Founded 1125

Policy number F8a

Reading School

Data Policy

Storage of Personal Data and Privacy

Responsibilities	
Policy Owner:	Name, Jo Lidbetter Title: Office Manager
Governors Committee	Finance
Audit Control	
Policy created:	22/06/21
Date of next review	June 2022
Version:	1.0
Statutory policy	Yes

Data Policy

Document Control and Approval

Version Control

Version	Author	Summary of Changes	Reviewed By	Date
1.0	Jonathan Hitchinson	Policy created	Jonathan Hitchinson	01/05/2021

Responsibilities

Job title	Responsible for;
Office Manager	Policy Owner
Chief Operating Officer	Policy Overview
Finance Committee	Committee Responsible

Policies Linked

Policy name	File location

Forms Linked

Form name	Form location

Staff that need to sign

Staff Group	Form location

Data Policy

Contents

Data Protection

Aims

Reading 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 UK General Data Protection Regulation (UK GDPR), tailored by the Data Protection Act 2018 (DPA 2018).

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 UK GDPR and the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data. In addition, this policy complies with our funding agreement and articles of association.

Definitions

Term	Definition
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.
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
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 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.

The data controller

Reading School processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller. The school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required

Roles and responsibilities

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

Governing board

The governing board has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

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 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.
- Our DPO is Satswana and is contactable via http://www.satswana.com.
- Their contact details are as follows:

Pembroke House,
St. Christopher's Place,Farnborough,
Hampshire GU14 0NH

Tel: 01252 516898**Email**: info@satswana.com

Headmaster

The headmaster acts as the representative of the data controller on a day-to-day basis.

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

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.

Collecting personal data

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 Chapter 2, sections 8 & 10 of the 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.

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 Retention Guidelines.

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 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.

Subject access requests and other rights of individuals

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 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.

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 13 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.

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.

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.

Parental requests to see the educational record

There is no automatic parental right to access the educational record in an Academy. However, at Reading School, we will consider requests from parents. Parents should put a request in writing to the Headmaster. The school will respond within 15 school days.

Biometric recognition systems

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils 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 pupils 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 pupils. For example, pupils can pay for school dinners in cash to the Finance Office if they wish.
Parents/carers and pupils 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 pupil 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 pupil's parent(s)/carer(s).

Where staff members or other adults use the school's 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.

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, or pupils aged 18 and over, for photographs and videos to be taken of pupils 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 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

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.

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 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)
- 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

Data security and storage of records

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
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- 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 as for school-owned equipment (see our E Safety Policy and ICT User Agreement)
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

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.

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.

Data Breach

Personal data breaches

Under GDPR, all organisations acting as data controllers must report security breaches involving personal data to the relevant supervisory authority if the breach is likely to result in a risk to individuals' rights and freedoms.

Such breaches must be reported without undue delay and, where feasible, within 72 hours of becoming aware of the breach. There is also a requirement to keep a record of such breaches.

While the GDPR is in relation to 'personal data', breaches involving any kind of data should also be reported internally and to appropriate personnel in accordance with this policy.

This policy should be considered in conjunction with:

- The internal data security policy.
- The management and retention of records policy.
- Personnel record keeping policy.
- The privacy notices.

- The ICT policies.

Responsibilities

All employees, workers, governors, and consultants are responsible for reporting any data breaches they discover, or are responsible for, and for assisting in investigations where required.

Data breaches must be reported to the data protection officer (DPO) to consider what actions need to be taken with management and IT to address the incident, including whether to report the incident to the Information Commissioner's Office (ICO) and any affected individuals.

What is a personal data breach?

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to personal data. Broadly, it can be defined as a security incident that compromises the confidentiality, integrity or availability of personal data.

- 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

A data security breach can happen for a number of reasons:

- Loss or theft of data or equipment on which data is stored.
- Inappropriate access controls allowing unauthorised use.
- Equipment failure.
- Human error.
- Unforeseen circumstances, such as a fire or flood.
- Hacking attack.
- 'Blagging' offences where information is obtained by deceiving the organisation that holds it.

However the breach has occurred, there are four important elements to any breach management plan:

- Containment and recovery.
- Assessment of ongoing risk.
- Notification of breach.
- Evaluation and response.

What are the school's responsibilities?

Data Policy

We process personal data on behalf of our pupils, their parents or guardians and all personnel connected within the school, including our staff and volunteers. Under the GDPR,we are classed as a ‘data controller ‘and we are therefore responsible for ensuring compliance with the various laws in place to protect individual privacy rights. We have privacy notices in place for the various categories of individuals whose data we process.

Where we engage third parties to process personal data on our behalf, such as payroll, we must also ensure that they process our data in a way that is compatible with the GDPR to ensure that the personal data is not compromised in anyway. We have set up arrangements to ensure that any third parties we engage, known as ‘data processors’, are GDPR compliant and have in place appropriate breach protocols and notification requirements.

While this policy is largely focused on personal data and our obligations under the GDPR, internal data and commercially sensitive data must likewise be protected and secure. Data breaches relating to any sort of data should be reported to the DPO. What to do if you suspect there has been a data breach regarding personal data? Data breaches could involve anyone’s personal data that we process at the school. Do not investigate the matter yourself. Complete an incident form and pass it to the DPO.

What to do if you suspect there has been a data breach regarding personal data?

Data breaches could involve anyone’s personal data that we process at the school. Do not investigate the matter yourself. Complete an incident form and pass it to the Droplets see appendix 1 for the data breach incident form. Due to the legal requirements of reporting personal data breaches within 72 hours, or such reasonable time, it is crucial that breaches are addressed immediately. Do not ignore them because the consequences may be worse, and can include substantial fines and penalties as well as personal repercussions for you.

If the breach involves the compromising of servers/IT security systems, you should also contact the IT department, so that immediate action can be taken to limit any damage/exposure.

What happens next?

Data breaches, whether they involve personal data or not, will be considered in line with our data breach protocol (appendix 2). You may be required to assist with the investigation process and/or help resolve any security incidents as part of your role.

Links with other policies

Data Policy

This data protection policy is linked to our:

- Freedom of information publication scheme
- E Safety Policy
- Privacy Notices
- Child Protection Policy
- Safeguarding Policy
- ICT User Agreement

Appendix

Data Breach Incident Form

Description of the data breach		
Time and date the breach was identified and by whom	Time	Date
Who is reporting the breach	Name	Job Title
Contact details	Mobile	Email
Classification of data breached • Personal data • Internal data • Confidential data • Highly confidential data • Commercial data		
Volume of data involved		
Confirmed or suspected breach?		
Is the breach contained or ongoing?		
Who has been informed of the breach?		
Any other information		

Data Breach Protocol

This protocol sets out what we need to do in the event of a data breach. Stage one below is covered by the data breach policy. However, stages two to four will be carried out by the DPO with appropriate support from other personnel, such as IT support and the DPM.

The data breach protocol comprises four stages

- Incident report to the DPO.
- Containment and recovery/investigation and assessment of data breach.
- Consideration of reporting requirements to ICO/individual.
- Evaluation and response, record of breach kept, consideration of any additional security measures needed.

Stage one – incident report

Any data breaches must be reported to the DPO immediately in line with the data breach policy above.

Stage two – containment and recovery/investigation and assessment

Containment and recovery

Depending on the type of breach incident, it may be appropriate to take immediate steps to contain the threat or recover the data. Consult with IT and management.

The requirement to report breaches to individuals in high risk cases may require the DPO to notify individuals whose personal data has or may have been compromised of the situation straightaway. This consideration should be kept under constant review throughout the process.

Any 'data processor' breaches by any of the third parties we engage should also be reported to us to enable us to take appropriate action.

Investigation and assessment

Investigating the incident will involve:

- Considering the incident report.
- Discussing matters with appropriate personnel and obtaining relevant reports/statements.
- Finding out what has happened and what data is affected.
- Consideration of whether the data is high risk, commercially sensitive or includes personal data/special categories of personal data.
- Keeping a timeline/log and updating the developments of the breach.
- Consideration of whether, in the case of personal data, the breach affects the fundamental rights and freedoms of the data subject with regard to:
    - Any resulting physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights,

discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.

- The severity of the breach generally.

Stage three – breach reporting

Given the length of time that incidents have to be reported by, it may be appropriate to report the incident without having fully investigated the issues. Matters may develop, and a log should be kept as they do.

If the breach does impact on the rights and freedoms of the data subject(s), report the breach to the ICO if appropriate at https://ico.org.uk/for-organisations/report-a-breach.

Notify any data subject of the personal data breach if appropriate where there is a high risk and without undue delay. This will allow the data subject to mitigate any immediate risks of damage. Notification should include:

- Details of the DPO.
- A description of the likely consequences of the personal data breach.
- A description of the measures taken, or proposed to be taken, to deal with the breach including any measures to mitigate any possible adverse effects.

Consideration must be given to whether our insurers need to be informed.

Stage four – evaluation and response

The final breach report should include a summary of the facts of the breach, its effects and the remedial action we have taken. Consideration of whether the issue is human error or not and how reoccurrence can be prevented.