

Data protection policy

(Inc. retention and deletion schedule and privacy notices)

Trinity School



Written by: Sandra Lee (DPO)

Date: 25/3/23

Approved by:

Next review due by: March '24

Contents

1. Aims.....	2
2. Legislation and guidance	2
3. Definitions	3
4. The data controller	4
5. Roles and responsibilities	4
6. Data protection principles.....	5
7. Collecting personal data.....	5
8. Sharing personal data	6
9. Subject access requests and other rights of individuals	6
10. Parental requests to see the educational record	8
11. Biometric recognition systems.....	8
12. CCTV	8
13. Photographs and videos	8
14. Data protection by design and default	9
15. Data security and storage of records.....	9
16. Disposal of records	10
17. Personal data breaches	10
18. Training.....	10
19. Monitoring arrangements	10
20. Links with other policies	10
Appendix 1: Personal data breach procedure	12
Appendix 2: Document retention and deletion schedule	14
Appendix 3: Privacy Notices.....	24

1. Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the [General Data Protection Regulation \(GDPR\)](#) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the [Data Protection Bill](#).

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 GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the [GDPR](#) and the ICO's [code of practice for subject access requests](#).

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

In addition, this policy complies with regulation 5 of the [Education \(Pupil Information\) \(England\) Regulations 2005](#), which gives parents the right of access to their child's educational record.

3. Definitions

Term	Definition
Personal data	<p>Any information relating to an identified, or identifiable, individual.</p> <p>This may include the individual's:</p> <ul style="list-style-type: none"> • Name (including initials) • Identification number • Location data • Online identifier, such as a username <p>It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.</p>
Special categories of personal data	<p>Personal data which is more sensitive and so needs more protection, including information about an individual's:</p> <ul style="list-style-type: none"> • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	<p>Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying.</p> <p>Processing can be automated or manual.</p>
Data subject	<p>The identified or identifiable individual whose personal data is held or processed.</p>
Data controller	<p>A person or organisation that determines the purposes and the means of processing of</p>

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

The school is registered as a data controller with the ICO and will renew this registration annually or as otherwise 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 Governing board

The governing board has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

5.2 Data protection officer

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

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

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

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

Our DPO is Sandra Lee and is contactable via the school office

Email: office@trinity.bardaglea.org.uk

Phone: 0203 435 5955

Fax: 020 8270 4969

5.3 Headteacher

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

5.4 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:
 - 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 European Economic Area
- 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 GDPR is based on data protection principles that our school must comply with.

The principles say that personal data must be:

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

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

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

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

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest**, and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the school 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 one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent (except for online counselling and preventive services). *In law we do not need to seek this consent from parents once a student reaches 13 years of age, however due to the complex needs of our students and their capacity to make informed consent, we will continue to seek parental consent for students of all ages.*

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

7.2 Limitation, minimisation and accuracy

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

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

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

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

We will not normally share personal data with anyone else, but may do so 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. *The consent to share with the NHS is sought for all pupils when they enter the school to allow collaborative working between the school and health professionals.*
- 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 which can provide sufficient guarantees that they comply with data protection law
 - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
 - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

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

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

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.

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

9. Subject access requests and other rights of individuals

9.1 Subject access requests

Individuals have a right to make a 'subject access request' 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
- 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

Subject access requests must be submitted in writing, either by letter, email or fax to the DPO. They should include:

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

If staff receive a subject access request 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 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.

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 school 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, therefore *in the majority of cases in this school, due to the additional needs of our students, we will continue to uphold the parent's right of access.*

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
- 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 will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

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, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- 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, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

11. Biometric recognition systems

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

12. CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's [code of practice](#) for the use of CCTV.

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 Vanessa Adair- 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, including as part of whole school assessment systems, communication profiles and feeding information.

We will obtain written consent from parents/carers 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 pupil.

Uses may include:

- Within school on notice boards and in school magazines, 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 for communication, marketing and promotional materials 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.

See our child protection and safeguarding policy/photography policy for more information on our use of photographs and videos.

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 privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- 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, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

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, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals

- 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 policy/acceptable use agreement/policy on acceptable use).
- Staff have the capacity to access servers from home. They are expected to use this and save work directly onto the server not onto their personal device.
- Staff are not to save work documentation that includes personally identifiable information on personal devices.
- Personal devices which are used to access email should be password or PIN protected and should not be used by family/friends unless app is specifically locked/protected.
- 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)

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. Dates for this to be carried out is included in the retention schedule in the appendix.

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.

17. Personal data breaches

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

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

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

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

18. 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.

19. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our school's practice. Otherwise, or from then on, this policy will be reviewed **every 2 years** and shared with the full governing board.

20. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- Online safety policy

- Acceptable use of ICT policy
- Child protection policy
- Photography policy
- Mobile phone policy
- Use of images policy

Appendix 1: 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 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
- The DPO will alert the headteacher and the chair of governors
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, 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 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
 - Discrimination
 - Identify 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

If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

- The DPO 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 on the school server in the DPOs assigned area.
- Where the ICO must be notified, the DPO 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 DPO 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 DPO will submit the remaining information as soon as possible
- The DPO 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 DPO 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 DPO 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 DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
 - Facts and cause
 - Effects
 - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored on the school server in the DPOs assigned area.

The DPO and headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

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.

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
- A school laptop containing non-encrypted sensitive personal data being stolen or hacked is to be reported to the DPO and ICT Team, who will manage the breach.

Appendix 2: Retention and deletion schedule.

Trinity school Data retention and deletion schedule.

In order to become compliant to the new GDPR, Trinity school must compile a list of the documentation that it holds along with the planned schedule of retention and deletion. The list below details the majority (if not all) of the data currently held.

It can be broken down into broad categories for the majority of data and these are shared below.

Information included:		Retention	Disposal	Authority
Pupil information files/ Integris	Characteristics (age, ethnicity, religion etc) Special educational needs Dietary requirements Free school meals/pupil premium/whether they are a looked-after child Eligibility for funding details - Ni number and/or Date of Birth/ NAAS number. Parent in the military Emergency contact details Transport entitlement GP contact details. Permissions for calling doctor and/or administer first aid in emergency	Removed from Integris when child no longer on roll- this could be following a transfer to another school via CFT, to educational welfare if no longer in education or off roll when of school leaving age. Paper copies until the pupil reaches 31	End of academic year in which the pupil's 31st birthday occurs All documents listed in this schedule are to be shredded/ sent to document disposal company at the correct time.	As per borough guidance.
Pastoral records.				
Pastoral records. (Buff folders)	Consent forms (photographs, school trips etc) Birth certificate number or Passport number Holiday permission forms (with accompanying letter) Behaviour incidents Attendance issues Accident reports SALT information	Removed from Integris when child no longer on roll- this could be following a transfer to another school via CFT, to educational welfare if no longer in education or off roll when of school leaving age. Paper copies until the pupil reaches 31	End of academic year in which the pupil's 31st birthday occurs Disposal company/ destruction.	As per borough guidance.
Admissions form- Legal surname Preferred surname First name Known name middle name(s) Date of birth Gender		Removed from Integris when child no longer on roll- this could be following a transfer to another school via CFT, to educational welfare if no longer in education or off roll when of school leaving age. Paper copies until the	End of academic year in which the pupil's 31st birthday occurs Disposal company/ destruction.	As per borough guidance.

	<p>Action taken</p> <p>CAFS, MARFs</p> <p>looked after children</p> <p>Contact details of other professionals</p> <p>ongoing email conversations/ paperwork shared with other professionals.</p>	years		<p>Borough Safeguarding guidance for storage to be followed e.g.</p> <p>Looked after children – 75 years</p>
Academic Information				
<p>CASPA data</p> <p>Ongoing assessment data</p> <p>In- class assessment portfolio's (Green folders)</p> <p>Records of interventions</p> <p>Personalised documentation</p>	<p>Inputted by us and then uploaded. CASPA can be opened and used to identified staff only</p> <p>PLO, PCOs and end of year assessments</p> <p>Phase data spreadsheets - assessment data including interventions- pupils individually identifiable.</p> <p>Phase data books - anonymised percentages however some individuals mentioned.</p> <p>2 build a profile - third party online storage of pupils images and ongoing work and assessment level.</p> <p>Photographs and assessment information inc levels .</p> <p>PPM notes and spreadsheets</p> <p>Behaviour tracking</p> <p>Risks assessment s</p> <p>Manual handling plans</p> <p>Behaviour plans</p> <p>Feeding mats</p> <p>Communication profiles.</p>	<p>Archived with other pupil files.</p> <p>Kept for current academic year and then one more by DHT.</p> <p>To be removed at the end of time with school/ or when subscription is no longer renewed- whichever is sooner.</p> <p>Work to be removed at the end of each academic year and then sent home the following Christmas.</p> <p>Kept for current academic year and then one more by DHT.</p> <p>Taken from</p>	<p>Deletion from sever</p> <p>Sent home to parents</p> <p>Disposal company/ destruction.</p> <p>Disposal</p>	<p>As per borough guidance.</p>

Reports to parents	Paper copies of year reports.	Integris, Entered into online exam portal.	company/ destruction.	
	Name, D.O.B, Unique Learner number, candidate number, gender, nationality, EAL status.	7 years from the date of certification	Returned to pupils	In line with Exam board guidance.
Exam board registration	Name, NOCN learner number, contact address and telephone number, Regulator reference and title of qualification the learner was registered on.	7 years from the date of certification	Disposal company/ destruction.	In line with Exam board guidance.
Exam results	Date of qualification achievement, Grade of qualification (if applicable)			
	Name, Name of school, ULN, Candidate number, examples of work.			
	BTEC (guidance) - work to be returned to students ASAP and not kept more than 12 weeks after the end of the course.	7 years from the date of certification		In line with Exam board guidance.
	WJEC- work is kept until the certificates arrive around autumn 1 half term.			
Accreditation work	AQA-generally no work to return just a tick sheet.		Disposal company/ destruction.	
	NOCN – record of assessment plan, Assessment decisions for each learner, details of who assessed, what was assessed (learning outcome reference and assessment criteria), where it was assessed and the date the assessment decision was made.	3 years after the year of assessment.		In line with Exam board guidance.
Work Experience				
Trident forms	Name, Date of birth, Contact details, Medical information, Permission request including permission to shared data. Student agreement generated by Trident following meeting and signed by parent and student. Job description.	Collated and then sent to Trident (work experience provider)	Disposal company/ destruction.	
			Disposal	

<p>Work experience diaries</p> <p>Risk assessment</p> <p>Generic risk assessment.</p> <p>EVA trip form</p> <p>Trident forms - students placed here</p>	<p>name,</p> <p>contact information for parents,</p> <p>consent to participate in work experience.</p> <p>Incoming student placement information forms/</p>	<p>See EVA forms</p> <p>Kept for that academic year and one more.</p>	<p>company/ destruction.</p> <p>Disposal company/ destruction.</p>	
Transition to adult placement				
<p>Transition information.</p> <p>See SALT notes below.</p>	<p>Name, date of birth, parental contact information, minutes of transition meeting.</p> <p>Communication passport</p>	<p>Sent to new placement</p>	<p>Sent to new placement</p>	<p>Retained under NHS guidance</p>
SALT Files				
<p>Pupil files</p> <p>Communication passport</p> <p>Training materials</p>	<p>Name</p> <p>Date of birth,</p> <p>NHS number,</p> <p>Letters from other professionals including GOSH and NHS feeding dysphasia specialist.</p> <p>Ongoing case notes</p> <p>Feeding mats</p> <p>Copies of EHC plans</p> <p>Communication profile</p> <p>Name,</p> <p>date of birth,</p> <p>photographs of pupils and family members.</p> <p>Names, photographs, narrative descriptions.</p>	<p>Kept on SALT drive on server.</p> <p>Paper copies in office and then archived to storage.</p> <p>To be deleted/ destroyed when no longer needed or when pupil have left school. (Whichever is first)</p>	<p>Disposal company/ destruction at age 31.</p> <p>Deleted from sever or disposal company/ destruction</p>	<p>As per NHS guidance</p>
HR				
<p>Recruitment information</p>	<p>Applicants' names and contact details</p> <p>Interview notes</p> <p>References</p> <p>DBS checks and disclosures.</p> <p>Verification of right to work in</p>	<p>Deleted when recruitment round is over</p> <p>Disclosure report -</p>	<p>Deleted from sever or disposal company/ destruction</p>	<p>As per borough guidance.</p>

<p>Copies of pre-employment checks</p> <p>Staff personnel files</p> <p>Appraisal records</p>	<p>the UK</p> <p>Names and contact details</p> <p>Salary</p> <p>P45 forms</p> <p>Disciplinary action taken</p> <p>Grievances</p> <p>Pension opt out forms</p> <p>support services referrals such as occupational health, physio and counselling.</p> <p>Risk assessments.</p> <p>Accidents at work</p> <p>Feedback from colleagues</p> <p>Appraisal notes and reports</p> <p>Objectives</p> <p>Pay and promotion recommendations</p>	<p>6 months, records of checking - 6 years after completion of contract.</p> <p>6 years after the end of employment by LBBDD.</p> <p>3 years after the end of the investigation.</p> <p>6 years after the end of employment by LBBDD.</p>	<p>Longer for any contentious issues</p> <p>Deleted from sever or disposal company/ destruction</p>	
<p>Finance</p> <p>Bursary forms- Parents'/carers' bank details</p>	<p>Bank details, name, address, date of birth, Postcode, FSM eligibility, vulnerable student status, Evidence of employment support and disability living allowance. (PIP - personal independence allowance)</p>	<p>7 years</p>	<p>Deleted from sever or disposal company/ destruction</p> <p>Deleted from RM finance or</p>	<p>As per borough guidance.</p> <p>As per borough</p>

Invoices paid			disposal company/ destruction	guidance.
Debt incurred	Company details including bank details.	7 years		
Free school meals	Parent Pay report - name and debt - info needed to create letters	7 years		
Egress email system	Those eligible - Name, addresses	7 years		
RM finance.	Havering pupil finance claims.	7 years		
Access and Lock - entry system also sent to the borough to produce the pass	Company contact details, income sources addresses, VAT number	7 years		
Inventory system	Name, date of birth, image and staff member	6 years		
Funding claims from the borough	Staff - first and last name and photo. Requires date of birth and is currently being anonymised. Time in and Out. Visitors - Title, first and surname, company, photograph, vehicle registration, time signed in.			
Extended school	list of names and funding bands. Statistics - list of names, age ethnicity, religion address and which clubs are being attended. Now being sent vis egress. (see separate box at bottom of document)	End of the academic year		
Governance				
Governor details	Name and contact details Register of interests Attendance records	For the duration of their term of office	Held by HR Deleted from sever or disposal company/ destruction	As per borough guidance.
Minutes	Governors' names Finance committee- pay and minutes Staff names and roles and hours Training and staff names	Principle set to be kept FOREVER- and other copies to be deleted after 3 years. 3 years 6 years after successful appointment		
Headteacher recruitment information	Applicants' names and contact details Interview and selection notes	6 years past the date the complaint was resolved and then review for further retention in case of		
Information from panels	Complaints			

	Disciplinary appeals Exclusions Admissions	contentious disputes Year of admission/ refusal plus one more.		
Photographs/ video recordings				
CCTV recordings Images of pupils and staff	Images of individuals Images of individuals	31 days after recording	Automated.	As per borough guidance.
Computing and Software				
RM - server/ PC log ons. Purple mash Education city partnership learning (phone system) Borough email system (elementary) Twinkl RM Parent hub	Pupils and staff first initial and surname Staff and pupil names - email address Generic school log in- no personal data. The only data we keep is telephone numbers and extension names, some of these names may be personal names however in our case most are just room numbers etc. All school emails email address, username, country and occupation, IP address. Parental contact details inc email, mobile number and app on phone or not	Removed at end of term that they leave the school Deleted when no longer needed, 5 years after date created	HR to email ICT team at the end of each term – ICT team to remove from system Elemetry to delete ICT team	As per borough guidance.
Health				
EHC plan Communication book Dieticians information and plans	minutes from meetings and EHC plans Names, ongoing requests for information/ support. Name, D.O.B, address,	As kept under NHS data storage guidance	Disposal/ destruction. Disposal/ destruction. Disposal/ destruction.	NHS data management protocols.

Management plans	management Name, D.O.B, address, condition, management		To be deleted in line with NHS protocols Disposal/ destruction.	
Email trail	Ongoing conversations regarding pupils	Only as long as needed		
Medication consent and administration forms	name, D.O.B, address, condition, management, record of administration			
After school Club				
Attendance and personal information regarding attendance at after school and holiday clubs – collated to send to borough	The spreadsheet contains the pupils Name, Date of Birth, Gender, Ethnicity, Primary SEN Need, Secondary SEN Need, Religion Postcode.	Collated and sent to borough	End of the academic year	In borough

Appendix 3 – Privacy Notice

1. Privacy notice for parents/carers.

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, Trinity School are the 'data controller' for the purposes of data protection law.

Our data protection officer is **Sandra Lee** (see 'Contact us' below).

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
- Ensure prompt communication with parents/carers
- Monitor and report on pupil progress
- Provide appropriate pastoral care
- Protect pupil welfare
- Assess the quality of our services
- 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. Our record retention schedule sets out how long we keep information about pupils.

The record retention policy is available online from the policy section of the school website or a paper version can be requested from the main school office. This can be done in person or by email. Please see the contact us section below.

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 – to meet our legal obligations to monitor the progress made by our pupils and ensure they are receiving a high standard of Education and care.
- The pupil's family and representatives – to support them to access the services that they require.
- Educators and examining bodies- to allow our pupils to receive qualifications which reflect their learning.
- Our regulator , e.g. Ofsted,
- Suppliers and service providers – to enable them to provide the service we have contracted them for, such as online learning platforms or data management software. This includes the use of Parenthub to facilitate communication with parents/carers.
- Financial organisations – such as those providing funding to the school.
- Central and local government
- Our auditors
- Health authorities – in order to provide ongoing excellent care,
- Security organisations

- Health and social welfare organizations – such as those providing respite or family support.
- Professional advisers and consultants- such as those who support our continuing professional development.
- Charities and voluntary organisations
- Police forces, courts, tribunals – in order to support the safety and wellbeing of our pupils and their families.

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 and early years 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.

Youth support services

Once our pupils reach the age of 13, we are legally required to pass on certain information about them to London Borough of Barking and Dagenham, as it has legal responsibilities regarding the education or training of 13-19 year-olds.

This information enables it to provide youth support services, post-16 education and training services, and careers advisers.

Parents/carers, or pupils once aged 16 or over, can contact our data protection officer to request that we only pass the individual's name, address and date of birth to the London Borough of Barking and Dagenham

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. However due to the additional needs of our pupils, we will continue to accept requests from parents regardless of age.

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 legal right to access to their child's **educational record**. To request access, please contact Sandra Lee – Data Protection Officer.

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 our **data protection officer, Sandra Lee**.

- Telephone : 0203 435 5955
- Email: office@trinity.bardaglea.org.uk
- In Person: please make a request via the school reception.
- Address: Trinity School,
Heathway,
Dagenham,
Essex,
RM10 7SJ

This notice is based on the [Department for Education's model privacy notice](#) for pupils, amended for parents and to reflect the way we use data in this school.

2. Privacy notice for pupils

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, Trinity school are the 'data controller' for the purposes of data protection law.

Our data protection officer is **Sandra Lee** (see 'Contact us' below).

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 in school assessment and progress as well as accreditation.
- 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 accredited course and assessments 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 have a record retention policy 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 obligations to share certain information with it, such as safeguarding concerns and exclusions
- The Department for Education – to meet our legal obligations to monitor the progress made by our pupils and ensure they are receiving a high standard of Education and care.
- Your family and representatives – to support them to access the services that they require.
- Educators and examining bodies- to allow you to receive qualifications which reflect your learning.
- Our regulator , e.g. Ofsted,
- Suppliers and service providers – to enable them to provide the service we have contracted them for, such as online learning platforms or data management software. This includes the use of Parenthub to facilitate communication with parents/carers.
- Financial organisations – such as those providing funding to the school.
- Central and local government
- Our auditors
- Health authorities – in order to provide ongoing excellent care,
- Security organisations
- Health and social welfare organizations – such as those providing respite or family support.
- Professional advisers and consultants- such as those who support our continuing professional development.
- Charities and voluntary organisations
- Police forces, courts, tribunals – in order to support the safety and wellbeing of our pupils and their families.

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.

Youth support services

Once you reach the age of 13, we are legally required to pass on certain information about you to the London Borough of Barking and Dagenham as it has legal responsibilities regarding the education or training of 13-19 year-olds.

This information enables it to provide youth support services, post-16 education and training services, and careers advisers.

Your parents/carers, or you once you're 16, can contact our data protection officer to ask us to only pass your name, address and date of birth to the London Borough of Barking and Dagenham

Your rights

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 **our data protection officer: Sandra Lee**

- Telephone : 0203 435 5955
- Email: office@trinity.bardaglea.org.uk
- In Person: please make a request via the school reception.
- Address: Trinity School,
Heathway,
Dagenham,
Essex,
RM10 7SJ

This notice is based on the [Department for Education's model privacy notice](#) for pupils, amended to reflect the way we use data in this school.

3. Privacy notice for staff

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, Trinity school are the 'data controller' for the purposes of data protection law.

Our data protection officer is **Sandra Lee** (see 'Contact us' below).

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
- Copy of DBS check
- Performance information
- Outcomes of any disciplinary and/or grievance procedures
- Absence data
- Attendance inc. entry/exit timing data as collected by the InVentry door access system.
- 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, accident 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 where:

- You have given us consent to use it in a certain way
- We need to protect your vital interests (or someone else's interests)

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 our record retention schedule

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 information about headteacher performance and staff dismissals
- The Department for Education
- Your family or representatives
- Educators and examining bodies
- Our regulator e.g. Ofsted,

- Suppliers and service providers – to enable them to provide the service we have contracted them for, such as RM for data management.
- Central and local government, predominantly the London borough of Barking and Dagenham for the purposes of HR and payroll.
- Our auditors
- Trade unions and associations
- Health authorities
- Security organisations
- Health and social welfare organisations
- Police forces, courts, tribunals
- Professional bodies
- Employment and recruitment agencies

Transferring data internationally

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

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 our **data protection officer: Sandra Lee**

- Telephone : 0203 435 5955
- Email: office@trinity.bardaglea.org.uk
- In Person: please make a request via the school reception.
- Address: Trinity School,
Heathway,
Dagenham,
Essex,
RM10 7SJ

This notice is based on the [Department for Education's model privacy notice](#) for the school workforce, amended to reflect the way we use data in this school.