GDPR

(General Data Protection Regulation) Policy

Date approved by Trust Board:	September 2021
Version:	03
Date revision approved by Trust Board:	October 2023
Publication Scheme:	Trust Website
Next Review Date:	Autumn Term 2024
Policy Owner:	Head of Safeguarding

1. Audience

1.1 This policy is for adoption and implementation by each Trust school and the Trust's Central Team.

2. Purpose

2.1 The Trust is required to keep and process certain information about its employees and pupils in accordance with its legal obligations under the UK General Data Protection Regulation (GDPR). This policy is in place to ensure all staff and governors are aware of their responsibilities and outlines how the Trust complies with the core principles of the UK GDPR.

3. Policy Statement

3.1 The Trust may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly the Department for Education, local authorities, other schools and academies and educational bodies.

3.2 Organisational methods for keeping data secure are imperative, and the Trust believes that it is good practice to keep clear practical policies, backed up by written procedures.

4. Scope

4.1 The Trust processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller and is registered with the ICO.

4.2 This policy ensures all personal data collected about staff, pupils, parents, governors, visitors and other individuals are collected, stored and processed in accordance with the UK GDPR. It applies to all personal data, regardless of whether it is in paper or electronic format.

4.3 The GDPR (General Data Protection Regulation) Procedures sets out how schools/central trust aim to comply with the processing and sharing of personal data.

5. Values and Principles

Principles	**What this means for NPCAT schools**
Nurturing	We protect our pupils, families and staff by ensuring their personal data and identity are safeguarded and secure.

Perseverance	We ensure that all tasks undertaken that involve the processing of personal data are compliant with legislative requirements.
Courage	We are open and transparent in our data processing.
Ambition	We act promptly with the right to access, rectification, erasure or restriction, or to object to such processing of information.
Tolerance and Respect	We use data sensitively and seek consent to processing, where required to do so.

6. Requirements

6.1 Data protection principles

6.1.1 The UK GDPR is based on data protection principles that the Trust 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.

6.2 Accountability

6.2.1 Appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the UK GDPR will be implemented by the Trust providing comprehensive, clear and transparent privacy notices.

6.2.2 Whenever personal data is first collected directly from individuals, they will be provided with the relevant information required by data protection law.

6.2.3 Internal records of processing activities will include the following:

- Name and details of the organisation
- Purpose(s) of the processing
- Description of the categories of individuals and personal data
- Retention schedules
- Categories of recipients of personal data
- Description of technical and organisational security measures
- Details of transfers to third countries, including documentation of the transfer mechanism safeguards in place.

6.2.4 Data protection impact assessments (DPIAs) should be used, where appropriate. DPIAs will allow identification and resolution to problems at an early stage, thus reducing associated costs and preventing damage from being caused to the Trust's reputation which might otherwise occur.

6.3 Lawfulness, fairness and transparency

6.3.1 The legal basis for processing data must be identified and documented prior to data being processed.

6.3.2 Personal data must only be processed where there are one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed to **fulfil a contract** with the individual, or the individual has asked for specific steps to be taken before entering into a contract.
- The data needs to be processed to **comply with a legal obligation**.
- The data needs to be processed to ensure the **vital interests** of the individual or another person i.e. to protect someone's life.
- The data needs to be processed so that the Trust, as a public authority, can **perform a task in the public interest or exercise its official authority.**
- The data needs to be processed for **legitimate interests** of the Trust (where the processing is not for any tasks the Trust performs as a public authority) or a third party, provided the individual's rights and freedoms are not overridden.
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**.

6.3.3 For special categories of personal data, one of the special category conditions for processing under data protection law must be met:

- 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.

6.3.4 For criminal offence data, both a lawful basis and a condition set out under data protection law must be met. 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.

6.3.5 Consideration must always be given to the fairness of data processing. Data must not be handled in ways that individuals would not reasonably expect, or personal data used in ways which have unjustified adverse effects on them.

6.4 Consent

6.4.1 Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.

6.4.2 Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.

6.4.3 Consent mechanisms must meet the standards of the UK GDPR. Where the standard of consent cannot be met, or consent is withdrawn, an alternative legal basis for processing the data must be found, or the processing must cease.

6.4.4 Where a child is under the age of 13, the consent of parents must be sought prior to the processing of their data, except where the processing is related to preventative or counselling services offered directly to a child.

6.5 Sharing personal data

6.5.1 Personal data should not normally be shared 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 staff or other pupils at risk.
- There is a need to liaise with other agencies (consent must always be sought as necessary before doing this).
- Suppliers or contractors need data to enable services to be provided to staff and pupils (for example, IT companies). When doing this:
  - Only suppliers or contractors will be appointed who have been procured through the central trust and can provide sufficient guarantees that they comply with the requirements of the UK GDPR.
  - A contract must be established with the supplier or contractor to ensure the fair and lawful processing of any personal data shared.
  - Data will only be shared that the supplier or contractor needs to carry out their service.

6.5.2 Personal data must be shared with law enforcement and government bodies where there is a legal requirement to do so.

6.5.3 Personal data should also be shared with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

6.5.4 Where personal data is transferred internationally, it will be done in accordance with the requirements of the UK GDPR.

6.6 Biometric recognition systems

6.6.1 The use of pupils' biometric data as part of an automated biometric recognition system (for example, pupils use fingerprints to receive school dinners instead of paying with cash), must comply with the requirements of the Protection of Freedoms Act 2012.

6.7 CCTV and photography

6.7.1 The recording of images of identifiable individuals constitutes processing personal information, and must be done in line with data protection principles

6.8 DBS data

6.8.1 All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.

6.8.2 Data provided by the DBS must never be duplicated.

6.8.3 Any third parties who access DBS information must be made aware of the data protection legislation, as well as their responsibilities as a data handler.

6.9 Data protection by design and default

6.9.1 Measures that meet the principles of data protection by design and default must be implemented, such as:

- Data minimisation
- Pseudonymisation
- Transparency
- Allowing individuals to monitor processing
- Continuously creating and improving security features

6.9.2 Measures must be put in place to show integrated data protection into all of data processing activities, including:

- Appointing a suitably qualified Data Protection Officer (DPO) and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge.
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law.

- Completing data protection impact assessments where the processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies.
- 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; keeping a record of attendance.
- Regularly conducting reviews and audits to test privacy measures and ensure there is compliance.
- Appropriate safeguards being put in place where there is transfer of any personal data outside of the UK, where different data protection laws may apply.
- Maintaining records of processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of the DPO and all information required to be shared about using and processing personal data (via privacy notices).
    - For all personal data held, maintaining an internal record of the type of data, type of data subject, how and why the data is used, any third-party recipients, any transfers outside of the UK and the safeguards for those, retention periods and storage of data.

6.10 Data security and storage of records

6.10.1 Personal data must be kept safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

6.11 Data retention and disposal of records

6.11.1 Data should not be kept for longer than is necessary. Personal data that has become inaccurate or out of date must also be disposed of confidentially and securely.

6.11.2 If a third party is used to safely dispose of records on the Trust's behalf, sufficient guarantees must be required from the third party to ensure it complies with data protection law.

6.12 Data Breach

6.12.1 Effective and robust breach detection, investigation and internal reporting procedures must be in place, which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified.

6.13 Publication of information

6.13.1 A a publication scheme is published on the school and central trust website outlining classes of information that will be made routinely available, including:

- Policies and procedures
- Minutes of meetings

- Annual reports
- Financial information

6.13.2 Classes of information specified in the publication scheme should be made available quickly and easily on request.

6.13.3 Personal information, including photographs, must not be published on websites without the permission of the affected individual.

6.13.4 When uploading information to websites consideration must be given to any metadata or deletions which could be accessed in documents and images on the site.

6.14 Monitoring arrangements

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

6.14.2 Each school and the central trust will need their own procedures outlining how they are adhering to, and implementing this policy.

7. Definitions

GDPR	General Data Protection Regulations
The Trust	Reference to "the Trust" includes schools and central services.
ICO	Information Commissioner's Office.
Data Controller	A person or organisation that determines the purposes and the means of processing of personal data.
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.
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	The UK GDPR singles out some types of personal data as likely to be more sensitive, and gives them extra protection. This type of data is referred to as 'special category personal data'. Personal data which is more sensitive and so needs more protection, including information about an individual includes:: • 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
Sensitive personal data	Referred to as 'special categories of personal data'. These specifically include the processing of genetic data, biometric data and data concerning health matters.
Genetic data	is defined as 'personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question'.
Biometric data	is defined as ' personal data resulting from specific technical processing relating to the physical, psychological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic (fingerprint) data'.
Health data	is defined as ' personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status'.

8. Legislation

- UK General Data Protection Regulation (UK GDPR)
  (the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020)
- Data Protection Act 2018 (DPA 2018)
- Protection of Freedoms Act 2012 (when referring to use of biometric data)

9. Related Policies

- ICT Systems Acceptable Use Policy
- Safeguarding and Child Protection Policy

- Social Media Policy
- Digital Imaging Policy
- Media Engagement Policy
- Remote Learning(Online Education) Policy

10. Related Procedures

- NPCAT GDPR (General Data Protection Regulation) Procedures
- ICT Systems Acceptable Use Procedures
- ICT Systems and Equipment Loan Agreement
- Safeguarding and Child Protection Procedures
- Remote Learning (Online Education) Procedures - primary
- Remote Learning (Online Education) Procedures - secondary

11. Standards and Guidelines

- Standards
- Guidelines

12. Supporting Information/Websites

Guidance published by the Information Commissioner's Office (ICO) on the UK GDPR.

13. Contacts

For advice on the content of this policy, please contact:

Jill Benson
Trust Head of Safeguarding / Data Protection Lead / Complaints Co-ordinator
Nicholas Postgate Catholic Academy Trust
Postgate House
Saltersgill Avenue
TS4 3JP
Tel: 01642 529200
Email: benson.j@npcat.org.uk

Jim Farquhar
Assistant Chief Executive Officer / Data Protection Officer
Nicholas Postgate Catholic Academy Trust
Postgate House
Saltersgill Avenue
TS4 3JP
Tel: 01642 529200
Email: farquhar.j@npcat.org.uk