CORPUSCHRISTI
CATHOLIC ACADEMY TRUST
We are His body, living and learning as one.

DATA PROTECTION POLICY

Document Record	
Policy title	Data Protection Policy
Date approved	2022
Review period	Annually
Date last reviewed	April 2025
Approved by	CEO
Purpose of policy	To establish procedures to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with UK data protection law.
Author	DPO

This policy will be published on the Trust's website

Contents

1. **Introduction**

   i. Corpus Christi Catholic Academy Trust (referred to hereafter as the Trust) has developed a number of key policies to ensure that the principles of Catholic Social Teaching in relation to respect, objectivity and belief in the dignity of the individual become embedded into every aspect of school life and these policies are reviewed regularly in this regard.

   ii. The distinctiveness of a Catholic school is lived out through the care and respect shown for each other. All staff are principally responsible for a Catholic school's ability to put into effect its ethos, aims and projects.

   iii. The Trust supports the creation of a safer culture to ensure the schools are an environment where everyone is safe and happy by reinforcing the safeguarding and well-being of children and young people in its care.

   iv. The Trust is mindful of its obligations and duties under the Equality Act 2010 and will be mindful of the protected characteristics in the Equality Act (i.e. age, disability, gender, gender reassignment, race, religion or belief, sexual orientation, pregnancy, maternity and marriage or civil partnership) in the application of this code of conduct.

   v. The Trust may take positive action to help redress any imbalances that may have arisen as a result of past discrimination or disadvantage. The aim of this positive action is to ensure that people from previously excluded groups are included.

   vi. This policy complies with the Data Protection Act 2018 (DPA 2018) and intends to comply with the Surveillance Camera Code of Practice 2013.

   vii. This policy meets the requirements of the UK General Data Protection Regulations (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.

   viii. This policy meets the requirements of the Protection of Freedoms Act 2012 when referring to the use of biometric data. This policy reflects the ICO's code of practice for the use of surveillance cameras and personal information.

2. **Scope of the policy**

   i. This policy applies to all employees who work at schools within the Trust.

   ii. This policy applies to self-employed staff, trainees, contractors, external consultants, volunteers, agency staff and governors, whether by direct contract with the Trust or otherwise. This policy also applies to parents, students, members of the public and users of the school or Trust website.

   iii. This policy should be read alongside relevant Trust Policies and Procedures.

   iv. This policy complies with the Trust's funding agreement and articles of association.

   v. Unless indicated otherwise, all references to "Governing Body" apply to school's Local Governing Body or Interim Management Board.

3. **Principles**

i. The Trust is required to establish procedures to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with UK data protection law.

ii. This policy is designed to meet statutory obligations when dealing with all data, whether it is in paper or electronic format, and sets out how the Trust deals with personal data, including data subject access requests, and employees' obligations in relation to personal data.

iii. The Trust collects and uses certain types of personal information about employees, students, parents and other individuals who come into contact with each school in the Trust in order to provide education and associated functions. In addition, the Trust may be required by law to collect and use certain types of information to comply with statutory obligations of Local (Education) Authorities (LAs), government agencies and other bodies.

4. **Definitions**

i. List of 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.

5. **Roles and responsibilities**

i. Corpus Christi Catholic Academy Trust is a legal entity and is registered with the Information Commissioner's Office (ICO). The Trust processes personal data relating to parents, pupils, staff, governors, visitors and others and therefore is the data controller. The Trust is therefore ultimately responsible for ensuring that its schools comply with all relevant data protection obligations. the data protection policy and any data breaches.

ii. The Trust requires that all employees have a confidentiality clause in their contracts of employment.

iii. The Trust has identified a data protection officer (DPO) to be responsible for overseeing the implementation of this policy, monitoring compliance with data protection law, developing related policies and guidelines where applicable.

iv. The Trust has delegated the day-to-day responsibility for the effective operation of this policy to the school's Local Governing Body.

v. The DPO will provide an annual report of their activities directly to the Trust Executive Board, and where relevant, report to the Trust Board their advice and recommendations on data protection issues.

vi. The Local Governing Body is responsible for monitoring the school's compliance with all relevant data protection obligations.

vii. The Headteacher acts as the representative of the data controller on a day-to-day basis and will ensure that employees comply with this policy.

viii. Employees will comply with this policy. In the course of their role, staff are often privy to sensitive and confidential information about the school, colleagues, pupils, parents and carers. Information must never be disclosed to anyone without the relevant authority.

ix. All staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy;
- Informing their school of any changes in their personal data, such as 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.

x. Employees' obligations regarding personal information:

- If an employee acquires any personal information in the course of their duties, they must ensure that:
    - The information is accurate and up to date, insofar as it is practicable to do so;
    - The use of the information is necessary for a relevant purpose and that it is not kept longer than necessary and;
    - The information is secure.
- In particular, an employee should ensure that they:
    - Do not share passwords or access data under someone else's credentials;
    - Use password-protected and encrypted software for the transmission and receipt of emails;
    - Securely store records, files and data; and
    - Ensure that information is securely disposed of in a shredder and not a wastepaper basket or recycle bin.
- If an employee acquires any personal information in error by whatever means, they shall inform the Headteacher immediately and, if it is not necessary for them to retain that information, arrange for it to be handled by the appropriate individual within the Trust and/or DPO.

xi. All employees are under an obligation to ensure that they have regard to the data protection principles and this policy when accessing, using or disposing of personal information. Failure to observe this policy may result in an employee incurring personal criminal liability. It may also result in disciplinary action up to and including dismissal. For example, if an employee accesses another employee's employment records without the requisite authority, the

Trust may treat this as gross misconduct and instigate its disciplinary procedures. Such gross misconduct may also constitute a criminal offence

6. **Data protection principles**

   i. The UK GDPR is based on data protection principles which must be complied with when handling personal data. These principles require 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 is it appropriately secure.

7. **Audits and impact assessments**

   i. The Trust will regularly conduct reviews and audits to test its privacy measures and ensure compliance.

   ii. The Trust and schools within the Trust will complete 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).

   iii. The Trust and schools will integrate data protection into internal documents including this policy, and any related policies and privacy notices.

   iv. The Trust will put appropriate safeguards in place if it transfers any personal data outside of the UK, where different data protection laws may apply.

   v. The Trust will maintain an internal record of the type of data, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the UK and the safeguards for those, retention periods and how we are keeping the data secure.

8. **Collecting personal data**

   i. Lawfulness, fairness and transparency

   The Trust will only process personal data where it has one of the six 'lawful bases' (legal reasons) to do so under protection law:

   1) 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;

   2) The data needs to be processed so that the school can **comply with a legal obligation**;

   3) The data needs to be processed to ensure the **vital interests** of the individual or another person i.e. to protect someone's life;

4) 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**;
5) 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;
6) 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, the Trust will also meet one of the special categories for processing under data protection law:

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

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

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

- The data needs to be processed for reasons of **substantial public interest** as defined in legislation.

Whenever the Trust first collects data directly from individuals, it will provide them with the relevant information required by data protection law.

The Trust will always consider the fairness of its data processing. The Trust will ensure it does 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.

ii. Limitation, minimisation and accuracy

The Trust will only collect personal data for specified, explicit and legitimate reasons. The Trust will explain these reasons to the individuals when it first collects their data.

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

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

The Trust 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 Trust's record retention schedule.

9. **Sharing personal data**

i. The Trust will not normally share personal data with anyone else without consent, but there are certain circumstances where it 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 its staff at risk;
- The Trust needs to liaise with other agencies, however, it will seek consent as necessary before doing this;
- Suppliers or contractors to the Trust need data to enable the Trust to provide services to its 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.

ii. The Trust will also share personal data with law enforcement and government bodies where it is legally required to do so.

iii. The Trust may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of its pupils or staff.

iv. Where the Trust transfers personal data internationally, it will do so in accordance with UK data protection law, including the updated UK-US Data Bridge and EU-UK Adequacy Decision.

v. Where personal data is shared it will be in line with the Trust's Sharing Personal Data Policy and Procedure.

vi. Government guidance on information sharing for people who provide safeguarding services to children, young people, parents and carers can be found here: https://assets.publishing.service.gov.uk/media/623c57d28fa8f540eea34c27/Information_sharing_advice_practitioners_safeguarding_services.pdf

10. Subject access requests (SAR) Employees

i. The Data Protection Officer is responsible for dealing with subject access requests. If any SAR's are received in any form, staff must immediately inform the DPO.

ii. An employee has the right to access information kept by the Trust about themselves. This could include:

- Confirmation that their data is being processed;
- Access to a copy of that data;
- The purposes of the data processing;
- The categories of personal data concerned;
- Who the data has been with, 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.

iii. Subject access requests can be submitted in any form, however, the DPO may be able to respond more quickly to requests made in writing and include:

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

11. Subject access requests (SAR) Children

i. 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.

ii. 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 schools within the Trust 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. It may be the case that the school will discuss the request with the student and take their views into account when making a decision. A student with the competency to understand can refuse consent to the request for their records being disclosed to their parent or guardian.

iii. 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.

12. **Responding to subject access requests (SAR)**

i. When responding to requests, the DPO or school:

- May ask the individual to provide two 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 (apart from iii);
- May request proof of their entitlement to see the information before disclosure (such as when a child's permission is sought);
- May tell the individual that an extension is required, and will comply within 3 months of receipt of the request, where a request is complex or numerous. The DPO will inform the individual of this within 1 month, and explain why the extension is necessary.

ii. The Trust 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 it cannot reasonably anonymise, and it 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.

iii. If the request is unfounded or excessive, the Trust may refuse to act on it, or charge a reasonable fee to cover administrative costs. The Trust will consider whether the request is repetitive in nature when making this decision.

iv. The Trust will allow the individual access to hard copies of any personal information. However, if this involves a disproportionate effort on the part of the Trust, the employee shall be invited to view the information on-screen or inspect the original documentation at a place and time to be agreed by the Trust.

v. When a request is refused, the Trust will inform the individual why, and advise them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

vi. The Trust may reserve its right to withhold an individual's right to access data where any statutory exemptions apply.

13. **Other data protection rights of the individual**

i. 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, 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).

ii. 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.

14. **Parental requests to see the educational record**

i. As a Trust with academy status, the Education (Pupil Information) (England) Regulations 2005 does not apply in relation to a pupil's education record being available for inspection by a parent. There is no legal equivalent right to access a pupil's education record and therefore, the Trust will consider each case on its own merit.

ii. The Education (Independent School Standards) Regulations 2014 (part 6f) applies. Under these Regulations, academies must provide an annual written

report of each registered pupil's progress and attainment in the main subject areas taught, to the parents of that registered pupil (except that no report need be provided where the parent has agreed otherwise).

iii. The Trust will not communicate anything to a parent which it could not communicate to the student him/herself under the Act.

iv. The meaning of a parent is wider than the definition of who has parental responsibility. Parent means a person with parental responsibility or who has care of a child. Therefore, where a child is living with grandparents, the grandparents have a right to see the child's educational records even though they may not have parental responsibility. Information and guidance regarding parental responsibility can be found on the website www.gov.uk and the definition of a parent is defined in Section 576 of the Education Act 1996.

15. **Biometric recognition systems**

i. Where schools in the Trust use pupils' biometric data as part of an automated biometric recognition systems (for example, pupils use finger prints to receive school dinners instead of paying with cash), the Trusts will comply with the requirements of the Protection of Freedoms Act 2012;

ii. 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 it takes any biometric data from their child and first process it;

iii. Parents/carers and pupils have the right to choose not to use the school's biometric systems. The school will provide alternative means of accessing the relevant services for those pupils;

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

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

vi. Where staff members or other adults use the school's biometric systems, 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.

16. **CCTV**

i. **Aims**

- The Trust takes its responsibility towards the safety of staff, visitors and pupils seriously and uses CCTV cameras to monitor instances of aggression or physical damage to its community or property and to monitor any unauthorised access to any of its sites.
- The Trust manages and regulates the use of surveillance and CCTV systems which captures moving and still images of individuals who can be identified. The Trust justifies its use of such systems to ensure:
    - Compliance with data protection legislation;

- The images captured are useable for the purposes required;
- Assurance is given to those persons whose images are being captured that they are handled in accordance with the data protection legislation.

ii. **Scope of the CCTV system**

- Definitions:
  - Surveillance – monitoring the movements and behaviour of individuals; this can include video, audio or live footage. For the purpose of this policy only video and audio footage will be applicable;
  - Overt surveillance – any use of surveillance for which authority does not fall under the Regulation of Investigatory Powers Act 2000;
  - Covert surveillance – any use of surveillance which is intentionally not shared with the subjects it is recording. Subjects will not be informed of such surveillance;
- CCTV is intended for use in public areas. The Trust does not condone the use of covert surveillance when monitoring the school's staff, pupils or visitors. Covert surveillance will only be operable in extreme circumstances. Overt surveillance footage will be clearly signposted around the Trust schools.
- CCTV cameras will not be present in areas that intrude on an individual's privacy such as changing facilities.
- The system comprises a number of fixed and dome cameras located around the school sites. All cameras are accessed from individual schools' centralised Cloud Server and images are only available to selected senior staff via the server as well as remotely via an App.
- The CCTV system is owned by the school and all members of the school community will be made aware of the existence of the CCTV system in appropriate publications.
- The Trust does not need to ask individuals' permission to use CCTV, but schools make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use to ensure that all staff and visitors are aware of this.

iii. **Objectives of the use of surveillance and CCTV systems**

- To maintain a safe environment and increase personal safety and wellbeing of pupils, staff and visitors.
- To deter criminal acts, violent behaviour and damage to the school buildings and assets.
- To encourage good behaviour in the student body and deterring anti-social behaviour.

- To assist the police in identifying persons who have committed an offence

iv. **Operation of the surveillance and CCTV systems**

- The Scheme will be administered and managed by the headteacher, in accordance with the principles and objectives expressed in the code.
- The day-to-day management will be the responsibility of both the Leadership Team and the Site Team/ICT Team
- The system will only be staffed by appropriate staff members. Access to the CCTV system will be strictly limited.
- The CCTV system will be operated 24 hours each day, every day of the year.
- All staff with access to the system must ensure that they adhere to any guidance or security precautions.
- The ICT Team will check and confirm the efficiency of the system and in particular that the equipment is properly recording and that cameras are functional.
- If out of hours emergency maintenance arises, the system operators must be satisfied of the identity and purpose of contractors before allowing access.
- Other administrative functions will include maintaining storage of images, filing and maintaining occurrence and system maintenance logs.
- There will be periodic checks on the quality of the images being collected and whether the dates and times are accurate.
- Unless required for evidential purposes, the retention period of any images recorded by our CCTV footage is 30 days.
- Footage will be automatically destroyed on the server system after 30 days, when images are overwritten with new data. Images that have been copied on to an external storage device (e.g. a memory stick or DVD) for the purposes of an investigation will be destroyed after the investigation is complete, in line with the retention schedule of the GDPR policy. If images are stored on an external storage drive they will be locked in the safe.
- Images will only be viewed in an area where they cannot be accidentally viewed by others. Where a copy of images has been made for evidential purposes, subsequent viewings may take place in other suitably secure locations, e.g. the Headteachers office.

v. **Access**

- Under the Data Protection Act 2018, individuals have the right to obtain confirmation that their personal information is being processed.
- Systems containing images belong to and remain the property of the Trust.

- Requests by persons outside of the Trust for viewing or copying disks or digital recordings, will be assessed by the Data protection Officer and considered on a case by case basis with close regard to the data protection legislation.
- Releasing of recorded images to third parties will only be permitted in the following limited and prescribed circumstances and to the extent required permitted by law:
    - The police – where the images recorded would assist in a specific criminal inquiry;
    - Prosecution agencies – such as the Crown Prosecution Service (CPS);
    - Relevant legal representatives – such as lawyers and barristers;
    - Persons who have been recorded and whose images have been retained where disclosure is required by virtue of data protection legislation and the Freedom of Information Act 2000.

17. **Body-Worn Video (BWV) equipment**

vi. **Aims**

- The Trust takes its responsibility towards the safety of staff, visitors and pupils seriously and uses BWV equipment to support the safety of lettings staff, pupils and the wider school community, as well as to deter and record incidents of concern or potential criminal behavior.
- The Trust manages and regulates the use of surveillance and BWV equipment which captures moving and still images of individuals who can be identified. The Trust justifies its use of such systems to ensure:
    - Compliance with data protection legislation;
    - The images captured are useable for the purposes required;
    - Assurance is given to those persons whose images are being captured that they are handled in accordance with the data protection legislation.

vii. **Scope of the Body-Worn Video equipment**

- Definitions:
    - Surveillance – monitoring the movements and behaviour of individuals; this can include video, audio or live footage.
    - Overt surveillance – any use of surveillance for which authority does not fall under the Regulation of Investigatory Powers Act 2000;
    - Covert surveillance – any use of surveillance which is intentionally not shared with the subjects it is recording. Subjects will not be informed of such surveillance;
- BWV equipment is intended for use in public areas. The Trust does not condone the use of covert surveillance when monitoring the school's staff, pupils or visitors. Covert surveillance will only be operable in extreme circumstances. Overt surveillance footage will be clearly signposted around the Trust schools.

- BWV equipment will not be present in areas that intrude on an individual's privacy such as changing facilities.
- The BWV equipment is owned by the school and all members of the school community will be made aware of the existence of the BWV equipment in appropriate publications.
- The Trust does not need to ask individuals' permission to use BWV equipment, but schools make it clear where individuals are being recorded. BWV equipment is clearly visible and accompanied by prominent signs explaining that BWV equipment is in use to ensure that all staff and visitors are aware of this.

viii. **Objectives of the use of Body-Worn Video equipment**

- To maintain a safe environment and increase personal safety and wellbeing of pupils, staff and visitors.
- To deter criminal acts, violent or aggressive behaviour and damage to the school buildings and assets.
- To provide accurate and unbiased recording of events for the purpose of incident investigation, disciplinary procedures or law enforcement.
- To assist the police in identifying persons who have committed an offence.
- BWV equipment will not be used for general surveillance and must only be activated in specific situations where recording is necessary and proportionate.

ix. **Operation of the Body-Worn Video equipment**

- The BWV equipment will be administered and managed by the headteacher, in accordance with the principles and objectives expressed in the code.
- The day-to-day management will be the responsibility of both the Leadership Team and the School Business Manager.
- The system will only be staffed by appropriate staff members. Access to the BWV equipment will be strictly limited.
- All staff with access to the system must ensure that they adhere to any guidance or security precautions.
- The BWV equipment will be operated after school hours only, every day of the year.
- BWV equipment will be worn openly and will clearly display that recording may take place.
- All footage from the BWV equipment will be stored on an encrypted device.
- Audio recording will only be used when justified, and the use of both audio and video will be in line with a legitimate purpose under UK GDPR Article 6(1)(f) – legitimate interests.

- Recording on the BWV equipment will be limited to the duration necessary to capture the relevant incident or interaction and must not continue unnecessarily.
- Operation of the BWV equipment intends to comply with the Surveillance Camera Code of Practice 2013.
- Footage on the BWV equipment will only be viewed in an area where they cannot be accidentally viewed by others. Where a copy of images has been made for evidential purposes, subsequent viewings may take place in other suitably secure locations, e.g. the Headteachers office.

x. **Access**

- Access to BWV footage is strictly limited to authorised personnel only, including the Data Protection Officer (DPO).
- Under the Data Protection Act 2018, individuals have the right to obtain confirmation that their personal information is being processed.
- Systems containing images belong to and remain the property of the Trust.
- Requests by persons outside of the Trust for viewing or copying disks or digital recordings, will be assessed by the Data protection Officer and considered on a case by case basis with close regard to the data protection legislation.
- Releasing of recorded images to third parties will only be permitted in the following limited and prescribed circumstances and to the extent required permitted by law:
    - The police – where the images recorded would assist in a specific criminal inquiry;
    - Prosecution agencies – such as the Crown Prosecution Service (CPS);
    - Relevant legal representatives – such as lawyers and barristers;
    - Persons who have been recorded and whose images have been retained where disclosure is required by virtue of data protection legislation and the Freedom of Information Act 2000.

18. **Photographs and videos**

i. As part of school activities, photographs and images of individuals will be recorded and is done so in line with data protection principles.

ii. **Trust primary schools** will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. The schools will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, schools will ask that photos or videos with other pupils are not

shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this.

iii. **Trust secondary schools** 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 schools need parental consent, schools will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where schools don't need parental consent, they 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, schools 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.

iv. Where a school takes photographs and videos, 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

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

vi. 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.

19. **Security and storage of data and records**

i. The Trust will ensure that appropriate technical and organisational measures shall be taken against unauthorised or unlawful access or processing of personal data and against accidental loss or destruction of, or damage to, personal data.

ii. Schools will ensure that personal information about an individual is securely retained. Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data should be kept in locked filing cabinets/secure areas. 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.

iii. 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 that they should not reuse passwords from other sites.

iv. Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices.

v. Staff must not take any personal information away from the school's premises or their workplace, unless they have obtained the prior consent of the Headteacher to do so.

vi. Staff who have been granted approval to take personal information from the school premises may take only necessary and certain records off site. These are documents relating to certain meetings that cannot be held on site, such as meetings with specific health and safeguarding professionals.

vii. Staff taking records off site must ensure that they comply with the Trust's Off-site working policy and will not leave their laptop, other device or any hard copies of documents on the train, in the car or any other public place. Staff must also take care when observing the information in hard copy or on-screen that such information is not viewed by anyone who is not legitimately privy to that information

viii. Staff, pupils and governors who access information on their personal devices are expected to follow the same security procedures as for school-owned equipment and in line with the Trust's ICT and Internet Acceptable Use Policy.

20. Retention and disposal of records and data

i. The Trust will apply its Retention and Disposal of Records and Data Policy to ensure that information is not held longer than is necessary, in line with the retention timeframes set out in the IRMS toolkit (Academies).

ii. The Trust has a duty to retain some employee and student data for a period of time following their departure from their school, mainly for legal reasons, but also for other purposes such as being able to provide references. Different categories of records and data will be retained for different periods of time.

iii. 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 the Trust cannot, or does not, need to rectify or update it. In these cases, the Trust will shred paper-based records and overwrite or delete electronic files. The Trust may also use a third party to safely dispose of records on the school's behalf and requires the third party to provide sufficient guarantees that it complies with data protection law.

21. Training

i. The Trust provides training on data protection issues to staff and governors who handle personal information in the course of their duties and as part of the induction process.

ii. The Trust will provide refresher training where changes to legislation, guidance or the school's processes make it necessary. If any individual considers that they would benefit from refresher training, or as part of continuing professional development, this will be provided.

22. Breaches

i. This procedure is based on guidance on personal data breaches produced by the Information Commissioner's Office (ICO). On finding or causing a

breach, or potential breach, the staff member, governor or data processor must immediately notify the data protection officer (DPO).

ii. 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.

iii. Staff and governors will cooperate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation.

iv. If a breach has occurred or it is considered to be likely that is the case, the DPO will alert the headteacher and the chair of governors.

v. The DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the DPO with this where necessary, and the DPO should take external advice when required (e.g. from IT providers).

vi. The DPO will assess the potential consequences (based on how serious they are and how likely they are to happen) before and after the implementation of steps to mitigate the consequences.

vii. The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's self-assessment tool

viii. The DPO will document the decisions, in case the decisions are challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored in the Trust's Leadership folder.

ix. Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of the school's awareness of the breach. As required, the DPO will set out:

- A description of the nature of the personal data breach including, where possible:
    - The categories and approximate number of individuals concerned;
    - The categories and approximate number of personal data records concerned;
- The name and contact details of the DPO;
- A description of the likely consequences of the personal data breach;
- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individuals concerned.

x. If all the above details are not yet known, the DPO will report as much as they can within 72 hours of the school's awareness of the breach. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.

xi. Where the school is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:

- A description, in clear and plain language, of the nature of the personal data breach;
- The name and contact details of the DPO;
- A description of the likely consequences of the personal data breach;
- A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

xii. The DPO will consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals, for example, the police, insurers, banks or credit card companies.

xiii. 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).

xiv. Records of all breaches will be stored in the Trust's Leadership folder.

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

23. Actions to minimise the impact of data breaches

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

ii. 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 attempt to recall it from external recipients and remove it from the school's email system (retaining a copy as evidence if required.
- In any cases where the recall is unsuccessful or cannot be confirmed as successful, the DPO will consider whether it is appropriate to contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way.
- The DPO will endeavor to obtain a written response from all the individuals who received the data, confirming that they have complied with this request.
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.

iii. If safeguarding information is compromised, the DPO will inform the designated safeguarding lead and discuss whether the school should inform any of its safeguarding partners.

iv. Other types of breach that the DPO will consider include:

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

Appendix A Certificate

Data Protection Registration Certificate

Corpus Christi Catholic Academy Trust

Saint Paul's Catholic High School
Firbank Road
Newall Green
Wythenshawe
M23 2YS

Registration reference: ZA055222
Date registered: 23 May 2014
Registration expires: 22 May 2026

Data Protection Officer

Firbank Road
Newall Green
Wythenshawe
Manchester
M23 2YS

Email: DPO@CorpusChristiTrust.co.uk

Issued by: Information Commissioner's Office,
Wycliffe House, Water Lane, Wilmslow, Cheshire
SK9 5AF

Telephone: 0303 123 1113
Website: ico.org.uk

Appendix B Privacy Notice for employees

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 for the Trust.

We, Corpus Christi Catholic Academy Trust, are the 'data controller' for the purposes of data protection law.

To contact our data protection officer, please see 'Contact us' below.

The personal data we hold

We process data relating to those we employ, or otherwise engage, to work for our Trust. 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 and tax status information
- Recruitment information, including copies of documentation, references and other information included in an application form or cover letter as part of the application process
- Qualifications and employment records, including work history, job titles, working hours, training records and professional memberships
- Performance information
- Outcomes of any disciplinary and/or grievance procedures
- Absence data
- Copy of driving licence
- Photographs
- CCTV footage
- Data about your use of the school's information and communications system

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

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

Why we use this data

The purpose of processing this data is to aid the recruitment process by:

- 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 equalities 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)
- We have legitimate interests in processing the data – for example, where:
    - To consider positive discrimination where applicable
    - To ensure we comply with the faith requirements for certain positions in Catholic schools in accordance with the Bishops' Memorandum.

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 the 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 records management policy.

A copy of the Trust's data protection policy and record management policy can be obtained from our data protection officer.

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
- Suppliers and service providers to enable them to provide the service we have contracted them for, such as HR and recruitment support
- Professional advisers and consultants to enable them to carry out their responsibilities and/or provide the service we have contracted them for, such as school improvement partners
- The Department for Education to meet our legal obligations to share certain information with it, such as teacher reference numbers
- Ofsted who is our regulator to meet our legal obligations to share certain information with it, such as our single central record
- Financial organisations to meet our legal obligations and/or to provide the service we have contracted them for, such as our monthly returns
- Our auditors to meet our legal obligations to share certain information with it, such as finances and recruitment processes
- Survey and research organisations, where appropriate, to provide the service we have contracted them for, such as survey monkey
- Health authorities where necessary to share certain information with it, such as contagious diseases
- Security organisations provide the service we have contracted them for, such as contact names and numbers for the security of premises
- Health and social welfare organisations provide the service we have contracted them for, such as health referrals and counselling services

- Employment and recruitment agencies provide the service we have contracted them for, such as payroll
- Charities and voluntary organisations provide the service we have contracted them for, such as contact names and numbers for churches within our Parish
- Police forces, courts and tribunals to share certain information with it, such as when criminal investigations take place or there are safeguarding concerns
- Professional bodies to share certain information with it, such as the Local Authority

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 including the updated UK-US Data Bridge and EU-UK Adequacy Decision.

Your rights

How to access the 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 a 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 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**:

- Postal address: Data Protection Officer, St Anthony's Catholic Primary School Dunkery Road Wythenshawe Manchester M22 0NT
- Email: DPO@CorpusChristiTrust.co.uk

Appendix C 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, Corpus Christi Catholic Academy Trust, are the 'data controller' for the purposes of data protection law.

To contact our data protection officer, please 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
- Monitor and report on pupil progress

- Provide appropriate pastoral care
- Protect pupil welfare
- Assess the quality of our services
- Administer admissions waiting lists
- Carry out research
- Comply with the law regarding data sharing

Our legal basis for using this data

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

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

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

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

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

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

Collecting this information

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

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

How we store this data

We keep personal information about pupils while they are attending our school. We may also keep it beyond their attendance at our school if this is necessary in order to comply with our legal obligations. Our record retention management policy sets out how long we keep information about pupils.

A copy of the Trust's record retention policy and schedule can be obtained from our data protection officer.

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 in order to meet our legal obligations to share certain information with it, such as safeguarding concerns and exclusions
- The Department for Education
- The pupil's family and representatives to comply with our education information regulations
- Educators and examining bodies to complying with our legal obligations and requirements
- Ofsted who is our regulator
- Suppliers and service providers to enable them to provide the service we have contracted them for
- Financial organisations to comply with the Education and Funding Skills Agency (EFSA) requirements
- Central and local government to comply with our legal duties and requirements
- Our auditors to fulfil our financial obligations
- Survey and research organisations where required and deemed appropriate
- Health authorities in order to meet our legal obligations to share certain information with it, such as health and safety and safeguarding concerns
- Security organisations to ensure the health and safety and safeguarding of our pupils, employees, community and visitors to the school
- Health and social welfare organisations in order to meet our legal obligations to share certain information with it, such as health and safety and safeguarding concerns
- Professional advisers and consultants to ensure the highest possible pupil attainment
- Charities and voluntary organisations when necessary
- Police forces, courts, tribunals as legally required
- Professional bodies to enable them to carry out their responsibilities

National Pupil Database

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

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 including the updated UK-US Data Bridge and EU-UK Adequacy Decision.

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.

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.

There is no legal right for parents/carers to access their child's educational record if their child attends an English academy, a free school or an independent school. As an academy, we will consider each request on its own merit.

We will provide an annual written report of each registered pupil's progress and attainment in the main subject areas taught, to the parents of that registered pupil (except that no report need be provided where the parent has agreed otherwise).

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 D**ata Protection Officer**:

- Postal address: Data Protection Officer, St Anthony's Catholic Primary School Dunkery Road Wythenshawe Manchester M22 0NT
- Email: DPO@CorpusChristiTrust.co.uk

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 and within the Trust.

Appendix D Privacy Notice for job applicants

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 applying for jobs at the Trust.

We, Corpus Christi Catholic Academy Trust, are the 'data controller' for the purposes of data protection law.

To contact our data protection officer, please see 'Contact us' below.

Successful candidates should refer to our privacy notice for the school workforce for information about how their personal data is collected, stored and used. This is available on each individual school's intranet or shared area.

The personal data we hold

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

- Contact details
- Copies of right to work documentation
- References
- Evidence of qualifications
- Employment records, including work history, job titles, training records and professional memberships

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 and sexual orientation
- Disability and access requirements

Why we use this data

The purpose of processing this data is to aid the recruitment process by:

- Enabling us to establish relevant experience and qualifications
- Facilitating safe recruitment, as part of our safeguarding obligations towards pupils
- Enabling equalities monitoring
- Ensuring that appropriate access arrangements can be provided for candidates that require them

Our legal 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:

- 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)
- We have legitimate interests in processing the data – for example, where:
    - To consider positive discrimination where applicable
    - To ensure we comply with the faith requirements for certain positions in Catholic schools in accordance with the Bishops' Memorandum.

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 the 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

Personal data we collect as part of the job application process is stored in line with our data protection policy.

When it is no longer required, we will delete your information in accordance with our records management policy.

A copy of the Trust's data protection policy and record management policy can be obtained from our data protection officer.

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 shortlists of candidates for a Headteacher position
- Suppliers and service providers to enable them to provide the service we have contracted them for, such as HR and recruitment support
- Professional advisers and consultants to enable them to carry out their responsibilities
- The Department for Education upon request
- Ofsted who is our regulator upon request
- Our auditors to fulfil our recruitment obligations
- 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 including the updated UK-US Data Bridge and EU-UK Adequacy Decision.

Your rights

How to access the 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 a 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 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**:

- Postal address: Data Protection Officer, St Anthony's Catholic Primary School Dunkery Road Wythenshawe Manchester M22 0NT
- Email: DPO@CorpusChristiTrust.co.uk

Appendix E Privacy Notice for Trust Governance roles

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 for the Trust.

We, the Corpus Christi Catholic Academy Trust, are the 'data controller' for the purposes of data protection law.

To contact our data protection officer, please see 'Contact us' below.

The personal data we hold

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

- Contact details
- Personal identifiers, contacts and characteristics (such as name, date of birth, contact details and postcode)
- Governance details (such as role, start and end dates and governor ID)
- Copy of driving licence/passport/proof of address for DBS purposes
- Photographs
- CCTV footage
- Data about your use of the school's information and communications system

Why we use this data

The personal data collected is essential, in order for the school, academy or academy trust to fulfil their official functions and meet legal requirements.

We collect and use governance information, for the following purposes:

- To meet the statutory duties placed upon us
- Facilitate safe recruitment, as part of our safeguarding obligations towards pupils
- Support effective performance management across schools in the Trust

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)
- We have legitimate interests in processing the data

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

We collect personal information via governor forms.

Governance roles data is essential for the Trust's operational use. Whilst the majority of personal information you provide to us is mandatory, some of it may be requested on a voluntary basis. In order to comply with UK-GDPR, we will inform you at the point of collection, whether you are required to provide certain information to us or if you have a choice in this.

How we store this data

We hold data securely for the set amount of time shown in our data retention schedule.

The information we retain kept secure and is only used for purposes directly relevant to your governance role. Once your governance role has ended with us has ended, we will delete the information in it in accordance with our records management policy.

A copy of the Trust's data protection policy and retention & record management policy can be obtained from our data protection officer.

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:

We routinely share this information with:

- Our local authority to meet our legal obligations to share certain information, such as safeguarding concerns
- Professional advisers and consultants to enable them to carry out their responsibilities and/or provide the service we have contracted them for, such as school improvement partners
- The Department for Education to meet our legal obligations to share certain information
- Ofsted who is our regulator to meet our legal obligations to share certain information, such as our single central record
- Our auditors to meet our legal obligations to share certain information
- Health authorities where necessary to share certain information, such as contagious diseases
- Police forces, courts and tribunals to share certain information, such as when criminal investigations take place or there are safeguarding concerns
- Professional bodies to share certain information, such as the Local Authority

Department for Education (DfE)
The Department for Education (DfE) collects personal data from educational providers and local authorities. We are required to share information about individuals in governance roles with the Department for Education (DfE), under:

We are required to share information about individuals in governance roles with the Department for Education (DfE) under the requirements set out in the academy trust handbook.

All data is entered manually on the GIAS service and held by the Department for Education (DfE) under a combination of software and hardware controls which meet the current government security policy framework.

For more information, please see the 'How Government uses your data' section.

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 the 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 a 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

The UK GDPR gives you certain rights about how your information is collected and used. To make a request for your personal information, contact our data protection officer.

Your rights include:

- the right to be informed about the collection and use of your personal data – this is called 'right to be informed'.
- the right to ask us for copies of personal information we have about you – this is called 'right of access', this is also known as a subject access request (SAR), data subject access request or right of access request.
- the right to ask us to change any information you think is not accurate or complete – this is called 'right to rectification'.
- the right to ask us to delete your personal information – this is called 'right to erasure'.
- the right to ask us to stop using your information – this is called 'right to restriction of processing'.
- the 'right to object to processing' of your information, in certain circumstances.
- rights in relation to automated decision making and profiling.

- the right to withdraw consent at any time (where relevant).
- the right to complain to the Information Commissioner if you feel we have not used your information in the right way.

There are legitimate reasons why your information rights request may be refused. For example, some rights will not apply:

- right to erasure does not apply when the lawful basis for processing is legal obligation or public task.
- right to portability does not apply when the lawful basis for processing is legal obligation, vital interests, public task or legitimate interests.
- right to object does not apply when the lawful basis for processing is contract, legal obligation or vital interests. And if the lawful basis is consent, you don't have the right to object, but you have the right to withdraw consent.

If you have a concern about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to the Information Commissioner's Office at raise a concern with ICO

For further information on how to request access to personal information held centrally by the Department for Education (DfE), please see the How Government uses your data section of this notice.

Withdrawal of consent and the right to lodge a complaint

Where we are processing your personal data with your consent, you have the right to withdraw that consent. If you change your mind, or you are unhappy with our use of your personal data, please let us know by contacting the data protection officer.

Last updated

We may need to update this privacy notice periodically so we recommend that you revisit this information from time to time. This version was last updated in November 2024.

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**:

- Postal address: Data Protection Officer, St Anthony's Catholic Primary School Dunkery Road Wythenshawe Manchester M22 0NT
- Email: DPO@CorpusChristiTrust.co.uk

CORPUSCHRISTI
We are His body, living and learning as one.

Appendix F Letter to suppliers

Dear Supplier

As part of our duties to ensure the safeguarding of our students and staff, we must ensure that all relevant employment checks have been carried out for any staff or contractors working at schools within the Corpus Christi Catholic Academy Trust who are deployed through third party agencies.

In line with Keeping Children Safe in Education, could you therefore please confirm that all of the following checks, where applicable, have been completed and returned as satisfactory for any staff/contractors that are supplied to us from yourselves:

- Identity checks
- Right to Work in the UK checks
- Barred List checks
- Enhanced DBS Certificate checked
- Prohibited from Teaching checks
- Prohibited from Management S128 checks
- EEA Teacher checks
- Overseas checks (for any employees that have worked overseas in the last 5 years for a period of 6 months or more)

Could you also please confirm that they have received safeguarding training within the last 3 years.

Please complete and return the reply slip below.

Kind regards

Business Manager

Name of Supplier: ……..

We confirm that all of the relevant employment checks requested in your letter have been carried out on all of the staff/contractors that we supply to yourselves. We also confirm that they have received safeguarding training within the last 3 years.

Signed: ……..

Print: ……. Date: ……

Position: …….