Our Rock Academy

Online Safety 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

Purpose

Our Rock Academy is committed to providing a safe, secure and inclusive digital environment where technology enhances learning whilst protecting pupils from online harm.
This policy sets out how the school promotes safe and responsible use of technology, safeguards pupils from online risks, and responds to online safety concerns. It applies to all pupils, staff, governors, volunteers, contractors and visitors who use school technology, access school systems or engage with the school online.

Legal Framework

- This policy has been developed with reference to:
- Keeping Children Safe in Education (current edition)
- Working Together to Safeguard Children
- Education Act 2002
- Equality Act 2010
- UK GDPR and Data Protection Act 2018
- Prevent Duty Guidance
- Independent School Standards Regulations

This policy should be read alongside the Safeguarding and Child Protection Policy, Behaviour Policy, Staff Code of Conduct, Data Protection Policy and Acceptable Use Agreements.

Aims

The school aims to:

- protect pupils from online harm;
- promote safe, responsible and respectful use of technology;
- teach pupils how to manage online risks confidently;
- support positive digital citizenship;
- maintain secure school systems and data;
- respond effectively to online safety incidents;
- work in partnership with parents and carers to promote online safety.

Roles and Responsibilities

Role	Responsibilities
Governing Body	Ensure appropriate online safety arrangements are in place, including effective filtering and monitoring systems. Review their effectiveness at least annually and provide strategic oversight of online safeguarding.
Headteacher	Ensure this policy is implemented, appropriate training is provided and online safety is embedded across the school. Ensure the school's filtering and monitoring arrangements are maintained, checked and reviewed.
Designated Safeguarding Lead (DSL)	Lead on safeguarding concerns relating to online safety, provide advice to staff, manage referrals and monitor emerging risks.
Staff	Promote safe online behaviour, teach online safety, supervise technology use appropriately and report concerns immediately.
Pupils	Use technology safely, responsibly and respectfully, following school expectations and reporting anything that makes them feel unsafe.
Parents and Carers	Encourage safe technology use at home and work in partnership with the school where concerns arise.

Teaching Online Safety

Online safety is embedded throughout the curriculum and wider school life. Learning is adapted to pupils' age, developmental stage, communication needs and individual vulnerabilities.

Pupils are taught about:

- protecting personal information;
- respectful online communication;
- healthy online relationships;
- cyberbullying;
- online scams and phishing;
- misinformation and fake news;
- gaming and livestreaming;
- online exploitation and grooming;
- consent and sharing images online;
- radicalisation and extremist content;
- digital footprints and reputation;
- artificial intelligence and responsible use;
- managing screen time and digital wellbeing.

Online safety is reinforced through Personal Development, Computing, therapeutic interventions and individual support where appropriate.

Staff Training

All staff receive regular online safety training as part of the school's safeguarding programme. Training reflects:

- current safeguarding guidance;
- emerging technologies;
- artificial intelligence;
- filtering and monitoring procedures;
- cyber security awareness;
- local and national safeguarding risks.

All staff are expected to read Part One of *Keeping Children Safe in Education* and understand their responsibilities for safeguarding pupils online.

Safe Use of Technology
Technology should always be used safely, responsibly and for legitimate educational purposes.

Users are expected to:
- keep passwords secure;
- protect personal and confidential information;
- use school systems appropriately;
- communicate respectfully online;
- report inappropriate content or behaviour immediately;
- follow all acceptable use expectations.

Users must not:
- deliberately bypass filtering or monitoring systems;
- access inappropriate or illegal material;
- share passwords;
- misuse school equipment or accounts;
- access another person's account without permission.

School devices, networks and accounts remain the property of the school.

Filtering and Monitoring
The school uses filtering and monitoring systems to reduce the risk of pupils accessing harmful or inappropriate material and to identify safeguarding concerns.

Filtering and monitoring arrangements are proportionate to the age, needs and vulnerabilities of pupils.

The Governing Body will review the effectiveness of filtering and monitoring arrangements at least annually, considering:
- emerging online risks;
- safeguarding incidents;
- monitoring reports;
- system effectiveness;
- required improvements.

Use of school devices, networks and accounts may be monitored for safeguarding and security purposes. The school will explain this monitoring in its privacy notices and limit access to monitoring information to authorised staff.

Concerns identified through filtering or monitoring will be reviewed promptly and managed in accordance with safeguarding procedures.

Artificial Intelligence (AI)
Artificial intelligence (AI) is increasingly used in education and everyday life. The school recognises that AI can support learning when used safely and responsibly.

Pupils may use approved AI tools where authorised by staff to support learning, research and creativity.

AI must not be used to:
- complete assessed work dishonestly;

- generate harmful, abusive or inappropriate content;
- impersonate another person;
- create or distribute misleading or manipulated images or videos;
- input confidential, personal or safeguarding information into publicly available AI platforms.

Pupils will be taught to critically evaluate AI-generated content and understand that AI responses may be inaccurate, biased or misleading.

Staff remain responsible for checking the accuracy and suitability of any AI-generated material used within teaching.

Responding to Online Safety Concerns

Any online safety concern involving a pupil will be treated as a safeguarding matter.

Staff must:

- respond calmly and reassure the pupil;
- preserve evidence where appropriate;
- report concerns immediately to the Designated Safeguarding Lead;
- record concerns using the school's safeguarding recording system;
- follow the Safeguarding and Child Protection Policy.

Parents and carers will be informed where appropriate. External agencies, including the police or children's social care, will be involved where required.

Cyber Security

The school takes reasonable steps to protect its systems, information and users through:

- secure passwords and multi-factor authentication where appropriate;
- regular software updates;
- secure data backups;
- restricted user permissions;
- anti-virus and security software;
- monitoring of cyber security alerts and incidents by the person or service responsible for the school’s IT systems;
- staff awareness training.

Any suspected cyber security incident must be reported immediately to the Headteacher.

Monitoring and Review

The Headteacher is responsible for implementing this policy.

The Governing Body will review the effectiveness of the school's online safety arrangements annually, considering safeguarding incidents, filtering and monitoring reports, staff training, cyber security and changes to national guidance.

The policy will also be reviewed following any significant safeguarding or cyber security incident, or where changes in legislation or guidance require it.

Appendix A
Staff Acceptable Use Agreement

All staff are expected to use technology safely, professionally and in accordance with safeguarding responsibilities.

Staff will:

- use school technology for legitimate educational and professional purposes;
- protect usernames and passwords and never share login details;
- use strong passwords and multi-factor authentication where available;
- lock devices when unattended;
- keep personal and confidential information secure;
- only use approved software and applications;
- report suspected cyber security incidents immediately;
- follow the school's Data Protection Policy;
- maintain professional boundaries when communicating online;
- model positive digital behaviour for pupils.

Staff must not:

- access inappropriate, offensive or illegal material;
- deliberately bypass filtering or monitoring systems;
- install unauthorised software;
- use personal email accounts to store or send confidential school information;
- communicate privately with pupils using personal social media accounts or messaging services;
- photograph or record pupils using personal devices unless authorised in exceptional circumstances.

Artificial Intelligence (AI)
Staff may use approved AI tools to support planning, administration and resource development where appropriate.

Staff must:

- check the accuracy of AI-generated content;
- ensure work remains professionally appropriate;
- never enter confidential, personal or safeguarding information into publicly available AI platforms;
- comply with copyright, data protection and safeguarding requirements.

Failure to comply with this agreement may result in disciplinary action.

Name: _____

Signature: _____

Date: _____

Appendix B
Pupil Acceptable Use Agreement

Pupils are expected to use technology safely, respectfully and responsibly.

Pupils agree to:

- use technology to support learning;
- treat others with kindness and respect online;
- keep passwords private;
- tell a trusted adult if something online makes them feel worried, upset or unsafe;
- follow staff instructions when using technology;
- take care of school equipment.

Pupils must not:

- access unsuitable websites;
- share personal information without permission;
- attempt to bypass school filtering;
- deliberately damage equipment;
- bully, threaten or upset others online;
- record or photograph others without permission.

Where AI tools are used, pupils must:

- use them only when authorised by staff;
- complete their own work honestly;
- understand that AI may sometimes provide incorrect information.

Failure to follow this agreement may result in restrictions on technology use and other appropriate consequences.

Pupil Name: _____

Signature: _____

Date: _____

Appendix C
Filtering and Monitoring Statement

Our Rock Academy uses filtering and monitoring systems to help safeguard pupils and protect school systems.

Filtering aims to prevent access to harmful or inappropriate online content.

Monitoring helps identify potential safeguarding concerns, inappropriate use of technology and cyber security risks.

Filtering and monitoring arrangements are proportionate to the age, needs and vulnerabilities of pupils.

The school will:

- review filtering and monitoring arrangements at least annually;
- review arrangements following significant safeguarding or cyber security incidents;
- arrange technical support to maintain appropriate filtering and monitoring protection;
- respond promptly to alerts and safeguarding concerns;
- regularly consider emerging online risks.

Monitoring is used solely to support safeguarding, cyber security and the effective management of school systems.

Use of school devices, networks and accounts may be monitored for safeguarding and security purposes. The school will explain this monitoring in its privacy notices and limit access to monitoring information to authorised staff.

Appendix D
Artificial Intelligence (AI) Guidance

Artificial intelligence is becoming part of education and everyday life. Used appropriately, AI can enhance learning and support staff. Used inappropriately, it can create safeguarding, privacy and academic integrity risks.

Staff

Staff may use approved AI tools to:

- support lesson planning;
- generate ideas;
- create draft resources;
- improve accessibility;
- reduce administrative workload.

Staff must:

- review all AI-generated content before use;
- ensure resources remain accurate and appropriate**;**
- never upload confidential, personal or safeguarding information;
- ensure pupils continue to develop independent thinking.

Pupils

Pupils may use AI only when authorised by staff.

Pupils should:

- use AI to support learning rather than replace it;
- question whether AI responses are accurate;
- recognise that AI can produce incorrect or biased information;
- acknowledge AI use where appropriate.

AI must never be used to:

- cheat in assessments;
- create harmful, offensive or inappropriate material;
- impersonate another person;
- create or distribute manipulated images or videos intended to harm others.

Appendix E
Online Safety Incident Procedure

1. Immediate Action
Where there is an online safety concern:

- ensure the pupil is safe;
- listen and reassure;
- do not promise confidentiality;
- preserve evidence where appropriate (If the concern involves a nude or semi-nude image of a child, do not view, copy, screenshot, save or forward the image. Report it to the DSL immediately and follow the specific safeguarding guidance.)

2. Report
The concern must be reported immediately to the Designated Safeguarding Lead.
If the DSL is unavailable, report to a Deputy DSL or the Headteacher.

3. Record
Record the concern on the school's CPOMs, including:

- what happened;
- when it occurred;
- who was involved;
- any action already taken;
- a description of any evidence, and copies only where appropriate and lawful; never attach nude or semi-nude images of a child.

4. Risk Assessment
The DSL will consider:

- immediate safeguarding risks;
- whether parents should be informed;
- whether other pupils may be at risk;
- whether external agencies should be involved.

5. Further Action
Depending on the circumstances, action may include:

- support for the pupil;
- education and restorative work;
- behaviour sanctions where appropriate;
- referral to Children's Social Care;
- referral to the Police;
- referral to Prevent;
- reporting harmful online content to the appropriate platform or service.

6. Review
The DSL will:

- ensure appropriate support is provided;
- monitor ongoing risk;
- review whether additional education or changes to filtering and monitoring are required;
- record the outcome and any lessons learned.