Trinity Catholic High School

Data Protection Policy

Approved by:	Governing Board	**Date:** 22 October 2024
Last reviewed in:	June 2024	
Next review due by:	June 2025	

Contents

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 (DPA 2018)

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

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

It also reflects the ICO's guidance for the use of surveillance cameras and personal information.

In addition, this policy complies with 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	Any information relating to an identified, or identifiable, living individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of 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 and carers, pupils, staff, governors, visitors and others, and therefore is a data controller.

Trinity Catholic High School is registered with the ICO and has paid its data protection fee to the ICO, as legally required.

5. Roles and responsibilities

This policy applies to **all 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 (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 ICO.

Our DPO is:

The London Borough of Redbridge at: -

Email: dataprotection.schools@redbridge.gov.uk

The designated data protection lead at Trinity is Magine Taylor, who manages data protection on a day-to-day basis. Magine Taylor is contactable via:

Trinity Catholic High School,

Mornington Road,

Woodford Green,

IG8 0TP

Email: mtaylor@tchs.org.uk

Tel: 020 8504 3419

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 UK
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

6. Data protection principles

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

The principles say that personal data must be:

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

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

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have 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 or another person i.e., to protect someone's life
- The data needs to be processed so that the school, as a public authority, can **perform a task in the public interest or exercise its official authority**
- The data needs to be processed for the **legitimate interests** of the school (where the processing is not for any tasks the school performs as a public authority) or a third party, provided the individual's rights and freedoms are not overridden
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

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

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

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

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **consent**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of **legal rights**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation

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

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

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.

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

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which 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.

Where we transfer 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

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
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- The right to lodge a complaint with the ICO or another supervisory authority
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual
- The safeguards provided if the data is being transferred internationally

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

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

If staff receive a subject access request, they must immediately forward it to the Designated Data Protection Lead.

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 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.

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)
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

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

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts

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. We will take into account whether the request is repetitive in nature when making this decision.

If a requestor is dissatisfied with a response that has been provided, they can request a review of the original request. Please see schedule 7.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

9.4 Other data protection rights of the individual

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

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing which 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 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 Designated Data Protection Lead. If staff receive such a request, they must immediately forward it to the Designated Data Protection Lead.

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. (See schedule 1)

If the request is for a copy of the educational record, the school may charge a fee to cover the cost of supplying it.

This right applies as long as the pupil concerned is under 18.

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

Note that in the context of the Protection of Freedoms Act 2012, a "child" means a person under the age of 18.

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use fingerprints to receive school dinners instead of paying with cash or in some cases for registration), we will comply with the requirements of the Protection of Freedoms Act 2012.

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

Parents/carers and pupils have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils. For example, pupils can pay for school dinners in cash at each transaction if they wish.

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

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

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

12. CCTV

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

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

Enquiries about the CCTV system should be sent to the Director of Lower Site or the Director of Upper Site.

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/carers, or pupils aged 18 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers (or pupils where appropriate) have agreed to this.

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

- Within school on notice boards and in school publications, 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
- Year 11 school leavers year book

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph(s) / video(s) 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, with the exception of the year book, and newsletter.

See our Safeguarding and Child Protection Policy or our Photography Policy for more information on our use of photographs and videos.

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 Bard. Trinity Catholic High School recognises that AI has many uses to help pupils learn, but also poses risks to sensitive and personal data.

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

If personal and/or sensitive data is entered into an unauthorised generative AI tool, Trinity Catholic High School will treat this as a data breach, and will follow the personal data breach procedure outlined in schedule 6.

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 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 the UK and the safeguards for those, retention periods and how we are keeping the data secure

16. Data security and storage of records

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

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use.
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, or left anywhere else where there is general access.
- Where personal information needs to be taken off site, staff must sign it in and out from the school office.
- Passwords that are at least eight 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 and they should not reuse passwords from other sites.
- Encryption software is used to protect all portable devices and removable media containing personal data, such as laptops and USB storage 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 IT Policy).
- Staff should only access data about a data subject when there is a clear, work-related need to do so.
- Staff who are also a parent of a student at the school, must take particular care and must not access their child's information on an informal basis.
- 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 use confidential waste sacks for paper-based records, and overwrite or delete electronic files. We use a third party to safely dispose of records on the school's behalf. In doing so, we require the third party to provide sufficient guarantees that it complies with data protection law.

18. Personal data breaches

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

In the event of a suspected data breach, we will follow the procedure set out in the London Borough of Redbridge Data Security Breach Guidance and Procedure document.

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

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

19. Training

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

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

20. Monitoring arrangements

The Designated Data Protection Lead is responsible for monitoring and reviewing this policy.

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

Note: the annual review frequency here reflects the Department for Education's recommendation in its advice on statutory policies. This document has now been withdrawn, however the DfE's latest guidance does not include data protection in its list of statutory policies for maintained schools or academies, including free schools, however it is a legal requirement that schools have data protection policies and procedures in place.

21. Links with other policies

This data protection policy is linked to our:

- Freedom of Information Policy
- Safeguarding and Child Protection Policy
- IT Policy
- Information Security Policy
- Photography Policy
- Biometrics Data Guidance
- Data Security Breach Guidance and Procedure
- Privacy notices

Schedule 1: Disclosure of Educational Records relating to pupils

From time to time the school may receive subject access requests for copies of a pupil's educational record. The Data Protection Act 2018 defines an "educational record" as a record if information which:

a. is processed by or on behalf of the proprietor of, or a teacher at, a school in England and Wales (which includes an Academy);

b. relates to an individual who is or has been a pupil at the school; and

c. originated from, or was supplied by or on behalf of, any of the following persons:

   I. a teacher or other employee at the school (including an educational psychologist engaged by the proprietor under a contract for services);

   II. the pupil to whom the record relates;

   III. a parent, as defined by section 576(1) of the Education Act 1996, of that pupil.

The definition of "educational record" does not apply to information (notes, emails between teachers etc.) which is processes by a teacher solely for the teacher's own use i.e., uses for the purposes of teaching.

If a request is made for a pupil's file/educational records, the following information will be provided where it is available and may be redacted where necessary (if that information references third parties whose consent to disclosure has been withheld). Please note that information requested by a parent may be withheld if a pupil refuses consent to disclosure (and their consent is required). Information may also be withheld if an exemption applies in accordance with the Data Protection Act 2018 and reference will be made to any relevant exemption when a request is made.

A pupil's educational record will comprise the following:

1. The pupil's personal information such as; his/her unique pupil number; surname; former surname; forename(s); date of birth; gender; ethnic group; first language; nationality; country of birth; proficiency in English and emergency contact information.
2. Attendance records, including details of absences (authorised or otherwise).
3. All records of educational achievement including curricular records, examination records and annual school (or headteacher) reports.
4. All SEN statements or Educational Health and Care Plans, including any supporting professional reports, annual reviews and personalised learning plans.
5. Any individual Health Plan, including associated medical reports.
6. Any Child Protection Record.
7. Any behaviour log and /or accident reports, including any supplementary information provided in connection therewith.
8. Parental communications.
9. Third party communications, including other agencies and regulatory bodies.

Schedule 2: Personnel files relating to employees

If we are asked to disclose an employee's personnel/HR records, the following information will be provided where it is available and may be redacted where necessary. Information may be withheld if an exemption applies in accordance with the Data Protection Act 2018:

1. [Personal contact details such as name, title, addresses, telephone numbers, and email addresses.]
2. [Date of birth.]
3. [Gender.]
4. [Marital status and dependants.]
5. [Next of kin and emergency contact information.]
6. [National Insurance number.]
7. [Bank account details, payroll records and tax status information.]
8. [Salary, annual leave, pension and benefits information.]
9. [Teacher Reference Number.]
10. [Start date.]
11. [Location of employment or workplace.]
12. [Copy of identification.]
13. [Recruitment information.]
14. [Employment records (including job titles, work history, working hours, training and professional memberships).]
15. [Compensation history, including pensions.]
16. [Performance information.]
17. [Disciplinary and grievance information, including warnings issued.]
18. [Photographs.]
19. [Information about race or ethnicity, religious beliefs, sexual orientation and political opinions.]
20. [Trade union membership.]
21. [Information about health, including any medical condition, health and sickness records.]
22. [Biometric data.]
23. [Information about Disclosure and Barring Service checks.]

Schedule 3: Personal data of Governors

If we are asked to disclose a file the school holds about a governor, the following information will be provided where it is available and may be redacted where necessary. Information may be withheld if an exemption applies in accordance with the Data Protection Act 2018:

1. [Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses.]
2. [Date of birth.]
3. [Gender.]
4. [Occupation.]
5. [Start date.]
6. [Skills and experience.]
7. [Recruitment information.]
8. [Information relating to the governor's religious belief where relevant.]
9. [Copy of identification.]
10. [Information about pecuniary or business held by the governor or their family members.]
11. [Information about other posts held by the governor.]
12. [Information about conduct.]
13. [Photographs.]
14. [Information about Disclosure and Barring Service checks.]

Schedule 4: Consent Form Year 7-11

Biometric Data Consent: Fingerprint data is retained solely by the school for the administration of our cashless catering system, library loans and registration data. We are required to ask for your permission to collect and use this data. Please indicate your approval or objection. **My child can use their fingerprints to access services such as the canteen.**	**Please delete as necessary** **Yes/No**
Parish Levy: Data is collected to ascertain the number of students residing in each parish. **I give permission for my child's name and address to be shared with the Brentwood Diocese.**	**Please delete as necessary** **Yes/No**
Images Consent Collection: From time to time, we may use images of students for internal and external purposes to celebrate their achievements and the achievement of the school. **Images of my child can be used on the school website (and newsletter if electronic)** **Images of my child can be used in newsletters and printed literature** **Images of my child can be used in internal displays** **Images of my child can be used by local and national media outlets such as newspapers** **Images of my child can be used on social media such as Twitter, Instagram and Facebook** **Video images of my child can be used for promotional purposes**	**Please delete as necessary** **Yes/No** **Yes/No** **Yes/No** **Yes/No** **Yes/No** **Yes/No**
School Work: **I give consent for work produced by my child to be shown on the school website (note: we will also always ask your child for their permission for any piece of work we would like to put on the website).**	**Please delete as necessary** **Yes/No**
Representing the School – School Transport / Physical Education Lessons: Our school has an extensive off-site playing field. Your son/daughter will travel to and from this facility as appropriate, in relation to their Physical Education via coach transport provided by the London Borough of Redbridge. Your son/daughter may be asked to represent Trinity or to take part in educational visits that involve having to travel using school transport. Please confirm that you give your permission for your son/daughter to travel with members of the school staff and using school transport. **I give permission for my child to travel to and from events using school transport**	**Please delete as necessary** **Yes/No**
Other information: Please write here any additional information that you would like us to know:	

Student Name: **Year / Form Group:**

Parent Signature: _____

I confirm my child has seen the form ☐

You have the right to withdraw consent at any time by contacting the school office for the relevant key stage.

Data Protection: Please note; the details provided on this form may be used in accordance with the school's data protection policy as described in our Curriculum Handbook. We adhere with data protection legislation and will not keep your information longer than necessary. For more information, please see our privacy notice.

Schedule 5: Consent Form Year 12 – 13

Biometric Data Consent: Fingerprint data is retained solely by the school for the administration of our cashless catering system and in some cases registration data. We are required to ask for your permission to collect and use this data. Please indicate your approval or objection. **I give permission for my fingerprints to be used to access services such as the canteen and registration.**	**Please delete as necessary** **Yes/No**
Parish Levy: Data is collected to ascertain the number of students residing in each parish. **I give permission for my name and address to be shared with the Brentwood Diocese.**	**Please delete as necessary** **Yes/No**
Images Consent Collection: From time to time, we may use images of students for internal and external purposes to celebrate their achievements and the achievement of the school. **Images of me can be used on the school website (and newsletter if electronic)** **Images of me can be used in newsletters and printed literature** **Images of me can be used in internal displays** **Images of me can be used by local and national media outlets such as newspapers** **Images of me can be used on social media platforms such as Twitter, Instagram and Facebook** **Video images of me can be used for promotional purposes**	**Please delete as necessary** **Yes/No** **Yes/No** **Yes/No** **Yes/No** **Yes/No** **Yes/No**
School Work: **I give consent for work I produce to be shown on the school website (note: we will also always ask for your permission for any piece of work we would like to put on the website).**	**Please delete as necessary** **Yes/No**
Representing the School – School Transport / Physical Education Lessons: Our school has an extensive off-site playing field. You may be required to travel to and from this facility as appropriate, in relation to your Physical Education via coach transport provided by the London Borough of Redbridge. You may be asked to represent Trinity or to take part in educational visits that involve having to travel using school transport. Please confirm that you give your consent to travel with members of the school staff and using school transport. **I give my consent to travel to and from events using school transport**	**Please delete as necessary** **Yes/No**
Other information: Please write here any additional information that you would like us to know:	

Student Name: **Year / Form Group:**

Student Signature: _____

I confirm my parent/guardian has seen the form ☐

You have the right to withdraw consent at any time by contacting the relevant sixth form office.

Data Protection: Please note; the details provided on this form may be used in accordance with the school's data protection policy as described in our Curriculum Handbook. We adhere with data protection legislation and will not keep your information longer than necessary. For more information, please see our privacy notice.

Schedule 6: Data Breach Reporting Procedure

A personal data breach is “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed”. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing data.

Examples of data breaches can include:

- access by an unauthorised third party to confidential or highly confidential school data;
- human error/sending personal data to an incorrect recipient;
- equipment failure/computing devices containing personal data being lost or stolen;
- alteration of personal data without permission;
- unforeseen circumstances such as a fire or flood;
- hacking attack
- ‘blagging’ offences where information is obtained by deceit

The following process must be followed to ensure incidents are reported in a timely manner and can be properly investigated.

1. If Trinity Catholic High School (TCHS), or any employee, discovers or is made aware of a security incident, the headteacher (Dr Doherty) and the member of the senior leadership with data protection responsibility (Nathan Barnes) should be informed immediately.

2. If the data breach is caused by an email sent only to students/staff at the school, the IT department should be contacted immediately as they might be able to retract/delete the email before it is read.

3. The Information Risk Officer (IRO) and the Designated Data Protection Lead will be informed of the incident by Dr Doherty. On so doing, investigations will be carried out to establish the nature and severity of the personal data breach and to contain the incident and recover the information (where possible).

4. The member of staff involved in the breach will provide a written report of the incident to the Designated Data Protection Lead, which includes; a description of the incident, chronology of the events, the lessons learnt and the actions taken to solve the problem or changes made to processes to reduce the risk of the breach happening again.

5. Where TCHS acts as a data processor for another organisation, the Designated Data Protection Lead will immediately notify the controller of any personal data breach that has occurred with the data they process on the organisation’s behalf.

6. On completion of the investigation, an assessment of the likely risk to individuals will be conducted, to establish the likelihood and severity of the actual or potential risk or negative consequence to the affected individuals.

7. If on assessing the risk to individuals, the IRO/Designated Data Protection Lead concludes the breach is not likely to result in a risk to individuals’ rights and freedoms; the breach, the decision not to notify and reasons will be documented in the data protection reporting log and on the borough’s ISI completion form.

8. Where there is a very likely or actual or potential high risk to individuals, UK GDPR requires organisations to notify the individuals affected. This should be carried out in a tactful way not to cause unnecessary distress by the line manager of the person involved in the breach, or to a delegated member of staff. Calling or visiting the individuals or parent/guardian or carer of the individuals affected should be considered where there is an actual or potential immediate high risk, harm or likely to have a significant effect on them.

9. The borough notification form and ISI completion form will be completed with the information gathered from the investigation process and breach report by the Designated Data Protection Lead, and will be reviewed by the IRO. The form will be signed off by the line manager of the person involved in the breach, prior to the form(s) being submitted to the Redbridge Data Protection Team.

10. Following the submission of the notification and completion forms to the Redbridge Data Protection Team, the Information Governance Lead will advise if the Data Protection Officer (DPO) will need to notify the Information Commissioner's Office (ICO) about the breach. If the DPO is required to notify the ICO this will be carried out within 72 hours of becoming aware of the breach.

11. The Information Governance Lead will inform the school once the data breach process is complete.

12. All breaches will be documented and records maintained by the Designated Data Protection Lead at Trinity Catholic High School.

Schedule 7: Subject Access Request Internal Review Procedure

Trinity Catholic High School following the receipt of a subject access request, will aim to provide a response to the data subject or representative within the statutory timeframe of one calendar month.

If the requestor is dissatisfied with the response and would like a review of what has been submitted, the following procedure will be applied.

NB. A request for a review of a subject access request will need to be received within 60 days of the response being provided.

1. Once the complaint or request for a review of the subject access request has been received from the requestor, the 20-working day timeframe will begin.

2. The line manager of the staff member who provided the response, will be nominated to lead the review, if they were not involved with the initial request process. If the nominated line manager had any involvement in the original request, the Headteacher will nominate an alternative senior manager to complete the review.

3. A letter will be sent to the reviewer, within 24 hours to acknowledge receipt of the request, to confirm the time scales for the response to the review.

4. The review process of the original request will include the following:

    - A review of the original request.
    - A review of the material collected, including what was provided and what was withheld or redacted.
    - Discussions with staff involved in the original request or information holders about the processes that were followed.
    - Clarification will be sought about the reasoning behind refusal and any exemptions used under the Data Protection Act 2018.
    - A decision will be made about whether the request was handled appropriately and if the material that should have been released was released.
    - Advice will be sought from the Redbridge Information Governance Lead where necessary.
    - A report will be written summarising the review and detailing the outcome. If the complaint is upheld, the rationale will be explained to the requestor and any additional disclosures made. If the complaint is not upheld, the rationale will be explained to the requestor.

5. The reviewer will send the response to the review within the 20-working day timeframe, either amending or supporting the original decision.

6. The requestor will be informed of their right to appeal to The Information Commissioner, if they are still dissatisfied.