GDPR, Privacy, Data Protection Policy

Approved by:	Paula Tucker	**Date:** 15/9/25
Review by:	31/9/26	

CONTENT

1. Introduction

Under UK data protection law, individuals have a right to be informed about how our school uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about **pupils at our school**.

2. Policy Statement

2.1 Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (UK GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

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

2.3 This policy meets the requirements of the UK GDPR and the expected provisions of the DPA 2018. It's based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR and the ICO's code of practice for subject access requests

2.4 It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data. It also reflects the ICO's code of practice for the use of surveillance cameras and personal information. In addition, the Governors have agreed that the academy will comply with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents of children in maintained schools the right of access to their child's educational record. Finally, this policy complies with our funding agreement and articles of association.

3. Why we use this data

3.1 We use the data listed above to:

- Support pupil learning

- Monitor and report on pupil progress
- Provide appropriate pastoral care
- Protect pupil welfare
- Assess the quality of our services
- Administer admissions waiting lists
- Carry out research
- Comply with the law regarding data sharing
- Make sure our information and communication systems, equipment and facilities (e.g. school computers) are used appropriately, legally and safely

3.2 Who does this policy apply to?

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

4. Who is responsible for carrying out this policy?

The Governing Board supports the Executive Headteacher who has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

4.1 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.

4.2 They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on school data protection issues. The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO. Full details of the DPO's responsibilities are set out in their job description.

DPO at ReFocus is Paula Tucker

01933 391660 paula@refocus.school

4 Knox road Wellingborough Northants NN8 1HW

4.3 Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy.
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
  - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
  - If they have any concerns that this policy is not being followed
  - If they are unsure whether they have a lawful basis to use personal data in a particular way o If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
  - If there has been a data breach
  - Whenever they are engaging in a new activity that may affect the privacy rights of individuals o If they need help with any contracts or sharing personal data with third parties

5. Data protection principles

5.1 The UK 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 school aims to comply with these principles.

6. Definitions

6.1 Personal data:

- 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.

6.2 Special categories of personal data: Personal data which is more sensitive and so needs more protection, including information about an individual's:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetics
- Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes
- Health – physical or mental
- Sex life or sexual orientation

6.3 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.

6.4 Data subject: The identified or identifiable individual whose personal data is held or processed.

6.5 Data controller: A person or organisation that determines the purposes and the means of processing of personal data.

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

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

7. The data controller

7.1Our school processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

7.2 The school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

8 Collecting personal data

8.1 Lawfulness, fairness and transparency

We 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 school, 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 school 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

8.2 For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the UK GDPR and Data Protection Act 2018. If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent where the pupil is under 13 (except for online counselling and preventive services). Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

8.3 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit, and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

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

Staff must only process personal data where it is necessary in order to do their 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 school's record retention schedule as outlined in the record management policy.

9. Sharing personal data

9.1 We 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
- We need 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, we will:

- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
- 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 we share
- 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

9.2 We will also share personal data with law enforcement and government bodies where we are 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 (Risks include misinformation, disinformation, AI-generated abuse, deepfakes, and synthetic media as highlighted in KCSIE)

10. Subject access requests and other rights of individuals

10.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed (NB Requests may be refused if they are manifestly unfounded or excessive (UK GDPR)
- 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 their 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
- If staff receive a subject access request they must immediately forward it to the DPO.

10.2 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 their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent. Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or

carers of pupils at our school may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis

10.3 Responding to subject access requests When responding to requests, we

- 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 we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary
- We 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, we 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 we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

10.4 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 we are 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.

11. Parental requests to see the educational record

10.1 As an independent school, parents do not have an automatic parental right of access to the educational record. The educational record contains most information about the student. The Execuive Headteacher has taken the decision that parents, or those with parental responsibility, will have a right to free access to their child's educational record, and that the school would endeavour to meet this within 15 school days of receipt of a written request.

12. CCTV

12.1 We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.
12.2 We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

13. Photographs and videos

13.1 As part of our school activities, we may take photographs and record images of individuals within our school.
13.2 We will obtain written consent from parents/carers, or pupils aged 18 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.
13.3 Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used. Uses may include:
Within school on notice boards and in school magazines, brochures, newsletters, etc.
Outside of school by external agencies such as the school photographer, newspapers, campaigns
Online on our school website or social media pages
13.4 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.
13.5 When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.
See our safeguarding and e-safety policies for more information on our use of photographs

14. Data protection by design and default

14.1 We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:
14.2 Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
14.3 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
14.4 Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
14.5 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 we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)

- 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 and storage of records

15.1 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
- Measures include encryption of devices and emails, multi-factor authentication for staff accounts, and use of only approved secure cloud services)