Our Rock Academy

Data Protection Policy

" A nurturing, ambitious and inclusive school where every child feels known, valued and connected."

Author: Michelle Homer

Approved by: Emmanuel Ajayi

Date: 2nd September 2026

Review Date: 2nd September 2027

Version Control

Date	Revisions

Resilience, Ownership, Creativity and Kindness

Introduction

Our Rock Academy is committed to protecting the privacy, dignity and rights of all members of its community. The school recognises that it holds and processes significant amounts of personal information relating to pupils, families, staff, governors, volunteers and other individuals. Maintaining the confidentiality, integrity and security of this information is fundamental to safeguarding, effective education and the trust placed in the school.

This policy explains how the school manages personal data and demonstrates its commitment to complying with data protection legislation. It provides the framework through which personal information is collected, used, stored, shared and disposed of appropriately whilst enabling the school to fulfil its educational, legal and safeguarding responsibilities.

Purpose

The purpose of this policy is to ensure that personal information is processed lawfully, fairly and securely throughout the school.
It establishes the principles that govern the handling of personal data, clarifies the responsibilities of those working within the school and provides assurance that information is managed in accordance with current legislation and recognised good practice.

Scope

This policy applies to all personal data processed by or on behalf of Our Rock Academy, regardless of whether that information is held electronically, on paper, within photographs, audio recordings or other formats.

It applies to every person who processes information on behalf of the school, including employees, agency staff, volunteers, contractors, governors, consultants and external service providers. Everyone working for or on behalf of the school has a responsibility to protect personal information and comply with this policy.

Legal Framework

Our Rock Academy processes personal information in accordance with the requirements of the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and subsequent amendments to UK data protection legislation, including the Data (Use and Access) Act 2025 where applicable.

The school also recognises its wider statutory duties relating to safeguarding, education, employment, equality and health and safety, all of which may require the lawful processing or sharing of personal information.

Data Protection Principles

The school is committed to ensuring that personal information is processed in accordance with the principles established by UK data protection legislation.

Personal information will only be collected where there is a clear and lawful reason for doing so. Information will be used fairly and transparently, collected only for specified purposes and limited to that which is necessary. The school will take reasonable steps to ensure that information remains accurate and up to date and will not retain personal information for longer than necessary. Appropriate technical and organisational measures will be implemented to protect information against unauthorised access, loss, alteration or destruction. The school will also be able to demonstrate compliance with these principles through effective governance, staff training and documented procedures.

Roles and Responsibilities

The Proprietor has overall responsibility for ensuring that the school complies with its legal obligations relating to data protection and provides appropriate governance and oversight.

The Headteacher has operational responsibility for implementing this policy, ensuring appropriate procedures are in place and promoting a culture of good information governance throughout the school.

Managers are responsible for ensuring that staff within their areas understand and follow the school's procedures, whilst every member of staff shares responsibility for protecting personal information and reporting concerns promptly.

The school will nominate the Headteacher as the Data Protection Officer to provide advice, monitor compliance and act as the primary contact for the Information Commissioner's Office (ICO).

Personal Information Processed by the School

To fulfil its educational and legal responsibilities, the school processes information relating to pupils, parents and carers, members of staff, governors, volunteers, contractors and visitors.

This information may include contact details, attendance records, assessment information, safeguarding records, health information, special educational needs documentation, employment records, financial information, photographs, CCTV images and other information necessary for the effective operation of the school.
Where the school processes special category information, including health data or information relating to safeguarding, it will ensure that an appropriate lawful basis and additional condition for processing has been identified.

Lawful Processing

The school will only process personal information where there is a lawful basis for doing so. Most information is processed because it is necessary to fulfil legal obligations placed upon the school, to carry out tasks in the public interest, to fulfil contractual responsibilities or to protect the vital interests of individuals.

Where consent is relied upon, it will be freely given, specific, informed and capable of being withdrawn.

The school will ensure that the lawful basis for processing is identified before personal information is collected.

Individual Rights

Individuals whose personal information is processed by the school have a number of legal rights under data protection legislation.

These include the right to be informed about how their information is used, the right to request access to personal information held about them, the right to request correction of inaccurate information and, in certain circumstances, the right to request deletion, restriction or objection to processing.

Requests relating to personal information will be managed promptly and within the statutory timescales.

Individuals may complain to the school about how their personal information has been used. The school will acknowledge data protection complaints within 30 calendar days, investigate without undue delay, keep the complainant informed and explain the outcome.

The school will provide clear Privacy Notices explaining how personal information is collected and used.

Information Security

Protecting personal information is everyone's responsibility.

The school will implement appropriate physical, organisational and technical security measures to protect information from accidental or unlawful loss, unauthorised disclosure or inappropriate access.

Electronic systems will be password protected, supported by appropriate access controls and regularly updated. Paper records containing confidential information will be stored securely when not in use.
Staff are expected to exercise professional judgement when handling personal information and should ensure that confidential information cannot be viewed or accessed by unauthorised individuals.

Information Sharing

Sharing information appropriately is an important part of safeguarding and supporting pupils. The school will only share personal information where there is a lawful basis for doing so or where there is a clear safeguarding, legal or educational reason.

Information sharing decisions will always consider necessity, proportionality and the rights of the individual whilst recognising that concerns about data protection should never prevent appropriate action being taken to safeguard a child.

Where external organisations process information on behalf of the school, appropriate contractual arrangements will be in place to ensure compliance with data protection legislation.

Data Retention and Disposal

Personal information will only be retained for as long as there is a legitimate educational, legal or operational reason for doing so.

The school maintains a separate Records Retention Schedule which specifies appropriate retention periods for different categories of information.

When records reach the end of their retention period they will be disposed of securely in a manner that protects confidentiality and prevents unauthorised access.

Data Breaches

Despite robust security measures, there may be occasions where personal information is lost, accessed without authority or disclosed inappropriately.

Any suspected or actual data breach must be reported immediately to the Headteacher or designated member of the senior leadership team so that appropriate action can be taken without delay.

The school will investigate every reported breach, take action to minimise any potential harm, notify affected individuals where appropriate and report breaches to the Information Commissioner's Office where the legal threshold for notification has been met.

The school maintains a separate Data Breach Procedure to support the effective management of incidents.

Training and Awareness

Effective data protection relies upon the knowledge and vigilance of all staff.

All employees will receive data protection training appropriate to their role as part of their induction and through regular refresher training. Additional guidance will be provided whenever legislation, technology or school procedures change.

Staff are expected to seek advice whenever they are uncertain about the correct handling of personal information**.**

Monitoring and Review

The Headteacher will monitor compliance with this policy through regular review of information management practices, staff training, audits and incident reporting.

The Proprietor will receive appropriate assurance that the school continues to meet its statutory responsibilities and that any significant risks are identified and addressed promptly.

This policy will be reviewed annually or sooner where changes to legislation, statutory guidance or operational practice require amendment.

Appendix 1
Data Breach Procedure

Purpose
Our Rock Academy is committed to protecting the personal information it holds about pupils, families, staff and other members of the school community. Despite robust security measures, there may be occasions where personal information is lost, accessed without authorisation, disclosed in error or otherwise compromised.
This procedure explains how suspected or actual personal data breaches must be reported, investigated and managed to minimise harm and ensure compliance with UK data protection legislation.

1. **What is a Personal Data Breach?**

A personal data breach is any incident that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information.
Examples include sending confidential information to the wrong recipient, losing paperwork containing personal information, leaving confidential records unsecured, cyber-attacks, stolen devices or unauthorised access to school systems.
Not every incident will require notification to the Information Commissioner's Office (ICO), but every suspected breach must be reported internally.

2. **Reporting a Breach**

Any member of staff who becomes aware of a suspected or actual data breach must report it immediately to the Headteacher or, in their absence, the senior member of staff on duty.
Staff should not attempt to conceal incidents or assume that someone else has reported them. Prompt reporting enables the school to reduce potential harm and meet statutory reporting timescales where necessary.
The report should include:

- what happened;
- when the incident occurred;
- what information was involved;
- who may be affected; and
- any immediate action already taken.

3. **Immediate Action**

On receiving a report, the Headteacher will take immediate steps to contain the incident wherever possible.
This may include recovering information, recalling emails, changing passwords, restricting access to systems, contacting recipients, securing documents or temporarily disconnecting affected equipment.
The priority will always be to minimise any risk to individuals whose personal information may have been affected.

4. Investigation

Every reported breach will be investigated to determine:

- what happened;
- the type of information involved;
- how many individuals are affected;
- the likelihood of harm;
- whether the breach has been contained; and
- what further action is required.

The investigation will also consider whether changes to procedures, systems or staff training are needed to prevent a recurrence.

5. Notification

Where a breach is likely to result in a risk to the rights and freedoms of individuals, the school will notify the Information Commissioner's Office without undue delay and, where required, within 72 hours of becoming aware of the breach.
Where the breach is likely to result in a high risk to individuals, those affected will also be informed promptly unless an exemption applies.

6. Recording Breaches

All suspected and confirmed data breaches, regardless of severity, will be recorded in the school's Data Breach Register.
The record will include:

- the date of the incident;
- the nature of the breach;
- the information affected;
- action taken;
- whether the ICO was notified; and
- lessons learned.

Maintaining a complete record supports accountability and continuous improvement.

7. Learning from Incidents

Following any breach, the school will review the circumstances surrounding the incident to identify opportunities for improvement.
This may include updating procedures, improving technical security, providing additional staff training or strengthening existing controls.
The aim is to reduce the likelihood of similar incidents occurring in the future.

8. Responsibilities

Every member of staff shares responsibility for protecting personal information and reporting concerns promptly.
The Headteacher is responsible for managing reported breaches, maintaining appropriate records and ensuring compliance with statutory reporting requirements.
Where appointed, the Data Protection Officer will provide advice and support throughout the investigation and notification process.

9. Monitoring and Review

This procedure will be reviewed annually or sooner if changes to legislation, guidance or operational practice require amendment.