



TTLT Data Protection Policy

Approved by:	TTLT Finance and Resources Committee	Date: 23 June 2026
Last reviewed on:	Summer 2026	
Next review due by:	Summer 2029	

Contents

1. Aims.....	3
2. Legislation and guidance.....	3
3. Definitions.....	4
4. The data controller.....	5
5. Roles and responsibilities.....	5
6. Data protection principles.....	6
7. Collecting personal data.....	7
8. Sharing personal data.....	8
9. Subject access requests and other rights of individuals.....	8
10. Parental requests to see the educational record.....	10
11. Biometric recognition systems.....	11
12. CCTV.....	11
13. Photographs and videos.....	11
14. Artificial intelligence (AI).....	12
15. Data protection by design and default.....	12
16. Data security and storage of records.....	13
17. Disposal of records.....	13
18. Personal data breaches.....	14
19. Complaints.....	14
20. Training.....	14
21. Monitoring arrangements.....	14
22. Links with other policies.....	14
Appendix 1: Personal data breach procedure.....	16

1. Aims

Our school aims 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](#)
- [Data \(Use and Access\) Act 2025](#)

It is based on guidance and resources published by the Information Commissioner (IC) on the [UK GDPR](#) and a policy paper from the Department for Education (DfE) on [Generative artificial intelligence in education](#).

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

3. Definitions

TERM	DEFINITION
Personal data	Any information relating to an identified, or identifiable, living individual, whether identified directly or indirectly. This may include the individual's: 1. Name (including initials) 2. Identification number 3. Location data 4. 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: 1. Racial or ethnic origin 2. Political opinions 3. Religious or philosophical beliefs 4. Trade union membership 5. Genetics 6. Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes 7. Health – physical or mental 8. Sex life or sexual orientation
Processing	Any activity that involves the use of personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual, and also includes transmitting or transferring personal data to third parties.
Data subject	The identified or identifiable individual whose personal data is held or processed.

TERM	DEFINITION
Data controller	A person or organisation that determines the purposes and the means of processing personal data. The data controller is responsible for establishing practices and policies in line with the UK GDPR.
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. A data processor acts only on the instructions of the controller and does not determine the purposes or means of the processing.
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 school processes personal data relating to parents and carers, pupils, staff, governors, visitors and others. In carrying out these activities, the school acts as a data controller.

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

5. Roles and responsibilities

This policy applies to **all staff** employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Trust Board

The Trust Board has overall responsibility for ensuring that our Trust and schools comply with all relevant data protection obligations.

5.2 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 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 IC.

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

The Trust's Data Protection working party is made up of the following DPOs, including Rebecca Cheetham Nursery and Children's Centre who are working in partnership with TTLT:

Rohan Allen, Head Teacher, Rebecca Cheetham Nursery

Shella Lawrenson, Executive Head Teacher, Ranelagh and North Beckton Primary Schools

Swasthi Mahabeer, Teacher at Curwen Primary School

Shazidur Rahman, TTLT Operations Manager

Rozina Rashid, Deputy School Business Manager, North Beckton Primary School

To avoid conflict of interest, as far as is practicably possible, TTLT shares expertise between the DPOs of each school in the Trust.

5.3 CEO

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

5.4 Head Teacher / Head of School

The Head Teacher / Head of School and all those in managerial or supervisory roles throughout the school are responsible for developing and encouraging good information handling practices within the school; responsibilities are set out in individual job descriptions.

The Head Teacher / Head of School, a member of the senior management team, is accountable to the CEO for the management of personal information within their school and for ensuring that compliance with data protection legislation and good practice can be demonstrated.

This accountability includes:

- Development and implementation of the PIMS as required by this policy
- Security and risk management in relation to compliance with the policy

The Head Teacher has been appointed to take responsibility for the school's compliance with this policy on a day-to-day basis and, in particular, has direct responsibility for ensuring that the school complies with the GDPR, as do managers in respect of data processing that takes place within their area of responsibility.

The DPO have specific responsibilities in respect of procedures such as the Subject Access Request Procedure and are the first point of call for employees / staff seeking clarification on any aspect of data protection compliance before contacting the Head Teacher.

5.5 All staff

Staff 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:
 - If they have 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

We adhere to the principles relating to processing of personal data set out in the UK GDPR, which requires personal data to be:

- Processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency);
- Collected for specified, explicit and legitimate purposes (purpose limitation);
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed (data minimisation);
- Accurate and, where necessary, kept up to date (accuracy);

- Kept for no longer than is necessary for the purposes for which it is processed (storage limitation);
- Processed in a way that ensures it is appropriately secure (security, integrity and confidentiality);
- Not transferred to another country without appropriate safeguards in place (transfer limitation); and
- Handled in a way that respects the rights of data subjects and allows them to exercise those rights (data subject rights and requests)

We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (accountability).

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 Trust/school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the Trust/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 Trust/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 Trust/school (where the processing is not for any tasks the Trust/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**

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

6. The individual (or their parent/carer when appropriate in the case of a pupil) has given **explicit consent**
7. The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law**
8. 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
9. The data has already been made **manifestly public** by the individual
10. The data needs to be processed for the establishment, exercise or defence of **legal claims**
11. The data needs to be processed for reasons of **substantial public interest** as defined in legislation
12. 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

13. 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
14. 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:

1. The individual (or their parent/carer when appropriate in the case of a pupil) has given **consent**
2. 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
3. The data has already been made **manifestly public** by the individual
4. 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**
5. 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.

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 necessary.

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 school's record retention schedule.

8. Sharing personal data

Generally, we are not allowed to share personal data with third parties unless certain safeguards and contractual arrangements have been put in place.

There will be certain circumstances where we may be required to share personal data. These include, but are not limited to, situations where:

- (a) There is an issue with a pupil, or a parent or carer that puts the safety of our staff at risk
- (b) We need to liaise with other agencies – we will seek consent as necessary before doing this
- (c) 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

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.

When deciding what information to share, schools should consider the relevancy of the information, what the receiving setting needs to know and whether the information is clearly presented and suitably contextualised.

Staff should use professional judgement to make sure that any information shared is focused and proportionate

Where a pupil is changing settings and information indicates a risk to others and/or the individual pupil, the receiving school is responsible for assessing risk and putting a safety and support plan in place; the DSLs from both settings should have a conversation where there are concerns.

Where we transfer personal data internationally, we will do so in accordance with UK data protection law.

9. Subject access requests and other rights of individuals

9.1 Subject access requests (SARs)

By law, individuals have a right to make a 'subject access request' (SAR) to gain access to personal information that the school 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 IC 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:

- The 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.

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 schools 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.

9.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- 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). The Trust/school will pause or "stop the clock" on the 1-month response window while actively waiting for a requester to clarify their identity or narrow down a broad request.
- 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 (these timeframes continue to apply when the school is closed during holidays).

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

Reasonable and Proportionate Search: The school/Trust is only legally required to undertake a "reasonable and proportionate search" for records.

If the request is vexatious 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 IC or they can seek to enforce their subject access right through the courts.

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
- Receive certain information about the data controller's processing activities
- 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 public interest, official authority or 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 personal data breach (in certain circumstances)
- Make a complaint to the IC
- 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.

10. Parental requests to see the educational record

Parents, or those with parental responsibility, can make a request for their child's educational record (which includes most information about a pupil). The request should be made in the same format as a Subject Access Request and the processing and response times by the school will remain the same.

If the request is for a copy of the educational record, the school may charge a fee to cover the cost of supplying it, however the fee must not exceed the cost of supply.

This right applies as long as the pupil concerned attends a school in the Trust.

There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced.

11. Biometric recognition systems

The schools in our Trust do not use biometric recognition systems for pupils and thus we do not collect any biometric data for pupils.

Where staff members or other adults use the school's biometric system(s), we will also obtain their explicit 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.

Use of Voice Recognition and Audio Recording Software

Audio Recording and Automated Minutes - The Trust/school utilises automated voice recognition and transcription software to record and generate written minutes for specified internal meetings, such as staff briefings, trustee meetings, LAB meetings and parental consultations. This technology is strictly limited to settings where **only adults** are present; it is never deployed in classrooms or during meetings involving students.

The processing of this personal data is governed by the following strict safeguards:

- **Consent and Notification:** All participants are informed in advance, and at the start of the meeting, that audio recording and automated transcription are in use. Any participant may request that the recording be paused or turned off.
- **Data Minimisation:** The raw audio recording is used solely for the purpose of generating accurate written text. Once the final minutes are verified and approved, the underlying audio files are permanently deleted.
- **Security and Third-Party Processing:** The software used complies with UK GDPR and Data Protection Act 2018 standards. All data is encrypted both in transit and at rest, and the school ensures that vendor contracts prohibit the use of our data or audio for machine learning or software training purposes.

12. CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will follow the [IC'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 Head Teacher / Head of School / School Business Manager.

13. Photographs and videos

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

We will obtain written consent from parents and carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parents/carers and the pupil.

Any photographs and videos taken by parents and 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, unless all the relevant parents/carers have agreed to this.

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

- Within school on notice boards and in school brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school 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.

14. 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 and Google Gemini. The Trust/schools recognise 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, The Trust/schools will treat this as a data breach and will follow the personal data breach procedure outlined in appendix 1.

15. 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 (DPIAs) 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 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 / ICT / Cyber Security 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.

Data that is no longer needed will be disposed of securely in line with IRMS guidelines..

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 IC within 72 hours after becoming aware of it. 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

We will also notify the data subject where we are legally required to do so.

19. Complaints

We take any complaints about how we collect and use personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concerns about our data processing, please raise this with us in the first instance. You can make a complaint to us at any time by contacting the Trust/School Head Teacher or DPO.

Upon receiving a complaint, we will:

- Acknowledge receipt of the complaint within 30 days of receiving it
- Without undue delay, take appropriate steps to respond to the complaint, including:
 - Making appropriate enquiries based on the circumstances of the complaint
 - Keeping the complainant informed on the progress of the investigation
- Without undue delay, inform the complainant of the outcome of the investigation

20. 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.

21. Monitoring arrangements

The Trust DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed every 3 years and approved by the Trust's Finance, Operations and Resources Committee.

22. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- Privacy notices
- Child Protection Policy
- ICT / Cyber Security Policies
- Health and Safety Policy

Appendix 1: Personal data breach procedure

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

- On finding or causing a breach or potential breach, the staff member, trustee or LAB member or data processor must immediately notify the data protection officer (DPO).
- 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 trustee or LAB members 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 headteacher and the CEO and chair of Trustees
- 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). (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 IC, and the individuals affected using the IC's [self-assessment tool](#)
- The DPO will document the decisions (either way), in case the decisions are challenged at a later date by the IC or an individual affected by the breach. Documented decisions are recorded on the TTLT GDPR Learning Exercise Log and stored on the TTLT GDPR Drive.
- Where the IC must be notified, the DPO will do this via the ['report a breach' page](#) of the IC 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 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
- The DPO will document each breach, irrespective of whether it is reported to the IC. 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 recorded on the TTLT GDPR Learning Exercise Log and stored on the TTLT GDPR Drive.

- The DPO and headteacher/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
- The DPO and headteacher will meet regularly 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 TTLT 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 case 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 endeavor 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 local safeguarding partners

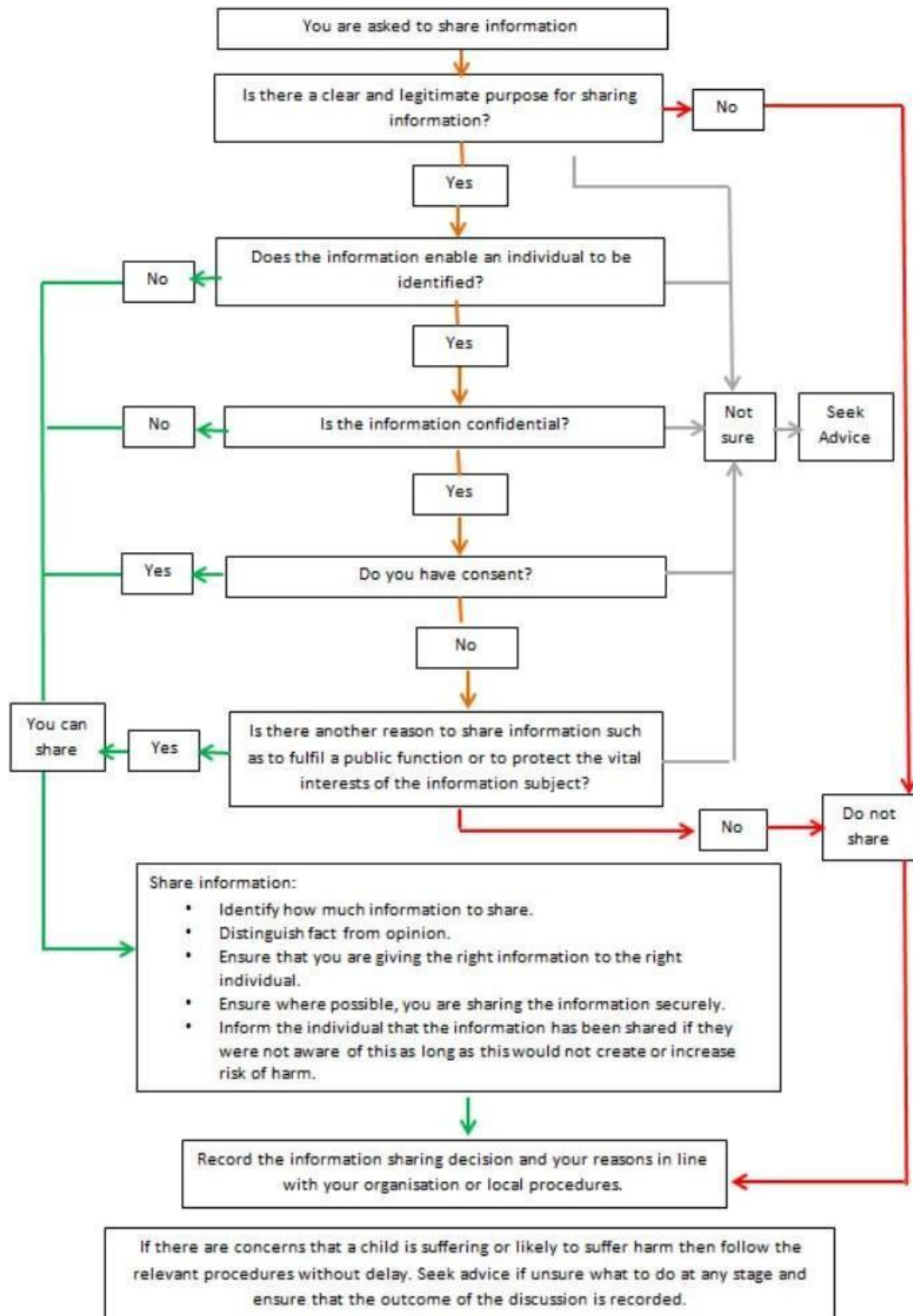
Other types of breach that you might want to consider could include:

- Details of pupil premium interventions for named children being published on the school website
- Non-anonymised pupil exam results or staff pay information being shared with governors

- A school laptop containing non-encrypted sensitive personal data being stolen or hacked
- The school's cashless payment provider being hacked and parents' financial details stolen
- Hardcopy reports sent to the wrong pupils or families

Appendix 2: Data Sharing Agreement

The Department for Education (DfE) produced guidance on information sharing for practitioners providing safeguarding services. Please also refer to section 8 - Sharing personal data for more information.



Appendix 3: Privacy Notice – The Trust as an Educational Setting

Privacy Notice – The Trust as an Educational Setting The Data Protection Act 1998: How we use pupil information

Why do we collect and use pupil information?

We collect and use pupil information under the Trust under the lawful basis for collecting and using pupil information for general purposes under Article 6 and Article 9 of the GDPR May 2018 Working Party, where data processed is special category data.

We use the pupil data:

- to support pupil learning;
- to monitor and report on pupil progress;
- to provide appropriate pastoral care;
- to assess the quality of our services;
- to comply with the law regarding data sharing;

The categories of pupil information that we collect, hold and share include:

- Personal information (such as name, unique pupil number and address);
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility);
- Attendance information (such as sessions attended, number of absences and absence reasons);
- Attainment, Examination & Assessment information to support pupil learning;
- Medical information provided by parents/carers and guardians;
- Special Educational Needs and Referral Information;
- Behavioural Information, including exclusions;
- Court of Protection/Safeguarding information;
- Photographic images in our schools, on school literature, websites or media;

Collecting pupil information

Whilst the majority of pupil information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain pupil information to us or if you have a choice in this.

Storing pupil data

We hold pupil data from the point that an application is made through our Schools or the Local Authority. These records are retained until the child is 25 years of age, as well as

being transferred to the relevant secondary school and held until the child is 25 years of age.

Who do we share pupil information with?

We routinely share pupil information with:

- Members and Trustees of Consortium in the support of pupil learning
- Trust staff in the support of pupil learning
- The school's Local Governing Body
- Consultants engaged by the Trust to support pupil learning
- Staff of other Trust schools in the support of pupil learning
- Staff of Partnership schools in the support of pupil learning
- Cloud based educational programmes to support pupil learning and communication
- Parents & Carers of our schools
- School Nursing & Dental Services
- External agencies; health, SEND, child protection, welfare and safeguarding services
- Local media publications
- Schools that the pupil's attend after leaving us
- The school's local authority
- The Department for Education (DfE)

Why we share pupil information

We do not share information about our pupils with anyone without consent, unless the law and our policies allow us to do so. We share pupils' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

We are required to share information about our pupils with the (DfE) under regulation 5 of The Education (Information about Individual Pupils) (England) Regulations 2013.

Data collection requirements:

To find out more about the data collection requirements placed on us by the Department for Education (for example; via the school census) go to:

<https://www.gov.uk/education/data-collection-and-censuses-for-schools>

The National Pupil Database (NPD)

The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

We are required by law, to provide information about our pupils to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.

To find out more about the pupil information we share with the department, for the purpose of data collections, go to <https://www.gov.uk/education/data-collection-and-censuses-for-schools>.

To find out more about the NPD, go to <https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information>.

The department may share information about our pupils from the NPD with third parties who promote the education or well-being of children in England by:

- conducting research or analysis;
- producing statistics;
- providing information, advice or guidance;

The Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data.

Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data;
- the purpose for which it is required;
- the level and sensitivity of data requested, and
- the arrangements in place to store and handle the data;

To be granted access to pupil information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit: <https://www.gov.uk/data-protection-how-we-collect-and-share-research-data>

For information about which organisations the department has provided pupil information, (and for which project), please visit the following website:

<https://www.gov.uk/government/publications/national-pupil-database-requests-received>

To contact DfE: <https://www.gov.uk/contact-dfe>

Requesting access to your personal data

Under data protection legislation, parents and pupils have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, contact the Data Protection Officer for the Trust who is Shazidur Rahman:

Shazidur.rahman@kensington.tlt.academy

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to the Information Commissioner's Office at <https://ico.org.uk/concerns/>

Contact:

If you would like to discuss anything in this privacy notice, please contact the Data Protection Officer for the Trust, who is Shazidur Rahman at:

Shazidur.rahman@kensington.tlt.academy

Appendix 4: Privacy Notice for Pupils

Privacy Notice for Pupils

Date:

You have a legal right to be informed about how our school uses any personal information that we hold about you. To comply with this, we provide a 'privacy notice' to you where we are processing your personal data.

This privacy notice explains how we collect, store and use personal data about you. We, The Tapscott Learning Trust (hereon called the "Trust" or "TTLT") and its schools are the 'data controllers' for the purposes of data protection law.

Our data protection officer can be found on the TTLT or school's website.

The personal data we hold

We hold some personal information about you to make sure we can help you learn and look after you at school.

For the same reasons, we get information about you from some other places too – like other schools, the local council and the government.

This information includes:

- Your contact details
- Your test results
- Your attendance records
- Your characteristics, like your ethnic background or any special educational needs
- Any medical conditions you have
- Details of any behaviour issues or exclusions
- Photographs
- CCTV images

Why we use this data

We use this data to help run the school, including to:

- Get in touch with you and your parents when we need to
- Check how you're doing in exams and work out whether you or your teachers need any extra help
- Track how well the school as a whole is performing
- Look after your wellbeing

Our legal basis for using this data

We will only collect and use your information when the law allows us to. Most often, we will use your information where:

- We need to comply with the law
- We need to use it to carry out a task in the public interest (in order to provide you with an education)

Sometimes, we may also use your personal information where:

- You, or your parents/carers have given us permission to use it in a certain way
- We need to protect your interests (or someone else's interest)

Where we have got permission to use your data, you or your parents/carers may withdraw this at any time. We will make this clear when we ask for permission, and explain how to go about withdrawing consent.

Some of the reasons listed above for collecting and using your information overlap, and there may be several grounds which mean we can use your data.

Collecting this information

While in most cases you, or your parents/carers, must provide the personal information we need to collect, there are some occasions when you can choose whether or not to provide the data.

We will always tell you if it's optional. If you must provide the data, we will explain what might happen if you don't.

How we store this data

We will keep personal information about you while you are a pupil at our school. We may also keep it after you have left the school, where we are required to by law.

We use the Information and Records Management Society's toolkit (IRMS) for schools which sets out how long we must keep information about pupils.

Data sharing

We do not share personal information about you with anyone outside the school without permission from you or your parents/carers, unless the law and our policies allow us to do so.

Where it is legally required, or necessary for another reason allowed under data protection law, we may share personal information about you with:

- Our local authority – to meet our legal duties to share certain information with it, such as concerns about pupils' safety and exclusions
- The Department for Education (a government department)
- Your family and representatives
- Educators and examining bodies
- Our regulator, e.g. OfSTED

- Suppliers and service providers – so that they can provide the services we have contracted them for
- Financial organisations
- Central and local government
- Our auditors
- Survey and research organisations
- Health authorities
- Security organisations
- Health and social welfare organisations
- Professional advisers and consultants
- Police forces, courts, tribunals
- Professional bodies

National Pupil Database

We are required to provide information about you to the Department for Education (a government department) as part of data collections such as the school census.

Some of this information is then stored in the [National Pupil Database](#), which is managed by the Department for Education and provides evidence on how schools are performing. This, in turn, supports research.

The database is held electronically so it can easily be turned into statistics. The information it holds is collected securely from schools, local authorities, exam boards and others.

The Department for Education may share information from the database with other organisations which promote children's education or wellbeing in England. These organisations must agree to strict terms and conditions about how they will use your data. You can find more information about this on the Department for Education's webpage on [how it collects and shares research data](#).

You can also [contact the Department for Education](#) if you have any questions about the database.

Transferring data internationally

Where we share data with an organisation that is based outside the UK, we will protect your data by following data protection law.

Your rights

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 school 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.

How to access personal information we hold about you

You can find out if we hold any personal information about you, and how we use it, by making a '**subject access request**', as long as we judge that you can properly understand your rights and what they mean.

If we do hold information about you, we will:

- Give you a description of it
- Tell you why we are holding and using it, and how long we will keep it for
- Explain where we got it from, if not from you or your parents
- Tell you who it has been, or will be, shared with
- Let you know if we are using your data to make any automated decisions (decisions being taken by a computer or machine, rather than by a person)
- Give you a copy of the information

You may also ask us to send your personal information to another organisation electronically in certain circumstances.

If you want to make a request please contact our data protection officer.

Your other rights over your data

You have other rights over how your personal data is used and kept safe, including the right to:

- Say that you don't want it to be used if this would cause, or is causing, harm or distress
- Stop it being used to send you marketing materials
- Say that you don't want it used to make automated decisions (decisions made by a computer or machine, rather than by a person)
- Have it corrected, deleted or destroyed if it is wrong, or restrict our use of it
- Claim compensation if the data protection rules are broken and this harms you in some way

Complaints

We take any complaints about how we collect and use your personal data very seriously, so please let us know if you think we've done something wrong.

You can make a complaint at any time by contacting our data protection officer. You can also complain to the Information Commissioner's Office in one of the following ways:

- Report a concern online at <https://ico.org.uk/concerns/>
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact the relevant data protection officer at your school.

Appendix 5: Privacy Notice for Parents / Carers

Privacy notice for Parents /Carers

Date:

Under data protection law, individuals have a right to be informed about how the school uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about **pupils**. We, [school name and address], are the 'data controller' for the purposes of data protection law.

Our data protection officer can be found on the TTLT or school's website.

The personal data we hold

Personal data that we may collect, use, store and share (when appropriate) about pupils includes, but is not restricted to:

- Contact details, contact preferences, date of birth, identification documents
- Results of internal assessments and externally set tests
- Pupil and curricular records
- Characteristics, such as ethnic background, eligibility for free school meals, or special educational needs
- Exclusion information
- Details of any medical conditions, including physical and mental health
- Attendance information
- Safeguarding information
- Details of any support received, including care packages, plans and support providers
- Photographs
- CCTV images captured in school

We may also hold data about pupils that we have received from other organisations, including other schools, local authorities and the Department for Education.

Why we use this data

We use this data to:

- Support pupil learning
- Monitor and report on pupil progress
- Provide appropriate pastoral care
- Protect pupil welfare
- Assess the quality of our services

- Administer admissions waiting lists
- Carry out research
- Comply with the law regarding data sharing

Our legal basis for using this data

We only collect and use pupils' personal data when the law allows us to. Most commonly, we process it where:

- We need to comply with a legal obligation
- We need it to perform an official task in the public interest

Less commonly, we may also process pupils' personal data in situations where:

- We have obtained consent to use it in a certain way
- We need to protect the individual's vital interests (or someone else's interests)

Where we have obtained consent to use pupils' personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent, and explain how consent can be withdrawn.

Some of the reasons listed above for collecting and using pupils' personal data overlap, and there may be several grounds which justify our use of this data.

Collecting this information

While the majority of information we collect about pupils is mandatory, there is some information that can be provided voluntarily.

Whenever we seek to collect information from you or your child, we make it clear whether providing it is mandatory or optional. If it is mandatory, we will explain the possible consequences of not complying.

How we store this data

We keep personal information about pupils while they are attending our school. We may also keep it beyond their attendance at our school if this is necessary in order to comply with our legal obligations. The Information and Records Management Society's toolkit (IRMS) for schools sets out how long we keep information about pupils.

Data sharing

We do not share information about pupils with any third party without consent unless the law and our policies allow us to do so.

Where it is legally required or necessary (and it complies with data protection law) we may share personal information about pupils with:

- Our local authority – to meet our legal obligations to share certain information with it, such as safeguarding concerns and exclusions
- The Department for Education
- The pupil's family and representatives
- Educators and examining bodies

- Our regulator [specify as appropriate, e.g. Ofsted, Independent Schools Inspectorate]
- Suppliers and service providers – to enable them to provide the service we have contracted them for
- Financial organisations
- Central and local government
- Our auditors
- Survey and research organisations
- Health authorities
- Security organisations
- Health and social welfare organisations
- Professional advisers and consultants
- Police forces, courts, tribunals
- Professional bodies

National Pupil Database

We are required to provide information about pupils to the Department for Education as part of statutory data collections such as the school census.

Some of this information is then stored in the [National Pupil Database](#) (NPD), which is owned and managed by the Department and provides evidence on school performance to inform research.

The database is held electronically so it can easily be turned into statistics. The information is securely collected from a range of sources including schools, local authorities and exam boards.

The Department for Education may share information from the NPD with other organisations which promote children's education or wellbeing in England. Such organisations must agree to strict terms and conditions about how they will use the data. For more information, see the Department's webpage on [how it collects and shares research data.](#)

You can also [contact the Department for Education](#) with any further questions about the NPD.

Transferring data internationally

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

Parents and pupils' rights regarding personal data

Individuals have a right to make a '**subject access request**' to gain access to personal information that the school holds about them.

Parents / carers can make a request with respect to their child's data where the child is not considered mature enough to understand their rights over their own data (usually under the age of 12), or where the child has provided consent.

Parents also have the right to make a subject access request with respect to any personal data the school holds about them.

If you make a subject access request, and if we do hold information about you or your child, we will:

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you or your child
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

Individuals also have the right for their personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request please contact our data protection officer.

Parents / carers also have a right to access to their child's **educational record**. To request access, please contact the DPO.

Other rights

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe, including the right to:

- Object to the use of personal data if it would cause, or is causing, damage or distress
- Prevent it being used to send direct marketing
- Object to decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact our data protection officer.

Complaints

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact our data protection officer.

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at <https://ico.org.uk/concerns/>
- Call 0303 123 1113

- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact the relevant **data protection officer**.

Appendix 6: Privacy Notice for Staff

Privacy Notice for Staff

Date:

Under data protection law, individuals have a right to be informed about how the school uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about individuals we employ, or otherwise engage, to work at our school.

We, [school name and address], are the 'data controller' for the purposes of data protection law.

Our data protection officers are:

Rohan Allen

Shella Lawrenson

Swasthi Mahabeer

Shazidur Rahman

Rozina Rashid

To avoid conflict of interest TTLT shares the DPO function between a group of schools and shares expertise by being the DPOs for each other's school.

.

The personal data we hold

We process data relating to those we employ, or otherwise engage, to work at our school. Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

- Contact details
- Date of birth, marital status and gender
- Next of kin and emergency contact numbers
- Salary, annual leave, pension and benefits information
- Bank account details, payroll records, National Insurance number and tax status information

- Recruitment information, including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process
- Qualifications and employment records, including work history, job titles, working hours, training records and professional memberships
- Performance information
- Outcomes of any disciplinary and/or grievance procedures
- Absence data
- Copy of driving licence
- Photographs
- CCTV footage
- Data about your use of the school's information and communications system

We may also collect, store and use information about you that falls into "special categories" of more sensitive personal data. This includes information about (where applicable):

- Race, ethnicity, religious beliefs, sexual orientation and political opinions
- Trade union membership
- Health, including any medical conditions, and sickness records

Why we use this data

The purpose of processing this data is to help us run the school, including to:

- Enable you to be paid
- Facilitate safe recruitment, as part of our safeguarding obligations towards pupils
- Support effective performance management
- Inform our recruitment and retention policies
- Allow better financial modelling and planning
- Enable ethnicity and disability monitoring
- Improve the management of workforce data across the sector
- Support the work of the School Teachers' Review Body

Our lawful basis for using this data

We only collect and use personal information about you when the law allows us to. Most commonly, we use it where we need to:

- Fulfil a contract we have entered into with you
- Comply with a legal obligation
- Carry out a task in the public interest

Less commonly, we may also use personal information about you when:

- You have given us consent to use it in a certain way
- We need to protect your vital interests (or someone else's interests)
- We have legitimate interests in processing the data – for example, where:
 - o [If you use this basis at all, set out the situations here]

Where you have provided us with consent to use your data, you may withdraw this

consent at any time. We will make this clear when requesting your consent, and explain how you go about withdrawing consent if you wish to do so.
Some of the reasons listed above for collecting and using personal information about you overlap, and there may be several grounds which justify the school's use of your data.

Collecting this information

While the majority of information we collect from you is mandatory, there is some information that you can choose whether or not to provide to us.

Whenever we seek to collect information from you, we make it clear whether you must provide this information (and if so, what the possible consequences are of not complying), or whether you have a choice.

How we store this data

We create and maintain an employment file for each staff member. The information contained in this file is kept secure and is only used for purposes directly relevant to your employment.

Once your employment with us has ended, we will retain this file and delete the information in it in accordance with the Information and Records Management Society's toolkit for schools (IRMS).

Data sharing

We do not share information about you with any third party without your consent unless the law and our policies allow us to do so.

Where it is legally required or necessary (and it complies with data protection law) we may share personal information about you with:

- Our local authority – to meet our legal obligations to share certain information with it, such as safeguarding concerns and [maintained schools only] information about head teacher performance and staff dismissals
- The Department for Education
- Your family or representatives
- Educators and examining bodies
- Our regulator [specify as appropriate e.g. OfSTED, Independent Schools Inspectorate]
- Suppliers and service providers – to enable them to provide the service we have contracted them for, such as payroll
- Financial organisations
- Central and local government
- Our auditors
- Survey and research organisations
- Trade unions and associations
- Health authorities
- Security organisations
- Health and social welfare organisations
- Professional advisers and consultants
- Police forces, courts, tribunals
- Professional bodies
- Employment and recruitment agencies

Transferring data internationally

If we are required to transfer personal data to a country or territory outside the UK, we will do so in accordance with data protection law.

Your rights

How to access personal information we hold about you

Individuals have a right to make a **‘subject access request’** to gain access to personal information that the school holds about them.

If you make a subject access request, and if we do hold information about you, we will:

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

You may also have the right for your personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request, please contact our data protection officer.

Your other rights regarding your data

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe. You have the right to:

- Object to the use of your personal data if it would cause, or is causing, damage or distress
- Prevent your data being used to send direct marketing
- Object to the use of your personal data for decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact our data protection officer.

Complaints

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact our data protection officer.

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at <https://ico.org.uk/concerns/>
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact the respective **data protection officer**:

Appendix 7: Multi-Purpose Consent Form

Multi-Purpose Parental Consent Form

Pupil			
Name			
Year		Class	

Parent / Carer	
Name	
Relationship to pupil	
Address	
Phone	
Mobile	
Email	

Off-site Activities

The On-site and off-site activities are written in line with the Educational Visits Policy.

I give my permission for my son / daughter to take part in:

Supervised visits to destinations away from the main school site, one-day non-residential visits within the UK and sporting activities	
--	--

For residential visits and international visits specific permission will be sought.

Medical consent

The medical consent is in line with the Health and Safety Policy, Supporting Children with Medical Needs and Safeguarding Policy.

I give my permission for:

My son / daughter's information to be shared with the NHS and other relevant health professionals	
Staff to administer the medicines I have listed below:	

Please outline any medical conditions/allergies:

.....

Please outline any food allergies / specific dietary requirements:

.....

Emergency release

The emergency release is in line with the Health and Safety Policy and Safeguarding Policy.

I give my consent for my son/daughter to be released to the following person(s) in the event of emergency or illness, if I cannot be contacted:

Person 1	
Name	
Address	
Relationship to child	
Contact number	

Person 2	
Name	
Address	
Relationship to child	
Contact number	

Information and image (including photographs and video recordings)

The use of information and image is in line with the Computing and E-Safety Policies.

I give permission for my child to be photographed and videoed	
---	--

I give my permission for my son / daughter's:

Work to be used in school displays and on the school website	
Image to be used • within school (for example, in wall-mounted displays) • in printed school publications (for example, the school prospectus) • on the school website and in the local media • by the school after the child has left	

The information in this form will be used throughout your child's time at school. You may withdraw your consent at any time by contacting the school.

Please sign and date the form before returning it to:

Signed:

Date:

Appendix 8: Personal data breach procedure

This procedure is based on [guidance on personal data breaches](#) produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
- The DPO will investigate the incident and fill in the Breach Incident Form (see Appendix H)
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out 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
- The DPO will review incident with another Trust DPO and agree severity and any remedial actions and determine the next required actions. They will consider whether personal data has been accidentally or unlawfully breached. A breach can be:
 - the disclosure of confidential data to unauthorised individuals
 - the loss or theft of portable devices or equipment containing identifiable personal, confidential or sensitive data e.g. PCs, USBs, mobile phones, laptops, disks etc.
 - the loss or theft of paper records
 - inappropriate access controls allowing unauthorised use of information
 - a suspected breach of the school's IT security and acceptable use policy
 - attempts to gain unauthorised access to computer systems, e.g. hacking
 - records altered or deleted without authorisation from the data 'owner'
 - viruses or other security attacks on IT equipment systems or networks
 - breaches of physical security, for example forcing of doors or windows into a secure room or filing cabinet containing confidential information
 - confidential information left unlocked in accessible areas
 - insecure disposal of confidential paper waste
 - leaving IT equipment unattended when logged in to a user account without locking the screen to stop others accessing information
 - the publication of confidential data on the internet in error and accidental disclosure of passwords
 - misdirected emails or faxes containing identifiable personal, confidential or sensitive data
- Both DPOs will:
 - alert the CEO / Head Teacher / Head of School and the Chair of Governors, as necessary
 - work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:

- Loss of control over their data
 - DiscriminationIdentify theft or fraud
 - Financial loss
 - Unauthorised reversal of pseudonymisation (for example, key-coding)
 - Damage to reputation
 - Loss of confidentiality
 - Any other significant economic or social disadvantage to the individual(s) concerned
- Both DPOs will document the decision (either way); in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored
- Where the ICO must be notified, the DPOs will do this via the [‘report a breach’ page of the ICO website](#) within 72 hours. 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 DPOs will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why and when the DPO expects to have further information. The DPOs will submit the remaining information as soon as possible
- Both DPOs will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPOs will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
 - 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 DPOs will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPOs 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 documented within the Breach Incident Form, as per the Health and Safety Policy.

- The DPO and CEO / Head Teacher / Head of School will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, 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.

Examples of actions (for different types of risky or sensitive personal data) are:

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 to recall it
- In any cases where the recall is unsuccessful, the DPO will 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 ensure we receive 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

Other types of breach that you might want to consider could include:

- Details of pupil premium interventions for named children being published on the school website
- Non-anonymised pupil exam results or staff pay information being shared with governors
- A school laptop containing non-encrypted sensitive personal data being stolen or hacked
- The school's cashless payment provider being hacked and parents' financial details stole

