Data Protection Policy

Date of Approval: 12/09/2025
Signed: Ruth Minhall

Position: CEO and Head of Centre

Next review: 01/09/2027
Last reviewed: 11 September 2026

1. Aims

Our education service aims to ensure that all personal data collected about staff, pupils, parents and carers, Executive Board members, 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.

Tuition Extra (Kent) Ltd provides specialist tuition to over 300 children and young people, the majority of whom have Special Educational Needs and Disabilities (SEND), supported by approximately 150 tutors. We hold significant volumes of special category, safeguarding and EHCP data relating to children. This policy is written on the basis that a data protection failure in our setting is also a safeguarding matter.

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)
- Data (Use and Access) Act 2025 (DUAA), which amends both the UK GDPR and the Data Protection Act 2018. The final provisions commenced during 2026 and are reflected throughout this policy.

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 also reflects the ICO's guidance for the use of surveillance cameras and personal information, and the DfE Digital and Technology Standards and Keeping Children Safe in Education 2026.

The Education (Pupil Information) (England) Regulations 2005, which create a right of access to a pupil's educational record, apply to maintained schools. They do not apply to Tuition Extra (Kent) Ltd as an independent provider. See section 10.

This policy complies with our articles of association and with the terms of our commissioning arrangements with Kent County Council and other local authorities. We do not hold a DfE funding agreement.

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, or an 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.
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; and sex life or sexual orientation.
Criminal offence data	Personal data relating to criminal convictions and offences or related security measures, including data relating to the alleged commission of an offence and to proceedings for an offence.
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.
Data controller	A person or organisation that determines the purposes and the means of processing personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data 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 data controller

Our Educational Service (Service) processes personal data relating to parents and carers, pupils, staff, visitors and others, and therefore is a data controller. The data controller is Tuition Extra (Kent) Ltd, a private limited company registered in England and Wales, of 8 Roper Yard, Roper Road, Canterbury, CT2 7EX. The Service is not a public authority for the purposes of the UK GDPR, the Data Protection Act 2018 or the Freedom of Information Act 2000.

The Education Service has paid its data protection fee to the ICO, as legally required.

Where we determine the purposes and means of processing jointly with another party, we will establish a written joint controller arrangement. Where we process personal data on behalf of another organisation, we act as a processor and will do so only under a written Article 28 agreement.

5. Roles and responsibilities

This policy applies to **all staff** employed by our Service, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action. It also applies to tutors, contractors, agency workers, volunteers and Executive Board members.

5.1 Data protection officer (DPO)

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 CEO and, where relevant, report to the CEO their advice and recommendations on data protection issues.

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

Full details of the DPO's responsibilities are set out in their job description.

Our DPO is Jean-Paul Muller and is contactable via jean-paul.muller@tuition-extra.co.uk

The DPO reports directly to the CEO, is not dismissed or penalised for performing their tasks, and is given the resources and access necessary to carry out the role independently.

5.2 DPO independence and conflict of interest

Article 38(6) of the UK GDPR permits a DPO to hold other roles, but requires the controller to ensure those roles do not give rise to a conflict of interest. A DPO must not determine the purposes and means of processing in an area they are then required to advise on and monitor independently.

Jean-Paul Muller currently holds the Data Protection Officer role. The Executive Board must ensure that the DPO's other responsibilities do not give rise to a conflict of interest under Article 38(6) of the UK GDPR. This assessment should be completed, recorded and reviewed if role responsibilities change.

5.3 Head of Service

The Head of Service acts as the representative of the data controller on a day-to-day basis.

The CEO holds overall accountability for compliance with data protection law. The Executive Board receives the DPO's annual report, approves this policy, and satisfies itself that data protection risk is being managed.

5.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the Service of any changes to their personal data, such as a change of address
- Completing data protection training before being given access to personal data, and annually thereafter
- Recognising a data protection request or complaint in whatever form it arrives, including verbally, and forwarding it to the DPO immediately
- 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 or not 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 Service 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 Service aims to comply with these principles. In addition, the Service is responsible for, and must be able to demonstrate, compliance with these principles — the accountability principle.

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 Service can **fulfil a contract** with the individual, or the individual has asked the Service to take specific steps before entering into a contract
- The data needs to be processed so that the Service 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 **public task** basis is not available to the Service. Tuition Extra (Kent) Ltd is a private limited company, is not a public authority, and does not exercise official authority conferred by law. We do not rely on Article 6(1)(e)
- The data needs to be processed for the **legitimate interests** of the Service or a third party, provided the individual’s rights and freedoms are not overridden. Where we rely on legitimate interests we complete and retain a written Legitimate Interests Assessment covering the purpose, necessity and balancing tests, reviewed by the DPO
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

Where we rely on legitimate interests, individuals have the right to object under Article 21 of the UK GDPR. We will stop the processing unless we can demonstrate compelling legitimate grounds which override the individual’s interests, rights and freedoms. Each objection is considered on its merits, with DPO advice, and the decision is recorded.

The Data (Use and Access) Act 2025 also introduced a list of recognised legitimate interests, including safeguarding vulnerable individuals, for which the balancing test does not need to be carried out. Where we rely on a recognised legitimate interest we will record which one applies.

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

7.2 Appropriate Policy Document

Several of the conditions in Schedule 1 to the Data Protection Act 2018 — including safeguarding of children and of individuals at risk, preventing or detecting unlawful acts, and protecting the public — may only be relied on where the controller has an Appropriate Policy Document in place. That document must explain our procedures for complying with the data protection principles and our policies on retention and erasure of the data concerned, and must be retained while the processing continues and for six months afterwards.

The Service maintains an Appropriate Policy Document covering CCTV. An equivalent document is required covering our wider processing of special category and criminal offence data — including SEND, EHCP, health, safeguarding and DBS data. Producing it is recorded as an outstanding action at section 21.

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 reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

Because the majority of our data subjects are children with SEND, we take particular care that our processing is fair to people who may not be able to understand a privacy notice or to exercise their rights unaided. Transparency information is produced in accessible, age-appropriate formats, and the Data (Use and Access) Act 2025 requirement to take account of children's higher protection matters is applied whenever we design or change a processing activity.

7.3 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 in order 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 Service's record retention schedule. The Service does not currently hold a formal record retention schedule. Producing one, covering pupil, staff, safeguarding, financial and CCTV records, is recorded as an outstanding action at section 21. Until it is in place, staff must seek the DPO's advice before deleting any record.

8. Sharing personal data

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. 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 staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors that can provide sufficient guarantees that they comply with UK data protection law
    - Establish a contract with the supplier or contractor 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
    - Put in place a written contract meeting the requirements of Article 28 of the UK GDPR before any processing begins, and record the supplier, the data involved, the retention applied, any sub-processors and the location of the data

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 situation that affects any of our pupils or staff.

Safeguarding information sharing. Data protection law does not prevent the sharing of information for the purposes of keeping children safe. Where there is a safeguarding concern, staff must not delay sharing information with the Designated Safeguarding Lead or, where appropriate, with children's social care or the police, out of concern about data protection. Fears about sharing

information must never be allowed to stand in the way of safeguarding a child. This is handled under the Child Protection and Safeguarding Policy.

Routine sharing with Kent County Council and other commissioners is governed by our commissioning arrangements and, where appropriate, a written data sharing agreement. The DPO maintains a record of these arrangements.

Where we transfer personal data internationally, we will do so in accordance with UK data protection law. This means relying on UK adequacy regulations where they apply, or otherwise putting in place an appropriate safeguard such as the International Data Transfer Agreement or the UK Addendum to the EU Standard Contractual Clauses, supported by a transfer risk assessment. The DPO must be consulted before any personal data is transferred outside the UK, including where a supplier stores or accesses data overseas.

9. Subject access requests and other rights of individuals

9.1 Subject access requests

Individuals have a right to make a ‘subject access request’ to gain access to personal information that the Service holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn’t possible, the criteria used to determine this period
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- The right to lodge a complaint with the ICO or another supervisory authority
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual
- The safeguards provided if the data is being transferred internationally

Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request in any form, they must immediately forward it to the DPO.

A request may be made verbally or in writing, to any member of staff, and need not mention data protection or use any particular wording. All staff are trained to recognise a subject access request and to pass it to the DPO the same day. The Service must carry out a reasonable and proportionate search for the information requested, as provided by Article 15(1A) of the UK GDPR, inserted by the Data (Use and Access) Act 2025.

9.2 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable

to understand their rights and the implications of a subject access request or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our Service may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our Service may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Age is an indicator of maturity, not a test. Because the majority of our pupils have SEND, a child's actual level of understanding may differ significantly from what their age would suggest, in either direction. Each assessment is made individually, with the DPO's advice and, where appropriate, input from the Designated Safeguarding Lead or SENDCo, and the reasoning is recorded.

9.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide proof of identity, where we have genuine doubt about who they are. We will only ask for what is reasonable and proportionate to confirm identity, and will not use identity checks to delay a response
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant)
- May pause the response period where we reasonably need the individual to confirm their identity or to clarify what they are asking for. The clock stops from the date we ask until the date we receive what we need, as provided by the Data (Use and Access) Act 2025
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We may not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent, and it would be unreasonable to proceed without it
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts. The Data (Use and Access) Act 2025 provides an express exemption for information in respect of which a claim to legal professional privilege could be maintained

If the request is unfounded or excessive, we may refuse to act on it or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

When we refuse a request, we will tell the individual why and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts. Any refusal requires the DPO's advice and the reasons are recorded.

9.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing that has been justified on the basis of legitimate interests
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
- Be notified of a data breach (in certain circumstances)
- Make a complaint to the ICO
- Complain directly to the Service about how we have handled their personal data, under section 164A of the Data Protection Act 2018 as inserted by the Data (Use and Access) Act 2025 (see section 9.5)
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

9.5 Complaints to the Service

Individuals have a statutory right to complain directly to the Service about our handling of their personal data. A complaint may be made by any reasonable means, including verbally, in writing or in person, and need not use any particular wording or cite any legislation. Complaints should be directed to the Data Protection Officer, Jean-Paul Muller, at jean-paul.muller@tuition-extra.co.uk.

Where we receive such a complaint we will acknowledge receipt within 30 days, take appropriate steps to investigate it, and respond without undue delay, keeping the complainant informed of progress and notifying them of the outcome. Complaints from children will be handled in clear, age-appropriate language and with support where needed. The DPO maintains a record of all data protection complaints and their outcomes, and reports on them annually to the Executive Board. Individuals retain the right to complain to the ICO at any time, and we will tell them how to do so.

10. Parental requests to see the educational record

The statutory right of access to a pupil's educational record under the Education (Pupil Information) (England) Regulations 2005 applies to maintained schools. It does not apply to Tuition Extra (Kent) Ltd, which is an independent provider. We therefore do not operate a separate educational record request process, and the 15 school day timescale does not apply to us.

Parents and carers who wish to see information we hold about their child should make a subject access request under section 9. That route is free of charge, must be answered within one calendar month, and is subject to the considerations at section 9.2 about whether the child is able to exercise the right themselves.

Where a child is able to understand their rights, the data belongs to them and a parent may only make a request with the child's consent.

The exemptions at section 9.3 apply, including where releasing information might cause serious harm to the physical or mental health of the pupil or another individual, or would reveal that a child is being or has been abused where disclosure would not be in the child's best interests.

11. CCTV

We use CCTV in various locations around the Service's 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.

CCTV is processed on the basis of our legitimate interests under Article 6(1)(f), supported by a written Legitimate Interests Assessment. Where footage constitutes special category or criminal offence data we rely on Article 9(2)(g) together with the relevant conditions in Schedule 1 to the Data Protection Act 2018, supported by an Appropriate Policy Document. A Data Protection Impact Assessment is maintained for the system. Footage is retained for 30 days and then overwritten automatically unless retained for a specific, authorised purpose. Audio is not recorded.

Any enquiries about the CCTV system should be directed to Jean-Paul Muller, Head of Systems and Processes. Full detail is set out in the CCTV Policy, which takes precedence in the event of any inconsistency with this section.

12. Photographs and videos

As part of our Service activities, we may take photographs and record images of individuals within our Service.

We will obtain written consent from parents/carers, or pupils aged 18 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and the pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used. Where a pupil under 18 is able to understand the decision, we will also seek the pupil's own agreement, and we will not use an image where the pupil objects even if a parent has consented.

Any photographs and videos taken by parents/carers at Service 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, unless all the relevant parents/carers (or pupils where appropriate) have agreed to this.

Where the Service takes photographs and videos, uses may include:

- Within Service on notice boards and in Service magazines, brochures, newsletters, etc.
- Outside of Service by external agencies such as the Service photographer, newspapers, campaigns
- Online on our Service website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

Consent records are maintained and reviewed at least annually so that we can evidence, for any image in use, that valid consent was given and has not been withdrawn. Images of children subject to a safeguarding or custody concern are not used externally.

13. Artificial intelligence (AI)

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT , Microsoft Copilot and Google Gemini. Tuition Extra recognises that AI has many uses to help pupils learn but also poses risks to sensitive and personal data.

To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots.

If personal and/or sensitive data is entered into an unauthorised generative AI tool, Tuition Extra will treat this as a data breach and will follow the personal data breach procedure outlined in appendix 1.

The Service maintains an AI Governance Framework and an AI Acceptable Use Policy, which take precedence in the event of any inconsistency with this section. In summary:

- AI tools may only be used where they appear on the AI Tools Register as approved for that purpose, including AI features switched on within existing products.
- A lawful basis must be identified before any personal data is processed by an AI tool, and an Article 9 condition where special category data is involved.
- A Data Protection Impact Assessment is mandatory before deploying any high-risk AI use case.
- Supplier due diligence must confirm data location, retention, sub-processors and, critically, whether inputs are used to train the provider’s models.
- A named human remains accountable for any output, decision or communication informed by AI. AI must never be the decision-maker for a safeguarding action, a risk or referral decision, a recruitment, performance or disciplinary outcome, or a final pupil report issued without human review.
- Privacy notices are updated to reflect any material AI processing, and individuals are informed where AI meaningfully affects them.

14. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of 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 Service’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). A DPIA is always required for large scale processing of special category data, for systematic monitoring of a publicly accessible area, and for processing concerning vulnerable data subjects including children — all of which apply to us. Where a DPIA identifies a high residual risk that we cannot mitigate, we must consult the ICO before the processing begins

- 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 service 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

The record of processing activities (ROPA) is owned by the DPO, held on SharePoint, and reviewed at least annually and whenever a new processing activity, system or supplier is introduced. A data protection audit is carried out annually and reported to the Executive Board.

15. 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 service office
- Passwords follow the NCSC “three random words” approach and the requirements of the Cyber Security Policy. Passwords must not be reused between work and personal accounts, must not be shared, and must be stored in the approved password manager. Multi-factor authentication is mandatory on every system and cloud service that offers it, and on all remote access
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff or pupils who store personal information on their personal devices are expected to follow the same security procedures as for service-owned equipment (see our 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)
- Access to personal data is granted on a role basis and on the principle of least privilege, is reviewed at least termly, and is removed promptly when a person leaves or changes role

The technical and organisational measures required by Article 32 of the UK GDPR are set out in full in the Cyber Security Policy and are assessed annually in the Cyber Security Risk Assessment. That policy takes precedence in the event of any inconsistency with this section.

16. 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 Service's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

Electronic devices and media are securely wiped or physically destroyed before disposal or reuse, and a record of disposal — including any destruction certificate provided by a third party — is retained. Disposal is carried out in accordance with the record retention schedule once that is in place.

17. Personal data breaches

The Service 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 after becoming aware of it. Such breaches in an Education Service context may include, but are not limited to:

- A non-anonymised dataset being published or circulated which identifies pupils and their SEND or EHCP status
- Safeguarding information being made available to an unauthorised person
- The theft of a Service laptop containing non-encrypted personal data about pupils
- A tutor emailing pupil information to the wrong recipient, or to a personal email account
- Personal or safeguarding data being entered into an unapproved AI tool
- A ransomware or other cyber attack resulting in loss of, or unauthorised access to, personal data

Where a breach arises from a cyber incident, the external reporting duties in section 8.5 of the Cyber Security Policy also apply, including reporting to Action Fraud, the NCSC, the Department for Education, commissioners and insurers as relevant. The ICO reporting decision remains with the DPO.

18. Training

All staff are provided with data protection training as part of their induction process. Training must be completed before access to personal data is granted, and is repeated at least annually. A record of completion is retained and reported to the Executive Board.

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

Training covers recognising a subject access request or a data protection complaint in any form, recognising and reporting a breach, safe handling of special category and safeguarding data, and the rules on AI tools. Role-specific training is provided to those handling SARs, completing DPIAs or managing supplier contracts. Executive Board members receive briefing appropriate to their governance role.

19. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed annually and approved by the CEO. A review will additionally be triggered by a change in data protection legislation or ICO guidance, a new version of Keeping Children Safe in Education, a significant personal data breach, the introduction of a significant new system or technology, or a finding from an audit, commissioner or insurer.

The DPO provides an annual report to the CEO and the Executive Board covering breaches and near misses, subject access requests and complaints received and how they were handled, training completion, audit findings, DPIAs completed, and progress against the outstanding actions at section 21.

20. Links with other policies

This data protection policy is linked to our:

- GDPR and Privacy statement
- CCTV Policy
- Child protection and Safeguarding Policy
- Internet and Acceptable Use Policy
- Cyber Security Policy and Cyber Security Risk Assessment
- AI Governance Framework and AI Acceptable Use Policy
- CCTV Legitimate Interests Assessment, Appropriate Policy Document and Data Protection Impact Assessment
- Record retention schedule (to be produced)
- Online Safety Policy and Staff Code of Conduct

21. Outstanding actions

The following are required to give full effect to this policy and should be tracked to completion by the DPO:

#	Action	Owner
1	Produce a formal record retention schedule covering pupil, staff, safeguarding, financial and CCTV records (section 7.3).	DPO
2	Produce an Appropriate Policy Document covering special category and criminal offence data beyond CCTV — SEND, EHCP, health, safeguarding and DBS data (section 7.2).	DPO
3	Assess and minute whether the combined DPO and DSL role creates a conflict of interest under Article 38(6), and record how it is managed (section 5.2).	Executive Board
4	Establish and populate the record of processing activities (section 14).	DPO
5	Review and update all privacy notices to reflect legitimate interests rather than public task, and the new complaints route.	DPO
6	Complete Legitimate Interests Assessments for each processing activity relying on Article 6(1)(f).	DPO

#	Action	Owner
7	Confirm Article 28 agreements are in place with all suppliers processing personal data on our behalf, and record data location for each.	DPO / Head of Systems
8	Brief all staff on the new complaints route and the requirement to recognise verbal requests.	DPO

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 or data processor must immediately notify the data protection officer (DPO) by emailing jean-paul.muller@tuition-extra.co.uk.
- Where the DPO is unavailable, or where the breach may involve the DPO, the report must be made to the CEO. Where a cyber incident is suspected, the Head of Systems and Processes must be notified at the same time under the Cyber Security Policy.
- 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, or made available to unauthorised people.
- Staff 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 considered to be likely that is the case, the DPO will alert the CEO.
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the DPO with this where necessary, and the DPO should take external advice when required (e.g. from IT providers). Where a child may be affected, the Designated Safeguarding Lead must be informed immediately.
- 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 at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the education service computer systems.
- 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 Service's awareness of the breach. As required, the DPO will set out a description of the nature of the breach including the categories and approximate number of individuals and records concerned; the name and contact details of the DPO; a description of the likely consequences; and a description of the measures taken or to be taken.
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours of the Service'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.
- Where the Service is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing, setting out the nature of the breach in clear and plain language, the DPO's contact details, the likely consequences, and the measures taken.
- Where the affected individual is a child, the notification will be written in language they can understand, and the parent or carer will normally also be informed unless doing so would place the child at risk.
- The DPO will consider, in light of 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.
- Where the breach arises from a cyber incident, the DPO will confirm with the Head of Systems and Processes that the external reporting duties in the Cyber Security Policy have been

discharged — Action Fraud, the NCSC, the Department for Education, commissioners and insurers as applicable.

- The DPO will document each breach, irrespective of whether it is reported to the ICO, recording the facts and cause, the effects, and the action taken to contain it and ensure it does not happen again.
- Records of all breaches will be stored on the education service computer systems.
- The DPO and CEO will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible. Lessons learned are recorded and any resulting change to policy or practice is tracked to completion.
- The DPO and CEO will meet regularly to assess recorded data breaches and identify any trends or patterns requiring action by the Service 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 support provision to attempt to recall it from external recipients and remove it from the Service'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 Service should inform the Kent Safeguarding Children Multi-Agency Partnership, Kent County Council as commissioner, and any other local authority that has placed an affected child

All other types of breach will be dealt with in a similar way.