

Data Protection

Approved by: Trust Board

Last reviewed: July 2026

Next review due: July 2027

DATA PROTECTION

Scope

This policy is written and approved at board level, but applies to all members, trustees, governors and employees of schools, settings, and services, hereafter the 'organisations,' within The Claxton Trust.

It has been created using a model policy created by The Key and has therefore been produced in consultation with external advisors and the professional associations/trade unions.

1. Aims

Our schools, settings and services aim to ensure that all personal data collected about staff, pupils, parents and carers, governors, visitors, and other individuals is collected, stored, and processed in accordance with UK data protection law.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This policy meets the requirements of the:

- UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by [The Data Protection, Privacy and Electronic Communications \(Amendments etc.\) \(EU Exit\) Regulations 2020](#)
- [Data Protection Act 2018 \(DPA 2018\)](#)

It is based on guidance published by the Information Commissioner's Office (ICO) on the [UK GDPR](#) and guidance from the Department for Education (DfE) on [Generative artificial intelligence in education](#).

It meets the requirements of the [Protection of Freedoms Act 2012](#) when referring to our use of biometric data.

It also reflects the ICO's [guidance](#) for the use of surveillance cameras and personal information.

In addition, this policy complies with our funding agreement and articles of association.

3. Definitions

TERM	DEFINITION
Personal data	Any information relating to an identified, or identifiable, living individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural, or social identity.

TERM	DEFINITION
Special categories of personal data	Personal data, which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina, and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing, or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed
Controller	A person or organisation that determines the purposes and the means of processing personal data.
Processor	A person or other body, other than an employee of the controller, who processes personal data on behalf of the controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

4. The controller

Our trust processes personal data relating to parents and carers, pupils, staff, governors, visitors, and others, and therefore is a controller.

The school is registered with the ICO and has paid its data protection fee to the ICO, as legally required.

5. Roles and responsibilities

This policy applies to **all employees of the trust**, and to external organisations or individuals working on our behalf, including volunteers. Employees who do not comply with this policy may face disciplinary action.

5.1 Trust board

The trust board has overall responsibility for ensuring that its schools, settings, and services comply with all relevant data protection obligations.

5.2 Local governing body

The local governing body has delegated local responsibility for ensuring that school complies with all relevant data protection obligations.

5.3 Data protection officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

Our DPO is Catherine Preston and is contactable via dpo@claxtontrust.org.uk

The DPO will:

- Advise the trust and its employees of their obligations under relevant UK data protection laws, including the UK GDPR
- Monitor compliance with UK data protection law, by:
 - Collecting information to identify data processing activities
 - Analysing and checking the compliance of data processing activities
 - Informing, advising, and issuing recommendations to the school
- Ensure the school's policies are followed within the school, by:
 - Assigning responsibilities to staff members
 - Raising awareness of UK data protection law, including the UK GDPR, across the school
 - Training staff
 - Conducting internal audits
 - Reporting to the governing board or the board of trustees on the school's data protection compliance
- Advise on and assist the school with carrying out data protection impact assessments (but not carry out impact assessments themselves)
- Act as a contact point for the Information Commissioner's Office (ICO) (as the 'supervisory authority'), involving:
 - Helping the ICO to access documents and information
 - Seeking advice on data protection issues
- Act as a contact point for individuals whose data is processed (staff, pupils, and parents, for example)
- Take a risk-based approach to data protection, involving:
 - Prioritising the higher-risk areas of data protection and focusing on these the most
 - Using their common sense to advise the school on whether it should conduct an audit, provide training in certain areas, and determine what the DPO should spend the most time doing

5.4 Headteacher

The headteacher acts as the representative of the controller on a day-to-day basis.

5.5 All employees

Employees are responsible for:

- Collecting, storing, and processing any personal data in accordance with this policy
 - Informing the school of any changes to their personal data, such as a change of address
 - Contacting the DPO in the following circumstances:
 - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
 - If they have any concerns that this policy is not being followed
- If they are unsure whether they have a lawful basis to use personal data in a particular way
- If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the UK
 - If there has been a data breach
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals
 - If they need help with any contracts or sharing personal data with third parties

6. Data protection principles

The UK GDPR is based on data protection principles that our school must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the school aims to comply with these principles.

7. Collecting personal data

7.1 Lawfulness, fairness, and transparency

We will only process personal data where we have 1 of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering a contract
- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual or another person i.e. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can **perform a task in the public interest or exercise its official authority**
- The data needs to be processed for the **legitimate interests** of the school (where the processing is not for any tasks the school performs as a public authority) or a third party, provided the individual's rights and freedoms are not overridden
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**
- Certain processing activities may rely on **Recognised Legitimate Interests** as defined in the Data (Use and Access) Act 2025.

For special categories of personal data, we will also meet 1 of the special category conditions for processing under data protection law:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **explicit consent**
- The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security, or social protection law**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for the establishment, exercise, or defence of **legal claims**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation
- The data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **archiving** purposes, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **consent**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual

- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise, or defence of **legal rights**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not expect or use personal data in ways which have unjustified adverse effects on them.

7.2 Limitation, minimisation, and accuracy

We will only collect personal data for specified, explicit, and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary.

Staff must only process personal data where it is necessary to do their jobs.

We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.

In addition, when staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's record retention schedule.

7.3 Children's Privacy and EdTech

We comply with the **Age Appropriate Design Code** and ensure EdTech providers meet UK GDPR standards.

Profiling or targeted advertising using children's data is prohibited.

8. Sharing personal data

There are certain circumstances where we may be required to share personal data without consent. These include, but are not limited to, situations where:

- There is an issue with a pupil or parent/carer that puts the safety of our employees at risk
- We need to liaise with other agencies for safeguarding reasons.
- Our suppliers or contractors need data to enable us to provide services to our employees and pupils – for example, IT companies. When doing this, we will:
 - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
 - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
 - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so.

We may also share personal data with emergency services and local authorities to help them to respond to an emergency that affects any of our pupils or employees.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

9. Subject access requests and other rights of individuals

9.1 Subject Access Requests (SARs)

Individuals have the right to request access to personal information we hold about them. This includes confirmation of processing, access to data, and related details.

When responding to SARs, we will:

- Accept requests in any format, but encourage written requests for clarity.
- Verify identity using two forms of identification where appropriate.
- Respond without undue delay and within **one month**, unless the request is complex or numerous, in which case we may extend by up to **two months** and will inform the requester within the first month.
- Provide information free of charge unless the request is manifestly unfounded or excessive.
- Apply the following provisions under the **Data (Use and Access) Act 2025**:
 - We may **pause the response timeframe ("stop the clock")** while awaiting clarification from the requester.
 - Searches will be **reasonable and proportionate**; we are not required to provide information already accessible to the requester.

9.2 Children and SARs

Personal data about a child belongs to the child. Requests from parents/carers will be considered based on the child's capacity to understand their rights, judged case by case. Children aged 12 and above are generally considered mature enough to consent.

9.3 Complaints Process

Before escalating to the ICO, individuals should use our **internal complaints procedure** for data protection concerns. Details are available in our Complaints Policy.

10. Parental requests to see the educational record

As we operate within a multi-academy trust, there is no automatic parental right of access to the educational record in our schools, settings, or services.

Such requests must be made by following our normal subject access request process.

11. Biometric recognition systems

Where we use pupils' biometric data as part of an automated biometric recognition system, we will comply with the requirements of the [Protection of Freedoms Act 2012](#).

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent from at least 1 parent or carer before we take any biometric data from their child and first process it.

Parents/carers and pupils have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils.

Parents/carers and pupils can withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

Where staff members or other adults use the school's biometric system(s), we will also obtain their consent before they first take part in it and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

12. CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will follow the [ICO's guidance](#) for the use of CCTV, and comply with data protection principles.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to the headteacher/manager in each school, setting or service, whose name will be published on their website.

13. Photographs and videos

Photographs & videos taken by the school

The school may capture photographs and videos of children and adults for legitimate school activities, including:

- **Internal Use:** display boards, children's learning records, and other educational and safeguarding purposes within the school premises.
- **External Use:** official school website and social media platforms

All photographs and videos will be taken using school-owned equipment and will be stored securely on our school network, in line with our data retention schedule.

All photographs and videos which are used externally will not be accompanied by any personally identifiable information to protect individuals' privacy.

Where we are aware of child protection relating to the identification of some children in our school, we will not use photographs or videos of these children externally.

We work on the assumption that we have permission to use the information in this way, as these are fundamental school activities which enable us to deliver a good standard of education and to keep children safe. However, permission may be withdrawn for some specific uses at any time by submitting a written request to the school office. Upon withdrawal, all relevant photographs and videos will be deleted, and we will discontinue using them for the specific purpose identified.

We reserve the right to refuse to comply with requests for withdrawal where this would significantly compromise our ability to deliver a good standard of education or keeping children safe.

Photographs & videos taken by a school photographer

Routinely, the school employs a third party photographer to take individual, class or family photographs or videos of children, either for parents/carers to purchase or for school use. We will always inform parents/carers that photographs are going to be taken in advance. If a parent/carer wants to withdraw permission, they must confirm this in writing to the school office.

Photographs & videos taken by, or for, external agencies

For photographs and videos taken by or for external agencies, explicit written consent will be obtained in advance from parents/carers of children under 18, or directly from pupils aged 18 and over. Examples include:

- individual and family photographs taken by the school photographer
- photographs / videos to be used in local or national newspapers.
- photographs / videos taken for commercial, marketing, or promotional uses by external agencies, such as lettings companies or sports clubs.

We will provide clear and detailed information in advance to parents/carers and pupils regarding the intended use of these photographs and/or videos.

Photographs & videos taken by parents/carers at school events

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation.

However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons.

14. Artificial intelligence (AI)

Artificial Intelligence (AI) tools can support learning but pose risks to privacy and data security. To comply with DfE guidance and UK GDPR:

- **Personal or sensitive data must never be entered into unauthorised generative AI tools or chatbots.**
- All AI use must be **risk assessed** and approved by the Data Protection Officer (DPO).
- Staff must complete **training on safe and ethical AI use**.
- AI systems must be transparent, avoid bias, and comply with the **Age Appropriate Design Code** for children's data.
- Any breach involving AI will be treated as a personal data breach under Appendix 1.

15. Automated Decision-Making (ADM) and Profiling

Where decisions are made solely by automated means:

- Individuals will be informed when such processing occurs.
- They have the right to request **human review** and to challenge decisions.
- ADM will only be used where a lawful basis applies and safeguards are in place.

16. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing data protection impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws may apply
- Maintaining records of our processing activities, including:
 - For the benefit of data subjects, making available the name and contact details of our school and DPO, and all information we are required to share about how we use and process their personal data (via our privacy notices)

- For all personal data that we hold, maintaining an internal record of the type of data, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the UK and the safeguards for those, retention periods and how we are keeping the data secure.

16. Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data, are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Passwords that are at least 10 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded that they should not reuse passwords from other sites
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our online safety policy, computing policy / acceptable use agreement)
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

17. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

18. Personal data breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

19. Training

All staff and governors are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

Training will include updates on DUAA 2025, AI governance, and SAR handling.

20. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed annually and approved by the full governing board.

21. Links with other policies

This data protection policy is directly linked to the following policies held at trust level:

- Complaints Policy
- Complaints Procedure
- Disciplinary
- Risk Management
- Safer Recruitment & Selection
- Safeguarding
- Whistleblowing

Appendix 1: Personal data breach procedure

This procedure is based on [guidance on personal data breaches](#) produced by the Information Commissioner's Office (ICO).

- On finding or causing a breach or potential breach, the staff member, governor or 'data processor' must immediately notify the data protection officer (DPO) by emailing dpo@claxtontrust.org.uk
- The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
 - Lost
 - Stolen
 - Destroyed
 - Altered
 - Disclosed or made available where it should not have been
 - Made available to unauthorised people
- Staff and governors will co-operate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation
- If a breach has occurred or it is likely that is the case, the DPO will alert the headteacher and the chair of governors
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or processors should help the DPO with this where necessary, and the DPO should take external advice when required (e.g. from IT providers). (See the actions relevant to specific data types at the end of this procedure)
- The DPO will assess the potential consequences (based on how serious they are and how likely they are to happen) before and after the implementation of steps to mitigate the consequences
- The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's [self-assessment tool](#)
- The DPO will document the decisions (either way), in case the decisions are challenged later by the ICO or an individual affected by the breach. Documented decisions are stored on the DPO shared drive.
- Where the ICO must be notified, the DPO will do this via the ['report a breach' page](#) of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of the school's awareness of the breach. As required, the DPO will set out:
 - A description of the nature of the personal data breach including, where possible:
 - The categories and approximate number of individuals concerned
 - The categories and approximate number of personal data records concerned
 - The name and contact details of the DPO
 - A description of the likely consequences of the personal data breach
 - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours of the school's awareness of the breach. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- Where the school is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:
 - A description, in clear and plain language, of the nature of the personal data breach
 - The name and contact details of the DPO

- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will decide, considering the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
 - Facts and cause
 - Effects
 - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored on the DPO shared drive.

- The DPO and headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible
- The DPO and headteacher will meet termly to assess recorded data breaches and identify any trends or patterns requiring action by the school to reduce risks of future breaches

Actions to minimise the impact of data breaches

We set out below the steps we might take to try and mitigate the impact of different types of data breach if they were to occur, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the [ICT department/external IT support provider] to attempt to recall it from external recipients and remove it from the school's email system (retaining a copy if required as evidence)
- In any cases where the recall is unsuccessful or cannot be confirmed as successful, the DPO will consider whether it's appropriate to contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The DPO will endeavour to obtain a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

If safeguarding information is compromised, the DPO will inform the designated safeguarding lead and discuss whether the school should inform any, or all, of its 3 local safeguarding partners