Data Protection and Information Security Policy

This Policy has been approved and adopted by the Xavier Catholic Education Trust
To be reviewed in January 2026

Committee Responsible: Risk & Audit Committee

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 and regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013.

The Information Commissioner's Office is responsible for:

- overseeing compliance with Data Protection legislation
- supporting organisations to become compliant
- enforcing the legal processing of data
- investigating complaints where organisations are not compliant

The Trust is registered with the ICO and maintains a current record of the information it is processing, the legal basis for processing the information and who it is being shared with.

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 and 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 is therefore 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 activities directly to the Trust Board and where relevant, report to the board his advice and recommendations on Trust data protection issues.

The Trust has appointed an independent Data Protection Officer as its DPO.

The independent Data Protection Officer is Roger Simmons and may be contacted via email at rsimmonsltd@gmail.com and via telephone on 07704 838512.

However, please contact the Trust in the first instance if you have a query regarding any aspect of data protection within the Trust via email: info@xaviercet.org.uk

5.3 ALL STAFF

All employees, Governors and any other individual handling personal information on behalf of the Trust have a responsibility to ensure that they comply with Data Protection legislation and the Trust's policies.

The Trust ensures that all staff who are involved in processing personal data undertake training as part of their Induction and the Trust provides mandatory data protection training as part of its Safeguarding responsibilities.

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 including new or additional uses of technology such as remote learning or video-conferencing.
  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 Trust is committed to maintaining the GDPR principles at all times and will:

- Inform individuals why their information is being collected
- Inform individuals when their information is shared, why it is being shared and with whom
- Check the quality and the accuracy of the information it holds
- Only retain information for as long as it is required
- Erase data securely when no longer required
- Ensure safeguards are in place to protect personal information from loss, theft and unauthorised disclosure
- Only share information when it is legally appropriate to do so
- Enable access to individual records through its Individual Rights Request process
- Ensure all staff understand the Trust's policies and procedures

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 comply with all relevant UK and European Union legislation, including:

- Human Rights Act 1998
- Data Protection Legislation (Data Protection Act 1998, GDPR, Data Protection Act 2018)
- Freedom of Information Act 2000
- Common law duty of confidence
- Copyright, Designs and Patents Act 1988
- Computer Misuse Act 1990
- Health and Safety at Work Act 1974
- Privacy and Electronic Communications (EC Directive) Regulations 2003

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 Trust can fulfil a contract with the individual or the individual has asked the Trust to take specific steps before entering into a contract.
- The data needs to be processed so that the Trust 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 under Article 9.

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). The majority of apps will be accessed by the Trust under the legal basis of undertaking a public task, and so will not require consent.

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 their personal data is being processed.
- Access to a copy of the data.
- The purposes of the data processing.

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

Subject Access Requests must be submitted in writing to the relevant school office, details can be found on the trust website, or it can be submitted to info@xaviercet.org.uk

If staff receive a Subject Access Request, they must immediately forward it to the DPO and info@xaviercet.org.uk

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 13 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 under the age of 13 may be granted without the express permission of the pupil.

Children aged 13 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 over the age of 13 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, via the info@xaviercet.org.uk. If staff receive such a request, they must immediately forward it to the DPO.

10. Information Security

Information that is confidential but doesn't relate to an individual or individuals includes the following:

- Trust business or corporate records containing organisationally or publicly sensitive information
- Any commercially sensitive information such as information relating to commercial proposals or current negotiations
- Politically sensitive information
- Information relating to security, investigations and proceedings
- Any information which, if released, could cause problems or damage to individuals, the public, the Trust or another organisation. This could be personal, financial, reputation or legal damage.

The Trust's information security responsibilities covers the creation, acquisition, retention, transit, use, and disposal of all forms of information.

It applies to all employees, Governors, volunteers and staff of service delivery partners who handle information for which the Trust is responsible. It forms the basis of contractual responsibilities in contracts with Data Processors where reference is made to the Trust's Data Protection and Information Security Policy.

The Trust will maintain the confidentiality, integrity and security of all data ensuring it is gathered, secured, stored, shared and erased in accordance with the data protection regulation. The Trust will review its data protection policies as part of its governance process. It will also check the effective implementation of these policies through the regular Governor led Safeguarding Audits.

Information systems will be checked regularly for technical compliance with relevant security implementation standards.

Operational systems are subjected to technical examination to ensure that hardware and software controls have been correctly implemented.

11. Management of Information

The Trust will manage information in accordance with the principles and procedures within this policy and other relevant policies and standards. The following principles apply to how we handle information in our schools:

- All identifiable personal information is treated as confidential and will be handled in accordance with the relevant legal and regulatory protocols.
- All identifiable information relating to staff is confidential except where national policy on accountability and openness requires otherwise.
- Procedures will be maintained to ensure compliance with Data Protection legislation, The Human Rights Act 1998, the common law duty of confidentiality, the Freedom of Information Act 2000 and any other relevant legislation or statutory obligation.
- Information is recorded, used and stored to protect integrity so that it remains accurate and relevant at all times.

12. Trust records

We will create and maintain adequate pupil, staff and other records to meet the Trust's business needs and to account fully and transparently for all actions and decisions. Such records can be used to provide credible and authoritative evidence where required; protect legal and other rights of the Trust, its staff and those who have dealings with our schools; facilitate audit; and fulfil the Trust's legal and statutory obligations.

Records will be managed and controlled effectively to fulfil legal, operational and information needs and obligations in the most cost-effective manner, in line with the IRMS Information Management Toolkit.

13. 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 Trust'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 school's biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant data alreadycaptured is deleted.

As required by law, if a pupil over the age of 13yrs 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'sparent(s)/carer(s).

Where staff members or other adults use a 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 theTrust will delete any relevant data already captured.

14. 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.

15. PHOTOGRAPHS & VIDEOS

As part of activities in Trust schools, we may take photographs and record images of individuals within our Trust. This includes remote learning and video conferencing where recordings of lessons/meetings may be taken, processed and stored as evidence.

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.
- As part of lessons or meetings recorded during remote sessions or video-conferencing. See the Xavier remote learning policy for specific details.

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.

16. 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 a Data Protection Impact Assessment where the Trust's processing of personal datapresents 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 Trustand its schools are compliant.
- Maintaining records of our processing activities in the Trust Record of Processing Activity (ROPA), 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 including secure methods of deletion/destruction of data not required by the Trust for processing under valid legal basis.

17. 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 and comply fully with the Homeworking/BYOD policy set out by the Trust.
- 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 shared including encryption and security and adequately protected (see section 8).

18. 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 Information Management Academy Toolkit 2019 (Informationand Records Management Society).

19. 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. We will record the breach on a 'Breach Management Form', which will be signed-off by the DPO. When appropriate, the DPO 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:

- Personal information being shared within an email, or attached to an email, that is sent to the wrong recipient(s).
- A non-anonymised dataset being published on the Trust 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.

20. TRAINING

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

Data protection will also form part of continuing professional development, where changes to

legislation, guidance or the Trust's processes make it necessary. The Trust offers online training as appropriate.

21. 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.

22. COMPLAINTS

The Trust takes any complaints about how we collect and use your personal data very seriously, so please let us know if you think we've done something wrong.
If you wish to make a complaint then please consult the complaints policy which can be found on the Trust's website Complaints policy.

You can also complain to the Information Commissioner's Office in one of the following ways:

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

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

- A Breach Management Form will be completed to gather the facts of the breach, what actions have been taken already and what actions must now be taken to resolve the breach.
- 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.

The completed Breach Management Report will be stored by the DPO electronically and electronic copy held by the Headteacher and Chair of Governors in the school's files for their reference.