO name and contact details). The DPO will act independently, report to the highest management level, advise on obligations and data protection impact assessments, monitor compliance and training, cooperate with the ICO and act as a contact point for data subjects and the regulator. The DPO will not be instructed on how to perform these tasks, penalised for doing so or placed in a conflict of interest.

Trust data protection lead and school leaders

- Coordinate operational compliance, requests, records, incidents and policy implementation.
- Consult the DPO promptly on high-risk or novel processing.
- Ensure local practices, suppliers and systems comply with this policy.

All users of personal data

- Access and use personal data only where authorised and necessary.
- Follow security, retention, sharing and incident-reporting procedures.
- Complete required training and seek advice when uncertain.

5. Lawful, fair and transparent processing

Before processing begins, the Trust will identify and document an Article 6 lawful basis. Depending on the activity, this may include legal obligation, public task, contract, vital interests, legitimate interests where available and appropriate, or consent. Consent will not be used by default and will be relied upon only where it is freely given, specific, informed, unambiguous, recorded and as easy to withdraw as to give.

Special-category data requires both an Article 6 basis and an Article 9 condition. Criminal-offence data will be processed only where lawful authority and the required condition or policy document apply. The Trust will document applicable statutory provisions and safeguards.

Privacy notices will be concise, transparent, accessible and written in clear language, including child-appropriate language where directed to pupils. They will explain the controller, DPO contact, purposes, lawful bases, recipients, retention, rights, complaint routes, international transfers and any relevant automated decision-making. Where data is obtained indirectly, the Trust will provide the required information within the applicable period unless a lawful exemption applies.

6. Purpose limitation, minimisation and accuracy

Personal data will be collected for defined purposes and will not be reused incompatibly. Before further processing, the Trust will document compatibility, lawful basis and transparency requirements unless legislation or an exemption permits otherwise.

Forms, datasets, access rights and reports will be reviewed to remove unnecessary or excessive data. Reasonable steps will be taken to keep data accurate and to correct or qualify inaccurate data without undue delay. Individuals should tell the Trust when relevant information changes.

7. Records, retention and disposal

The Trust will maintain records of processing activities, information-asset and data-flow records, lawful-basis decisions, privacy notices, consent records where relevant, data-sharing arrangements, processor contracts, DPIAs, incidents, complaints, rights requests and training.

Personal data will be retained according to an approved retention schedule that reflects statutory, safeguarding, operational, archival and limitation requirements. The Trust may use the Solihull Metropolitan Borough Council schedule as a reference only where it is current and suitable for the Trust. Emails and messages will be retained according to their content and business value, not deleted solely because of format or age. Legal holds, investigations and anticipated claims suspend routine deletion where necessary.

At the end of the retention period, data will be securely deleted, anonymised or transferred to an archive where lawful. Disposal methods will be appropriate to the medium and verified where required.

8. Data protection impact assessments

A data protection impact assessment (DPIA) must be completed before processing likely to result in a high risk to people's rights and freedoms. This includes relevant large-scale special-category processing, systematic monitoring, automated evaluation, innovative technology, biometric recognition and other high-risk processing identified by the ICO or DPO.

The DPIA will describe the processing, assess necessity and proportionality, identify risks, record mitigations and consult affected people where appropriate. The DPO will advise on the DPIA. The Trust will consult the ICO before processing where a high residual risk cannot be reduced adequately.

9. Information security

The Trust will use technical and organisational measures proportionate to risk, including role-based access, least privilege, strong authentication, multi-factor authentication where appropriate, encryption, secure configuration, supported software, patching, malware protection, logging, monitoring, tested backups, restoration, business continuity and secure disposal.

Portable devices and removable media containing personal data must be authorised and encrypted. Personal data taken off site must be limited to what is necessary, protected in transit

and storage, and never left unattended. Personal email, unapproved cloud services and unapproved removable media must not be used for Trust personal data.

Recipients and attachments must be checked before messages are sent. Sensitive data will use approved secure transfer methods. Staff must follow clear-desk, secure-printing, identity-verification, remote-working and physical-security procedures.

Access will be reviewed regularly and removed promptly when no longer needed. Security measures will be tested and reviewed, including after significant change or incident. Staff will receive data-protection and security training on induction, at least every two years and more frequently where risk or role requires; annual refreshers are the Trust's expected practice.

10. Data sharing

Personal data will be shared only where lawful, necessary, proportionate and secure. The Trust will verify the recipient, purpose, lawful basis, minimum data required and any restriction or duty of confidence. Routine or high-risk sharing arrangements will be documented in an agreement or protocol where appropriate.

Safeguarding information will be shared promptly where necessary to protect a child or another person. Data-protection law does not prevent justified safeguarding sharing. Staff will record significant decisions to share or withhold information and seek advice where practicable, without delaying urgent action.

11. Processors and procurement

Before appointing a processor, the Trust will undertake proportionate due diligence covering security, resilience, location, subprocessors, retention, deletion, incident handling and rights support. Processing must be governed by a written contract meeting Article 28 UK GDPR, including documented instructions, confidentiality, security, subprocessor controls, assistance, end-of-contract return or deletion, and audit or inspection rights.

The Trust will maintain a supplier and contract register and review processor assurance throughout the contract. Processors must notify the Trust of personal-data breaches without undue delay and must not change processing materially without authorisation.

12. International transfers

A restricted transfer of personal data outside the UK will occur only where permitted by UK data-protection law. The Trust will document the transfer, destination, recipients and lawful safeguard. Safeguards may include UK adequacy regulations, the International Data Transfer Agreement, the UK Addendum or another approved mechanism, with any required transfer risk assessment or data-protection test and supplementary measures.

Derogations, including explicit consent, will be used only exceptionally and where all legal conditions are met. Cloud hosting, remote support and supplier access will be assessed as potential transfers.

13. Individual rights

Subject to legal conditions and exemptions, individuals may have rights to be informed; access their personal data; rectify inaccurate data; erase data; restrict processing; receive portable data; object to processing; withdraw consent; and obtain safeguards concerning solely automated decisions with legal or similarly significant effects.

Requests may be verbal or written and need not use legal terminology. Staff must forward them immediately to the designated team. The Trust will verify identity proportionately, assist the requester where needed, search relevant systems, apply exemptions carefully, protect third-party rights and disclose securely.

The Trust will respond without undue delay and normally within one month. Where permitted, the period may be extended by up to two further months for complexity or multiple requests, with notice and reasons within the first month. A lawful pause or clarification mechanism will be used only where current legislation permits. Manifestly unfounded or excessive requests may be refused or charged for only in accordance with the law and with reasons and complaint rights.

A child's ability to exercise rights will be assessed according to understanding and competence, not a fixed age. A person with parental responsibility has no automatic right to all of a child's personal data. Requests on a child's behalf will be handled in the child's best interests, with safeguarding, confidence and applicable education-record rights considered.

14. Personal-data breaches

Any suspected loss, unauthorised access, disclosure, alteration, destruction, cyber incident or misdirection involving personal data must be reported immediately through the Trust's incident route. Staff must preserve evidence, follow containment instructions and must not conceal or investigate an incident independently.

The Trust will contain and investigate the incident, record the facts, assess risk to rights and freedoms, document the decision and take remedial action. Processors must notify the Trust without undue delay. Where required, the Trust will notify the ICO without undue delay and, where feasible, within 72 hours of becoming aware. Where a breach is likely to result in a high risk, affected people will be informed without undue delay unless a lawful exception applies.

The DPO and senior leaders will review trends and lessons learned. Every breach will be recorded, whether or not it is notified externally.

15. Complaints

Any person may complain about the Trust's use of personal data through the published data-protection complaint route. The Trust will make the process easy to use, acknowledge a complaint within 30 days, investigate without undue delay, keep the complainant informed where appropriate and provide an outcome explaining findings, action and the right to complain to the ICO.

Complaints may also be made directly to the ICO. The Trust will cooperate with the regulator and will not penalise anyone for raising a concern in good faith.

16. School-specific processing

Photographs, recordings and publications

The Trust will identify the purpose and lawful basis for photographs and recordings. Consent will be sought where it is the appropriate basis, including separate, specific choices for materially different optional uses such as external publicity or public social media. Refusal or withdrawal will be respected without detriment, subject to images already lawfully published and reasonable steps to cease future use.

Displays and publications will use the minimum identifying information necessary. Safeguarding concerns, court orders and individual risk assessments will take priority.

Performances and events

Personal or household recording by families may fall outside data-protection law, but the Trust may impose proportionate safeguarding, copyright, venue and privacy conditions. Families will be asked not to publish identifiable images of other children without appropriate authority.

CCTV

CCTV will be used only for documented, necessary and proportionate security, safety or crime-prevention purposes. The Trust will identify the lawful basis, provide clear signage and privacy information, restrict and log access, respond to lawful requests, review camera locations and complete a DPIA where required. Cameras will not be placed where people reasonably expect a high degree of privacy.

Footage will normally be retained for no longer than 30 days unless an incident, request, investigation or legal requirement justifies longer retention. The Trust will periodically verify that this period remains necessary and proportionate.

Automated biometric recognition

Before using pupil biometric recognition, the Trust will complete a DPIA, identify an Article 6 basis and Article 9 condition, assess the supplier and security, explain use and retention, and provide a reasonable non-biometric alternative.

For a pupil under 18, the Trust will notify each parent and obtain written consent from at least one parent. Processing will not begin or continue if a parent objects or withdraws consent. A pupil may object or refuse at any time regardless of age or capacity, and will not be disadvantaged for choosing the alternative. Biometric templates will be securely deleted when no longer required.

Online services, cookies and direct marketing

The Trust will comply with relevant electronic-communications rules when using non-essential cookies, electronic marketing or similar technologies. School communications necessary for

education, safeguarding or administration will be distinguished from optional promotional communications.

Artificial intelligence and automated decisions

AI tools must not be used with personal data unless approved. Approval will consider lawful basis, transparency, accuracy, bias, security, supplier reuse, international transfers, retention, human oversight, children's rights and the need for a DPIA. No solely automated decision with legal or similarly significant effects will be made unless lawful safeguards are in place.

17. Review, assurance and contacts

The Trust will monitor compliance through audits, spot checks, training records, processor reviews, incident analysis, request logs and reporting to trustees. This policy will be reviewed at least annually and after significant legislative, regulatory, organisational or technological change.

Questions, requests, incidents and complaints should be sent to the Trust's published data-protection contact. (Insert DPO details)