



**ST. PETER CATHOLIC
ACADEMY TRUST**
BY SERVICE, TOWARDS GOD

Diocese of Northampton - Duns Scotus Trust



DATA PROTECTION AND GDPR POLICY

This Data Protection and GDPR Policy been approved and adopted by the St Peter Catholic Academy Trust on 15th May 2018 and will be reviewed May 2020

The Academy Trust delegates the power of dismissal to the Final absence reviewer nominated in accordance with section 7 of this policy.

Signed by Director of the St Peter Catholic Academy Trust:

Signed by Principal/Head teacher:

Data Protection and GDPR Policy

1. Aims

Our school aims to ensure that all data collected about staff, pupils, parents and visitors is collected, stored and processed in accordance with the General Data Protection Regulations (GDPR)

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

2. Legislation and guidance

This policy meets the requirements of the GDPR May 2018.

This policy complies with our funding agreement and articles of association.

Definitions

Term	Definition
Personal data	Data from which a person can be identified, including data that, when combined with other readily available information, leads to a person being identified
Sensitive personal data	Data such as: <ul style="list-style-type: none">• Contact details• Racial or ethnic origin• Political opinions• Religious beliefs, or beliefs of a similar nature• Where a person is a member of a trade union• Physical and mental health• Sexual orientation• Whether a person has committed, or is alleged to have committed, an offence• Criminal convictions
Processing	Obtaining, recording or holding data
Data subject	The person whose personal data is held or processed
Data controller	A person or organisation that determines the purposes for which, and the manner in which, personal data is processed i.e. Payroll Provider, Suppliers, Bank, Local Authority, DFE, ESFA
Data processor	A person, other than an employee of the data controller, who processes the data on behalf of

Data Protection and GDPR Policy

	the data controller.
--	----------------------

4. The data controller

Our school processes personal information relating to pupils, staff and visitors, and, therefore, is a data controller. Our school delegates the responsibility of data controller to the Board of Trustees.* The Trust is registered as a data controller with the Information Commissioner's Office and renews this registration annually.

5. Data protection principles

The GDPR May 2018 is based on the following data protection principles, or rules for good data handling:

- Data shall be processed fairly and lawfully
- Personal data shall be obtained only for one or more specified and lawful purposes
- Personal data shall be relevant and not excessive in relation to the purpose(s) for which it is processed
- Personal data shall be accurate and, where necessary, kept up to date
- Personal data shall not be kept for longer than is necessary for the purpose(s) for which it is processed
- Personal data shall be processed in accordance with the rights of data subjects under the GDPR May 2018
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data, and against accidental loss or destruction of, or damage to, personal data
- Personal data shall not be transferred to a country or territory outside the European Economic Area unless the country or territory ensures an adequate level of protection for the rights and freedoms of data in relation to the processing of personal data

6. Roles and responsibilities

The Academy Committee at each school has overall responsibility for ensuring that the school complies with its obligations under the GDPR May 2018

Day-to-day responsibilities rest with the head teacher, or the Deputy Head in the head teacher's absence. The head teacher will ensure that all staff are aware of their data protection obligations, and oversee any queries related to the storing or processing of personal data.

Staff are responsible for ensuring that they collect and store any personal data in accordance with this policy. Staff must also inform the school of any changes to their personal data, such as a change of address.

Annually the Trust will ensure all of their schools complete an annual review of personal data held.

7. Privacy notice

7.1 Pupils and parents

We hold personal data about pupils to support teaching and learning, to provide pastoral care and to assess how the school is performing. We may also receive data about pupils from other organisations including, but not limited to, other schools, local authorities and the Department for Education.

This data includes, but is not restricted to:

- Contact details
- Results of internal assessment and externally set tests
- Data on pupil characteristics, such as ethnic group or special educational needs

Data Protection and GDPR Policy

- Exclusion information
- Details of any medical conditions

We will only retain the data we collect for as long as is necessary to satisfy the purpose for which it has been collected.

We will not share information about pupils with anyone without consent unless the law and our policies allow us to do so. Individuals who wish to receive a copy of the information that we hold about them/their child should refer to sections 8 and 9 of this policy.

We are required, by law, to pass certain information about pupils to specified external bodies, such as our local authority and the Department for Education, so that they are able to meet their statutory obligations.

7.2 Staff

We process data relating to those we employ to work at, or otherwise engage to work at, our school. The purpose of processing this data is to assist in the running of the school, including to:

- Enable individuals to be paid
- Facilitate safe recruitment
- Support the effective performance management of staff
- Improve the management of workforce data across the sector
- Inform our recruitment and retention policies
- Allow better financial modelling and planning
- Enable ethnicity and disability monitoring
- Support the work of the School Teachers' Review Body
-

Staff personal data includes, but is not limited to, information such as:

- Contact details
- National Insurance numbers
- Salary information
- Qualifications
- Absence data
- Personal characteristics, including ethnic groups
- Medical information
- Outcomes of any disciplinary procedures

We will only retain the data we collect for as long as is necessary to satisfy the purpose for which it has been collected.

We will not share information about staff with third parties without consent unless the law allows us to. We are required, by law, to pass certain information about staff to specified external bodies, such as our local authority and the Department for Education, so that they are able to meet their statutory obligations.

Any staff member wishing to see a copy of information about them that the school holds should contact HR/Finance Personnel in their school.

8. Subject access requests

Under the GDPR May 2018 pupils have a right to request access to information the school holds about them. This is known as a subject access request.

Subject access requests must be submitted in writing, either by letter, email or fax. Requests should include:

Data Protection and GDPR Policy

- The pupil's name
- A correspondence address
- A contact number and email address
- Details about the information requested

The school will not reveal the following information in response to subject access requests:

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

Subject access requests for all or part of the pupil's educational record will be provided within 15 school days.

If a subject access request does not relate to the educational record, we will respond within 40 calendar days.

9. Parental requests to see the educational record

Parents have the right of access to their child's educational record, free of charge, within 15 school days *of a request

Parents of pupils at this school do not have an automatic right to access their child's educational record. The school will decide on a case-by-case basis whether to grant such requests, and we will bear in mind guidance issued from time to time from the Information Commissioner's Office (the organisation that upholds information rights).

10. Storage of records

- Paper-based records and portable electronic devices, such as laptops and hard drives, that contain personal information are kept under lock and key when not in use
- Papers containing confidential personal information should not be left on office and classroom desks, on staffroom tables or pinned to noticeboards where there is general access
- Where personal information needs to be taken off site (in paper or electronic form), staff must sign it in and out from the school office
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals – refer to ICT Acceptable Use Policy
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices - refer to ICT Acceptable Use Policy
- Staff, pupils or Academy Committee members who store personal information on their personal devices are expected to follow the same security procedures for school-owned equipment – to include Academy Committee and Trustees

11. Disposal of records

Personal information that is no longer needed, or has become inaccurate or out of date, is disposed of securely.

For example, we will shred or incinerate paper-based records, and override electronic files. We may also use an outside company to safely dispose of electronic records.

12. Training

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

Data Protection and GDPR Policy

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

14. Monitoring arrangements

The Director Finance and Operations is responsible for monitoring and reviewing this policy.

The Data Protection Officer checks that the school complies with this policy by, among other things, reviewing school records annually.

This document will be reviewed **every 2 years** or when there are significant legislated changes

At every review, the policy will be shared with the Board of Trustees and Academy Committees.

15. Links with other policies

This data protection policy and privacy notice is linked to the freedom of information publication scheme.

Data Protection and GDPR Policy

Appendix A – Summary of Principles

Emails

- Remember to never share anyone's personal information unnecessarily. Only send the minimum relevant information required.
- Always password protect any information you have to share outside the school email system. Never send the password by email. Always ask the recipient to call you for the password.
- Always maintain a professional approach in your emails. Remember school email systems are not private systems.
- **Remember emails may be scrutinised under a subject access request.**

Photos of Pupils and Staff

- Always check consent has been obtained prior to publishing or displaying a photo.

Data Security - ICT

- Always ensure your screen is locked when you are away from your keyboard.
- Never share passwords.
- Removable drives including USB sticks should not be used. Where necessary these must be encrypted.
- Data files must be saved to the network drive and not to the local computer.
- Regularly review the data on your tablet/laptop/network drive and delete anything that is not required.
- Never leave your laptop in your car or anywhere unattended.

Physical Data

- All personal data when not in use must be locked away.
- Any personal data where is no longer required should be shredded or placed in the confidential sacks as per your schools arrangements.
- Regularly review information stored in cupboards and drawers and dispose of securely in line with the document retention policy.
- Maintain a clear desk.

Communication

- Be careful about conversations in public places.