Rednock School
Quality, Partnership, Success
E-mail: admin@rednockschool.org.uk
www.rednockschool.org.uk

Proposed Policy:	Data Protection Policy	Responsibility Of:	Data Protection Officer
Date of Ratification:	December 2020	Date of Review:	October 2022

DATA PROTECTION POLICY
General Data Protection Regulation

The Data Protection Act 2018 (DPA 2018) outlines the requirement for an Appropriate Policy Document (APD) to be in place when processing special category (SC) and criminal offence (CO) data under certain specified conditions.

This document meets the requirement at paragraph 1 of Schedule 1 to the Data Protection Act 2018 that an appropriate policy document be in place where the processing of special category personal data is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller or the data subject in connection with employment, social security or social protection.

It also meets the requirement at paragraph 5 of Schedule 1 to the Data Protection Act 2018 that an appropriate policy document be in place where the processing of special category personal data is necessary for reasons of substantial public interest. The specific conditions under which data may be processed for reasons of substantial public interest are set out at paragraphs 6 to 28 of Schedule 1 to the Data Protection Act 2018 and the School intends to rely on these as and when appropriate, with particular reliance on paragraph 18, 'Safeguarding of children and individuals at risk' and paragraph 17, 'Counselling'.

Contents

1. Introduction

In order to work effectively Rednock School has to collect and use information about people with whom it works. This may include (past, present and future) pupils, parents, teachers, trustees, members of the public, contractors and suppliers. In addition we may be required by law to collect and use information in order to comply with the requirements of the central government.

All personal information must be handled and dealt with properly, regardless of how it is collected, recorded and used, and whether it is on paper, in computer records or recorded by other means. We are all responsible for its safe handling.

This document sets out the principles of data protection, our responsibilities, and the access rights of individuals, as well as information sharing and complaints.

2. Scope/ Our Commitment

This policy applies to all staff, governors, contractors, agents, representatives and temporary staff, working for or on behalf of the School. The requirements of this policy are mandatory for all of these parties.

Rednock School regards the lawful and correct treatment of personal information as critical to its successful operation, maintaining confidence between the school and those it interacts with. The school will ensure that it treats personal information correctly in accordance with the law.

Rednock School fully endorses and adheres to the principles of Data Protection as set out in the Data Protection Act (2018) and the General Data Protection Regulation (GDPR).

Rednock School is committed to ensuring that their staff are aware of data protection policies, legal requirements and that adequate training is provided.

3. Aims

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

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

4. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, living individual. or from that data and other information which is in the possession of, or is likely to come into the possession of the data controller' (the School is a data controller), and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other in respect of the individual. This may include the individual's: ● Name (including initials) ● Identification number ● Location data ● Online identifier, such as a username
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 or beliefs ● Religious or philosophical beliefs ● Trade union membership ● Genetics ● Biometrics (such as fingerprints, retina and iris patterns) where used for identification purposes ● Physical or mental health/condition ● Sex life or sexual orientation ● Details of proceedings in connection with an offence or an alleged offence.
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.
Data subject	The identified or identifiable individual, whose personal data is held or processed.
Data protection officer	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.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
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.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

5. Roles and Responsibilities

5.1 The Data Controller

Rednock school processes personal data relating to parents, students, staff, governors, visitors and others, and therefore is a data controller.

Changes to the type of data processing activities being undertaken shall be notified to the ICO and details amended in the register.

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

Register of data controllers | ICO

5.2 Data Protection Officer

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.

Our DPO is
Gloucestershire County Council,
Schools Data Protection Team
Information Management Service
Shire Hall
Westgate Street
Gloucester

T: 01452 583619
Email: schoolsdpo@gloucestershire.gov.uk

5.3 Head Teacher

The Head Teacher 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 school of any changes to their personal data, such as 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 or not they have a lawful basis to use personal data in a particular way
    - 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
- If they need help with any contracts or sharing personal data with third parties.

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 and fairly
- 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, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in accordance with the data subject's rights
- Processed in a way that ensures it is appropriately secure.
- Not transferred to other countries without adequate protection

Guide to data protection | ICO

Key definitions of the Data Protection Act | ICO

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

7 Processing Personal Data

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law. When special category personal data, criminal conviction data or data about offences, is processed, a lawful basis and additional condition will be satisfied.

- 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 student) has freely given clear **consent**.

8 Fair Processing/Privacy Notice

We shall be transparent about the intended processing of all data including criminal offence data and communicate these intentions via notification to staff, parents and students prior to the processing of an individual's data.

Notifications shall be in accordance with ICO guidance and, where relevant, be written in a form understandable by those defined as 'Children' under the legislation.

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 Records Retention and Disposal Policy.

9 Sharing Personal Data

There may be circumstances where the school is required either by law or in the best interests of our pupils or staff to pass information on to external authorities, for example local authorities, Ofsted, or the department of health.

These authorities are up to date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

Any proposed change to the processing of an individual's data shall first be notified to them.

Personal data about pupils will not be disclosed to third parties without the consent of the child's parent or carer, unless it is obliged by law or in the best interest of the child. Data may be disclosed to the following third parties without consent:

- Emergency services and local authorities: to help them to respond to an emergency situation that affects any of our students or staff.
- Other schools - If a student transfers to another school, their academic records and other data that relates to their health and welfare will be forwarded onto the new school. This will support a smooth transition from one school to the next and ensure that the child is provided for as is necessary. It will aid continuation which should ensure that there is minimal impact on the child's academic progress as a result of the move.
- Examination authorities - This may be for registration purposes, to allow the students at our school to sit examinations set by external exam bodies.
- Health authorities - As obliged under health legislation, the school may pass on information regarding the health of children in the school to monitor and avoid the spread of contagious diseases in the interest of public health.
- Police and courts - If a situation arises where a criminal investigation is being carried out, we may have to forward information on to the police to aid their investigation. We will pass information on to courts as and when it is ordered.
- Social workers and support agencies - In order to protect or maintain the welfare of our pupils, and in cases of suspected child abuse, it may be necessary to pass personal data on to social workers or support agencies.
- Education division - Schools may be required to pass data on in order to help the government to monitor the national educational system and enforce laws relating to education.

Under no circumstances will the school disclose information or data:

- that would cause serious harm to the child's or anyone else's physical or mental health or condition
- indicating that the child is or has been subject to child abuse or may be at risk of it, where the disclosure would not be in the best interests of the child
- recorded by the pupil in an examination
- that would allow another person to be identified or identifies another person as the source, unless the person is an employee of the school or a local authority or has given consent, or it is reasonable in the circumstances to disclose the information without consent. The

exemption from disclosure does not apply if the information can be edited so that the person's name or identifying details are removed

Or

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

In addition, our suppliers or contractors may need data to enable us to provide services to our staff and students. 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.

10 Data Protection Rights of Individuals

10.1 Subject Access Requests

All individuals whose data is held by us, have a legal right to request access to such data or information about what is held. We shall respond to such requests within one month and they should be made in writing to:

The Headteacher
Rednock School
Kingshill Road
Dursley
GL11 4BY

Requests 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 Headteacher.

10.2 Responding to Subject Access Requests

When responding to requests, we

- May ask the individual to provide 2 forms of identification
- May contact the individual to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request

- 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 student 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.

10.3 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).
- Where personal data is no longer required for its original purpose, an individual can demand that the processing is stopped and all their personal data is erased by the school including any data held by contracted processors.

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

11 Biometric Recognition System

Where we use students' biometric data as part of an automated biometric recognition system (for example, students use finger prints to receive school dinners instead of paying with cash), we 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 school will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents / carers and students have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those students. For example, students can pay for school dinners using a PIN at each transaction if they wish.

Parents / carers and students can object to participation in the 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 student refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the student's parent(s) / carer(s).

Where staff members or other adults use the school biometric system(s), we will also obtain their 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 school will delete any relevant data already captured.

12 CCTV

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.

We do not need to ask an individual's 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.

Any enquiries about the CCTV system should be directed to the school's Facilities Manager and the CCTV Policy.

13 Photographs and Videos

As part of our school activities, we may take photographs and recorded images of individuals within our school.

We will obtain written consent from parents / carers, or students aged 18 and over, for photographs and videos to be taken of students for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and / or video will be used to both the parent / carer and student. Where we do not need parental consent, we will clearly explain to the student 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.

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 we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

14 Data Protection by Design and Default

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

- Appointing a suitably qualified 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 (see section 6)
- Completing privacy impact assessments where the school's processing of personal data presents a high risk to the 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 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

In order to assure the protection of all data being processed and inform decisions on processing activities, we shall undertake an assessment of the associated risks of proposed processing and equally the impact on an individual's privacy in holding data related to them.

Risk and impact assessments shall be conducted in accordance with guidance given by the ICO:

Risk and impact assessments | ICO

Security of data shall be achieved through the implementation of proportionate physical and technical measures. Nominated staff shall be responsible for the effectiveness of the controls implemented and reporting of their performance. The security arrangements of any organisation with which data is shared shall also be considered and where required these organisations shall provide evidence of their competence in the security of shared data.

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

17 Location of Information and Data

Hard copy data, records, and personal information are stored out of sight and in a locked cupboard or office. The only exception to this is medical information that may require immediate access during the school day. This will be stored with the school medical officer.

Sensitive or personal information and data should not be removed from the school site, however the school acknowledges that some staff may need to transport data between the school and their home in order to access it for work in the evenings and at weekends. This may also apply in cases where staff have offsite meetings, or are on school visits with pupils.

The following guidelines are in place for staff in order to reduce the risk of personal data being compromised:

- Paper copies of data or personal information should not be taken off the school site. If these are misplaced they are easily accessed. If there is no way to avoid taking a paper copy of data off the school site, the information should not be on view in public places, or left unattended under any circumstances.
- Unwanted paper copies of data, sensitive information or pupil files should be shredded. This also applies to handwritten notes if the notes reference any other staff member or pupil by name.
- Care must be taken to ensure that printouts of any personal or sensitive information are not left in printer trays or photocopiers.
- If information is being viewed on a PC, staff must ensure that the window and documents are properly shut down before leaving the computer unattended. Sensitive information should not be viewed on public computers
- Laptops that staff use must be password protected.

These guidelines are clearly communicated to all school staff, and any person who is found to be intentionally breaching this conduct will be disciplined in line with the seriousness of their misconduct.

18 Disposal of Records

The school recognises that the secure disposal of redundant data is an integral element to compliance with legal requirements and an area of increased risk.

All data held in any form of media (paper, tape, electronic) shall only be passed to a disposal partner with demonstrable competence in providing secure disposal services.

All data shall be destroyed or eradicated to agreed levels meeting recognised national standards, with confirmation at completion of the disposal process. Disposal of IT assets holding data shall be in compliance with ICO guidance:

IT asset disposal for organisations | ICO

19 Personal Data Breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches. The School will always treat any data breach as a serious issue, potentially warranting a disciplinary investigation. Each incident will be investigated and judged on its individual circumstances, addressed accordingly and carried out in line with the employee code of conduct.

We have appointed Gloucestershire County Council as our Data Protection Officer. They can be contacted on 01452 583619 or schoolsdpo@gloucestershire.gov.uk

Data breaches shall be notified within 72 hours to the individual(s) concerned and the ICO.

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 school's processes make it necessary.

21 Monitoring Arrangement

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our school's practice. Otherwise, or from then on, this policy will be reviewed **every 2 years** and shared with the Full Governing Body.

22 Complaints

Complaints about how the school processes data under the GDPR and responses to subject access requests are dealt with using the School's complaints procedure.

23 Links with Other Policies

This data protection policy is linked to our

- Freedom of Information Policy
- Acceptable Use Policy
- Complaints Procedure
- Child Protection and Safeguarding Policy
- Records Retention and Disposal Policy
- Privacy Notices for Students, Staff and Parents / Carers
- CCTV Policy