

**Policy: General Data Protection Procedures Policy**

|  |  |
| --- | --- |
| **Adopted by Governing Body on** |  **September 2020** |
| **Headteacher** | **Louise Jones** |
| **Date of Review** | **September 2021** |

**General Data Protection Policy**

1. Aims 2

2. Legislation and guidance 2

3. Definitions 2

4.The data controller 3

5. Roles and responsibilities………………………………………………………………………….3-4

6. Data protection principles 5

7. Collecting personal data 5

8. Sharing personal data ………………………………………………………………………………. 6

9. Subject access requests and other right of individuals…………………………………………7-8

10. Parental requests to see the educational record 9

11. Photographs and videos 9

12. Data proectection by design and default …………………………………………… …………10

13. Data security and storage of records 11

14. Disposal of records 11

15. Personal data breaches………………………………… ……………………………………11

16. Training………………………………………………………………………………………………12

17. Monitoring Arrangements…...……………………………………………………………………. 12

18. Links with other policies……..…………………………………………………………………… 12

Appendix 1: Data Sharing Agreement……………………………………………………………13-14

Appendix 2: Subject Access Request Proforma…………………………………………………15-16

Appendix 3: Appendix 3 - Privacy Impact Assessment……………………………………………………………………………………………..17

Appendix 4: Data Breach Record…………………….…………………………………………..18-19

# 1. Aims

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 (GDPR)](http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the [Data Protection Bill](https://publications.parliament.uk/pa/bills/cbill/2017-2019/0153/18153.pdf).

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

# 2. Legislation and guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner’s Office (ICO) on the [GDPR](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/) and the ICO’s [code of practice for subject access requests](https://ico.org.uk/media/for-organisations/documents/2014223/subject-access-code-of-practice.pdf).

In addition, this policy complies with regulation 5 of the [Education (Pupil Information) (England) Regulations 2005](http://www.legislation.gov.uk/uksi/2005/1437/regulation/5/made), which gives parents the right of access to their child’s educational record.

# 3. 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:* 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 |
| **Data processor** | A person, other than an employee of the data controller, who processes the 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. |

# 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 Headteacher.

The school is registered as a data controller with the Information Commissioner’s Office and renews this registration annually.

# 5. Roles and responsibilities

This policy applies to **all staff** employed by our school, 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 governing body has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

**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.

They will provide an annual report of their activities directly to the governing body and, where relevant, report to the body 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.

**5.3 Headteacher**

The headteacher 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 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 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, 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.

# 7. Collecting personal data

**7.1 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**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

**7.2 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 policy in line with **irms.org.uk.**

# 8. Sharing personal data

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 (see Appendix 1) 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

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
* Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Where we transfer personal data to a country or territory outside the European Economic Area, we 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 school 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 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.

**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 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 below the age of 12 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 our school may 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.

**9.3 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.

A request must be confirmed using the school template – see Appendix 2

**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 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.

# 10. Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free access to their child’s educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

# 11. Photographs and videos

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

We will obtain written consent from parents/carers for photographs and videos to be taken of their child 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 school on notice boards and in school magazines, brochures, prospectus, newsletters, etc.
* Outside of school by external agencies such as the school photographer, newspapers, campaigns, sporting clubs, companies who support school with additional learning opportunities
* 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 unless the photo is of a group.

See our Photography Policy for more information on our use of photographs and videos

# 12. Data protection by design and default

We 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 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 (see Appendix 3) 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). For more information see <https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf>
* 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

# 13. Data security and 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
* 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
* Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
* Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures for school-owned equipment

# 14. 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 school’s behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

# 15. Personal data breaches

The school 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 4.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

* A non-anonymised dataset being published on the school 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

# 16. 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.

# 17. Monitoring arrangements

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.

# 18. Links with other policies

This data protection policy is linked to our:

* Freedom of information publication scheme
* Online Safety Policy
* Acceptable use policy
* Photography Policy
* Retention policy

**Appendix 1 – Data Sharing Agreement request letter**

 Date:

Dear Sir/Madam

**Re: Compliance with the General Data Protection Regulation**

As I’m sure you’re aware, the General Data Protection Regulation (GDPR) comes into force in May 2018. As part of our preparations we are conducting due diligence on all suppliers with which we share individuals’ personal data to make sure they, and therefore we, are compliant.

We would appreciate it if you could answer the following questions to help us do this:

* What action are you taking to prepare for the GDPR?
* What technical and organisational security measures do you have in place to protect personal data?
* What policies and procedures do you have in place to protect personal data?
* How secure are your systems?
* Do you have any information management accreditation?

We also need to ensure that the contract we have with you reflects the GDPR, and is updated to include:

* The subject matter, duration, nature and purpose of the processing
* The type of personal data being processed
* The categories of the data subjects
* The obligations and the rights of the data controller (the school)
* That the data processer (you, the supplier) processes data only on the documented instructions of the school
* That the people who process the data are committed to confidentiality
* That you take measures to ensure secure processing
* That you will not engage another processor without prior written authorisation from the school, and that if you do so, that processor will also be bound by the same data protection conditions as are in your contract with us
* That you help the school comply with requirements regarding the data rights of individuals (e.g. to access, delete or rectify data), secure processing, the reporting and communication of data breaches, and the conducting of impact assessments where relevant
* That you delete or return the personal data to the school at the end of your provision of services
* That you make information available to us to demonstrate your compliance with the obligations in our contract, and allow us or a third party instructed by us to conduct audits and inspections

Please could you reply to this letter by post or e-mail to enquiries@royd.sheffield.sch.uk answering the above questions and confirming the amendment of our contract to reflect the GDPR and your full compliance with it. Should you wish to meet or speak with us to discuss this please do not hesitate to contact me on the e-mail address above or by telephoning on 0114 2882594.

Yours sincerely,

**Appendix 2: Subject Access Request Proforma**

**Re: subject access request**

Dear Louise Jones (Headteacher / Data Protection officer),

Please provide me with the information about me that I am entitled to under the General Data Protection Regulation. This is so I can be aware of the information you are processing about me, and verify the lawfulness of the processing.

Here is the necessary information:

|  |  |
| --- | --- |
| Name |  |
| Relationship with the school | Please select:Pupil / parent / employee / governor / volunteer Other (please specify): |
| Correspondence address |  |
| Contact number |  |
| Email address |  |
| Details of the information requested | Please provide me with:*Insert details of the information you want that will help us to locate the specific information. Please be as precise as possible, for example:** *Your personnel file*
* *Your child’s medical records*
* *Your child’s behavior record, held by [insert class teacher ]*
* *Emails between ‘A’ and ‘B’ between [date]*
 |

If you need any more information from me, please let me know as soon as possible.

Please bear in mind that under the GDPR you cannot charge a fee to provide this information, and in most cases, must supply me with the information within 1 month.

If you need any advice on dealing with this request, you can contact the Information Commissioner’s Office on 0303 123 1113 or at [www.ico.org.uk](http://www.ico.org.uk)

Yours sincerely,

Signed: Name: Date:

**Appendix 3 - Privacy Impact Assessment**

A privacy impact assessments is completed when the school’s processing of personal data presents a risk to rights and freedoms of individuals, and when introducing new technologies. Below shows an overview of the process. More information can be found at: <https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf>



**Appendix 4 Data Breach Record**

**Contact details**

|  |  |
| --- | --- |
| Name of person who raised the issue: |  |
| Contact email address of person who raised the issue:  |  |
| Contact telephone number of person who raised the issue:  |  |
| Job title: |  |
| Date:  |  |

**Incident information**

|  |  |
| --- | --- |
| Type of data breach:  |  |
|  Date and time of data breach:  |  |
| Date and time breach was noticed:  |  |
| Action taken when breach was identified:  |  |
| Identification code of devices involved: |  |
| Description and location of devices:  |  |
| Description of what caused the breach:  |  |
| If breach was due to human error, name the member of staff and when they last received data protection training:  |  |
| Details of any personal data that was compromised:  |  |
| Approximate number of data subjects affected: |  |
| Identity of user and website or service being accessed: |  |
| What is the likely impact of the breach?  |  |
| Have persons affected been informed of the breach and when were they informed? |  |
|  |  |
|  Have persons affected been informed on how the breach will be rectified?  |  |
| Have any external bodies been informed of the breach, e.g. the ICO?  |  |
| Description of any disciplinary action taken:  |  |
| Steps taken to prevent further data loss, including changes to existing procedure and refresher training given:  |  |
| Conclusion:  |  |

By signing this form, DPO agrees that the information within this form has been checked and is correct upon date of completion. All information in this form will be stored for school records so that the school can use the information to ensure their security systems are kept safe to minimise risks of a data breach.

**Name of DPO:**

**Signed (DPO):**

**Date form completed:**