Data Protection Policy

For the following:
Cardinal Newman Catholic Primary School
Holy Family Catholic Primary School
St Alban's Catholic Primary School
St Anne's Catholic Primary School
St Augustine Catholic Primary School
St Charles Borromeo Catholic Primary School
St Cuthbert Mayne Catholic Primary School
St Hugh of Lincoln Catholic Primary School
St John the Baptist Secondary Catholic School
St Polycarp's Catholic Primary School
St Thomas of Canterbury Catholic Primary School
St Peter's Catholic School
Salesian Catholic Secondary School
The Marist Catholic Primary School
Teach South East

This Policy has been approved and adopted by the Xavier Catholic Education Trust in May 2020

Committee Responsible: Risk & Audit Committee
To be reviewed every two years in May.

Contents

Any reference within this policy to Xavier Catholic Education Trust, XCET or the Trust also incorporates its constituent schools.

1. AIMS

The Xavier Catholic Education Trust aims to ensure that all personal data collected about staff, pupils, parents, governors, volunteers, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the provisions of the Data Protection Act 2018 (DPA 2018).

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. LEGISLATION & GUIDANCE

This policy meets the requirements of the GDPR and the provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR, the ICO's code of practice for Subject Access Requests and guidance material published by The Department for Education (DfE).

This policy also reflects the ICO's code of practice for the use of CCTV, surveillance cameras and personal information.

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

3. DEFINITIONS

Term: Personal Data.

Definition: Any information relating to an identified, or identifiable, 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.

Term: Special categories of personal data.

Definition: 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.

Term: Processing.

Definition: 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.

Term: Data subject.

Definition: The identified or identifiable individual whose personal data is held or processed.

Term: Data controller.

Definition: A person or organisation (school) that determines the purposes and the means of processing of personal data.

Term: Data processor.

Definition: A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.

Term: Personal data breach.

Definition: A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. THE DATA CONTROLLER

The Trust processes personal data relating to parents, pupils, staff, governors, volunteers, visitors and others, and therefore is a data controller. The Trust is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. ROLES & RESPONSIBILITIES

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

5.1 Governing Body

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

5.2 Data Protection Officer (DPO)

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

The DPO will provide an annual report of his/her activities directly to the Trust Board and, where relevant, report to the board his/her advice and recommendations on Trust data protection issues.

The DPO is also the first point of contact for individuals whose data the Trust processes, and for the ICO and, where applicable, Subject Access Requests.

Our DPO's contact details are below:

Contact Name:	Nicola Kenworthy
Contact Address:	Xavier Catholic Education Trust, c/o Salesian School,
	Guildford Road, Chertsey, Surrey KT16 9LU
Contact Email:	n.kenworthy@xaviercet.org.uk
Contact Telephone:	01932 582520

5.3 Chief Executive Officer

The Chief Executive Officer acts as the representative of the data controller on a day-to-day basis.

5.4 ALL STAFF

Staff are responsible for:

• Collecting, storing and processing any personal data in accordance with this policy

• Informing the Trust of any changes to his/her personal data, such as a change of address

• Contacting the DPO in the following circumstances:

a) With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure.

b) If he/she have any concerns that this policy is not being followed.

c) If he/she are unsure whether or not he/she have a lawful basis to use personal data in a particular way.

d) Whenever he/she are engaging in a new activity or project that may affect the privacy rights of the individual.

e) If there has been a data breach.

f) If he/she need support / guidance with any contracts or sharing personal data with third parties or transferring personal data outside the European Economic Area.

g) If he/she need to rely on or capture consent, draft Privacy Notices or deal with data protection rights invoked by an individual.

6. DATA PROTECTION PRINCIPLES

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

The principles say that personal data must be:

• Processed lawfully, fairly and in a transparent manner.

• Collected for specified, explicit and legitimate purposes.

• Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed.

• Accurate and, where necessary, kept up to date.

• Kept for no longer than is necessary for the purposes for which it is processed.

• Processed in a way that ensures it is appropriately secure.

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

7. COLLECTING PERSONAL DATA

7.1 Lawfulness, fairness and transparency

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

• The data needs to be processed so that the school can fulfil a contract with the individual, or the individual has asked the school to take specific steps before entering into a contract.

• The data needs to be processed so that the school can comply with a legal obligation.

• The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's life.

• The data needs to be processed so that the Trust, as a public authority, can perform a task in the public interest, and carry out its official functions.

• The data needs to be processed for the legitimate interests of the Trust or a third party (provided the individual's rights and freedoms are not overridden).

• The individual (or his/her 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 category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

If the Trust offers online services to pupils, such as classroom apps, and intends to rely on consent as a basis for processing, the Trust will get parental consent (except for online counselling and preventive services).

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

7.2 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 his/her data.

If the Trust wants to use personal data for reasons other than those given when it 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 his/her jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the Information and Records Management Society's toolkit for academies (2019).

8. SHARING PERSONAL DATA

The Trust will not normally share personal data with anyone else, but may do so where:

• There is an issue with a pupil or parent/carer that puts the safety of our staff at risk

• The Trust needs to liaise with other agencies – we will seek consent as necessary before doing this

• Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, the Trust will:

a) Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law.

b) Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data the Trust shares.

c) Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us.

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

• The prevention or detection of crime and/or fraud.

• The apprehension or prosecution of offenders.

• The assessment or collection of tax owed to HMRC.

• In connection with legal proceedings.

• Where the disclosure is required to satisfy our safeguarding obligations.

• Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided.

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 the Trust's pupils or staff.

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

9. SUBJECT ACCESS REQUESTS AND OTHER RIGHTS OF INDIVIDUALS

9.1 Subject Access Requests

Individuals have a right to make a 'Subject Access Request' to gain access to personal information that the Trust holds about them. This includes:

- Confirmation that his/her personal data is being processed.
- Access to a copy of the data.
- The purposes of the data processing.
- The categories of personal data concerned.
- Who the data has been, or will be, shared with.
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period.
- The source of the data, if not the individual.
- Whether any automated decision-making is being applied to his/her data, and what the significance and consequences of this might be for the individual.

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

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

If staff receive a Subject Access Request they must immediately forward it to the DPO.

9.2 Children and Subject Access Requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a Subject Access Request with respect to his/her child, the child must either be unable to understand their rights and the implications of a Subject Access Request or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a Subject Access Request. Therefore, most Subject

Access Requests from parents or carers of pupils at the Trust may be granted without the express permission of the pupil. The presumption of sufficient age is not law in England and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a Subject Access Request. Therefore, most Subject Access Requests from parents or carers of pupils at the Trust school may not be granted without **the express permission of the pupil.** The presumption of sufficient age is not law in England and a pupil's ability to understand his/her rights will always be judged on a case-by-case basis.

9.3 Responding to Subject Access Requests

When responding to requests, the Trust:

• May ask the individual to provide 2 forms of identification.

• May contact the individual via phone to confirm the request was made.

• Will respond without delay and within 1 month of receipt of the request.

• Will provide the information free of charge.

• May tell the individual it will comply within 3 months of receipt of the request, where a request is complex or numerous. The Trust will inform the individual of this within 1 month and explain why the extension is necessary.

The Trust will not disclose information if it:

• Might cause serious harm to the physical or mental health of the pupil or another individual.

• Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests.

• Is contained in adoption or parental order records.

• Is given to a court in proceedings concerning the child.

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

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

When the Trust refuses a request, it will tell the individual why, and tell them they have the right to complain to the ICO.

9.4 Other data protection rights of the individual

In addition to the right to make a Subject Access Request (see above), and to receive information when the Trust is collecting their data about how we use and process it (see section 7), individuals also have the right to:

• Withdraw their consent to processing at any time.

• Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances).

• Prevent use of their personal data for direct marketing.

• Challenge processing which has been justified on the basis of public interest.

• Request a copy of agreements under which their personal data is transferred outside of the European Economic Area.

• Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them).

• Prevent processing that is likely to cause damage or distress.

• Be notified of a data breach in certain circumstances.

• Make a complaint to the ICO.

• Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances).

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

10. PARENTAL REQUESTS TO SEE THE EDUCATIONAL RECORD

Parents may make a request to see their child's educational record. This request must be made in writing to the Headteacher via the relevant Trust school's office.

11. BIOMETRIC RECOGNITION SYSTEMS

If and where the Trust uses pupils' biometric data as part of an automated biometric recognition system (for example, pupils use finger-prints to receive school dinners instead of paying with cash), the Trust will comply with the requirements of the Protection of Freedoms Act 2012.

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

Parents/carers and pupils have the right to choose not to use the school's biometric system(s). If a biometric system is introduced the Trust will provide alternative means of accessing the relevant services for those pupils.

Parents/carers and pupils can object to participation in a Trust school's biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

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

Where staff members or other adults use the Trust school's biometric system(s), the Trust will also obtain his/her 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 Trust will delete any relevant data already captured.

12. CCTV

The Trust may use CCTV in various locations around the Trust schools' sites to ensure they remain safe. If the Trust uses CCTV it will adhere to the ICO's code of practice for the use of CCTV.

The Trust does not need to ask individuals' permission to use CCTV, but the Trust makes it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to the DPO.

13. PHOTOGRAPHS & VIDEOS

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

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

Uses may include:

• Within schools on notice boards and in school magazines, brochures, newsletters, etc.

• Outside of schools by external agencies such as the school photographer, newspapers, campaigns.

• Online on the Trust's or its schools' websites or social media pages. We will monitor regularly websites, brochures and display boards to ensure that images of pupils are not used if they have left the school unless specific consent has been provided for the use of the images after the child has left the school.

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

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

14. DATA PROTECTION BY DESIGN & DEFAULT

The Trust will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

• Appointing a suitably qualified DPO, and ensuring he/she have the necessary resources to fulfil his/her duties and maintain their expert knowledge.

• Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6).

• Completing privacy impact assessments where the Trust's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process).

• Integrating data protection into internal documents including this policy, any related policies and privacy notices.

• Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance.

• Regularly conducting reviews and audits to test our privacy measures and make sure the Trust is are compliant.

• Maintaining records of our processing activities, including:

a) For the benefit of data subjects, making available the name and contact details of the Trust's schools and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices).

b) For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

15. DATA SECURITY & STORAGE OF RECORDS

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

In particular:

• Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use.

• Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access.

• Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are

reminded to change their passwords at regular intervals. Neither staff nor pupils should share credentials for any access to school systems.

• Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices where personal information is stored.

• Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment

• Where the Trust needs to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8).

16. DISPOSAL OF RECORDS

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the Trust's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

Contract equipment which may contain data is disposed of securely. Photocopiers are purged of data and requests are made to return equipment to factory settings at the completion of a contract.

Data is stored and disposed of in line with the IRMS Toolkit for schools/academies 2019 (Information and Records Management Society).

17. PERSONAL DATA BREACHES

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

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

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

• A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium.

• Safeguarding information being made available to an unauthorised person.

• The theft of a school laptop containing non-encrypted personal data about pupils.

18. TRAINING

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

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

The school offers online training as appropriate.

19. MONITORING ARRANGEMENTS

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed every two years and ratified by the Trust Board.

Appendix 1 – Personal Data Breach Procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

• On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO

• The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:

a) Lost

b) Stolen

c) Destroyed

d) Altered

e) Disclosed or made available where it should not have been

f) Made available to unauthorised people

• The DPO will alert the Headteacher and relevant Chair of Governors, or Trustees or the Trust Chief Executive Officer.

• The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)

• The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen

• The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (eg, emotional distress), including through:

a) Loss of control over their data.

b) Discrimination.

c) Identify theft or fraud.

d) Financial loss.

e) Unauthorised reversal of pseudonymisation (for example, key-coding).

f) Damage to reputation.

g) Loss of confidentiality.

h) Any other significant economic or social disadvantage to the individual(s) concerned.

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

The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach.

Documented decisions are stored by the DPO electronically and electronic copy held by the Headteacher and Chair of Governors for their reference.

• Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:

a) 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.

b) The name and contact details of the DPO.

c) A description of the likely consequences of the personal data breach.

d) A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.

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

• The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

a) The name and contact details of the DPO.

b) A description of the likely consequences of the personal data breach.

c) A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

• The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies

• The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

a) Facts and cause.

b) Effects.

c) Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals).

Records of all breaches will be stored by the DPO electronically.

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

Actions to minimise the impact of data breaches

The Trust will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

• If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error.

• Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error.

• If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it.

• In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way.

• The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request.

• The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.

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

• Details of pupil premium interventions for named children being published on the school website.

• Non-anonymised pupil exam results or staff pay information being shared with Governors.

• A school laptop containing non-encrypted sensitive personal data being stolen or hacked.

• The school's cashless payment provider being hacked and parents' financial details stolen.