

Online Safety Policy

Staff Responsible:	**Mr D Frankish**
Date of Issue:	September 2026
Review Date:	September 2027

Introduction

The purpose of Online Safety at Ribbon Academy is to:

- Educate pupils about online safety issues and appropriate behaviours so that they remain safe, responsible and lawful online.
- Help pupils develop critical thinking skills and digital resilience.
- Promote the safe and secure use of technology for teaching, learning and communication.
- Minimise risks associated with handling sensitive and personal information.
- Protect children, staff and the wider school community from online harm.
- Ensure compliance with safeguarding, data protection and cyber security requirements.

This policy applies to all members of the school community, including pupils, staff, trustees, visitors, contractors and volunteers who access school systems, devices or networks.

This policy refers to all forms of digital technology including:

- Computers, laptops, Chromebooks, tablets, iPads and mobile devices.
- Smart watches and wearable technology.
- Digital cameras and recording devices.
- School networks and cloud-based services.
- Websites, online platforms and learning systems.
- Email and communication platforms.
- Social media platforms.
- Artificial intelligence (AI) tools and applications.
- Future technologies adopted by the school.

Online safety depends upon effective practice in the following areas:

- Education for responsible and safe technology use.
- A comprehensive and well-implemented Online Safety Policy.
- Effective safeguarding procedures.
- Secure, filtered broadband services.
- Effective filtering and monitoring systems.
- Strong cyber security arrangements.
- Staff training and awareness.
- Partnership working with parents and carers.

This policy should be read alongside:

- Child Protection and Safeguarding Policy.
- Behaviour Policy.
- Anti-Bullying Policy.
- Data Protection Policy.
- Staff Code of Conduct.
- Acceptable Use Agreements.
- Filtering and Monitoring Policy.
- Mobile Phone Policy.

This policy has due regard to relevant legislation and guidance including:

- Keeping Children Safe in Education (KCSIE).
- UK General Data Protection Regulation (UK GDPR).

- Data Protection Act 2018.
- Education for a Connected World.
- DfE Teaching Online Safety in Schools.
- DfE Filtering and Monitoring Standards for Schools and Colleges.
- DfE guidance on Harmful Online Challenges and Online Hoaxes.
- DfE guidance on Generative Artificial Intelligence in Education.
- Sharing Nudes and Semi-Nudes guidance.
- National Cyber Security Centre (NCSC) cyber security guidance.
- Voyeurism (Offences) Act 2019.
- Online Safety Act 2023.

Roles and Responsibilities

The Headteacher has overall responsibility for ensuring the safety and wellbeing of all members of the school community, including online safety.

The Headteacher will:

- Ensure appropriate Online Safety arrangements are in place.
- Appoint an Online Safety Leader.
- Ensure staff receive appropriate training.
- Ensure online safety forms part of safeguarding arrangements.
- Ensure effective filtering and monitoring arrangements are maintained.
- Ensure concerns are acted upon appropriately.

The Board of Trustees will:

- Provide strategic oversight of online safety.
- Review the effectiveness of filtering and monitoring systems annually.
- Ensure safeguarding risks arising from technology are understood and managed.
- Challenge and support leaders to maintain effective online safety provision.
- Ensure Online Safety and cyber security are considered within governance processes.

The Designated Safeguarding Lead (DSL) will:

- Take lead responsibility for online safeguarding.
- Monitor online safety incidents and emerging risks.
- Manage referrals and safeguarding concerns.
- Ensure online safety training is included in safeguarding training.
- Work with technical staff regarding filtering and monitoring systems.
- Maintain online safety records and incident logs.
- Report trends and concerns to senior leaders and trustees.
- Understand additional online risks faced by vulnerable pupils and pupils with SEND.

The Computing Leader will:

- Monitor implementation of this policy.
- Support curriculum delivery.
- Ensure resources are available for staff.
- Promote online safety across the school community.
- Coordinate online safety awareness events and campaigns.

ICT Technical Support Staff will:

- Maintain secure systems.
- Manage filtering and monitoring arrangements.
- Implement cyber security controls.
- Respond to technical incidents.
- Carry out regular system reviews.
- Support investigations into online safety concerns where appropriate.

All staff are responsible for:

- Following this policy and the Staff Code of Conduct.
- Maintaining professional behaviour online.
- Reporting concerns immediately through CPOMS.
- Delivering online safety education where appropriate.
- Supervising pupils when using technology.
- Understanding filtering and monitoring arrangements.
- Completing required training.

Pupils are responsible for:

- Following the Acceptable Use Agreement.
- Reporting concerns to trusted adults.
- Using school systems responsibly.
- Respecting others online.
- Understanding how to keep themselves safe online.

Parents and carers play a vital role and are encouraged to:

- Support the school's online safety messages.
- Monitor their child's use of technology.
- Report concerns to school.
- Engage with online safety information shared by the school.

Staff Training

All members of staff receive annual safeguarding training which includes online safety.

Training will include:

- Current online risks.
- Cyberbullying.
- Online grooming.
- Radicalisation and extremism.
- Child-on-child abuse online.
- Sextortion and online exploitation.
- AI and emerging technologies.
- Filtering and monitoring expectations.
- Cyber security awareness.
- Phishing awareness.
- Reporting procedures.

Additional training will be provided where emerging risks are identified.

Teaching and Learning

The internet is an essential element of modern life and learning. The school will provide pupils with high-quality access to digital technologies whilst maintaining appropriate safeguards.

Pupils will be taught:

- How to stay safe online.
- How to manage online relationships safely.
- Privacy and security awareness.
- Safe social media use.
- Critical evaluation of online information.
- Copyright and intellectual property.
- Online reputation management.
- The safe use of AI technologies.
- How to recognise scams, misinformation and manipulation.
- How to seek help and report concerns.

Online safety education is embedded throughout the curriculum and reinforced through assemblies, themed events, safeguarding activities and daily classroom practice.

Artificial Intelligence (AI)

The school recognises the growing role of Artificial Intelligence in education.

The use of AI must support learning whilst safeguarding children, staff and personal information.

Staff must:

- Only use approved AI tools where appropriate.
- Remain responsible for all content produced using AI.
- Verify the accuracy of AI-generated information.
- Never input personal, confidential or safeguarding information into public AI systems.
- Consider safeguarding, bias, equality and copyright implications.
- Use AI in accordance with data protection requirements.

Pupils will be taught:

- How AI systems work.
- The benefits and limitations of AI.
- The importance of fact-checking AI outputs.
- Responsible and ethical use of AI technologies.
- Risks associated with AI-generated content.

Pupils with SEND

The school recognises that some pupils with SEND face additional online risks.

To support these pupils:

- Online safety learning may be differentiated.
- Additional adult support may be provided.
- Visual resources may be used where appropriate.

- Individual risk assessments may be developed.
- Staff will consider communication and social understanding needs.
- Enhanced support may be offered during transition periods.

Managing Internet Access and Cyber Security

The school's ICT systems are managed and monitored to ensure safe and secure use.

The school will:

- Maintain secure network infrastructure.
- Use antivirus and malware protection systems.
- Monitor security risks.
- Restrict access to authorised users.
- Ensure secure access to cloud systems.
- Protect personal data appropriately.
- Regularly review cyber security arrangements.

Staff must:

- Use strong passwords.
- Keep passwords confidential.
- Lock devices when unattended.
- Report suspected cyber incidents immediately.
- Be alert to phishing attempts.
- Use approved systems for storing and sharing information.

Where available, multi-factor authentication will be implemented to strengthen account security.

Email

Approved school email systems must be used for educational and professional purposes.

Users must:

- Report offensive or concerning messages immediately.
- Treat unexpected emails and attachments with caution.
- Never reveal personal information unnecessarily.
- Follow safeguarding procedures where concerns arise.
- Avoid opening suspicious links or attachments.

Websites, Social Media and Published Content

The school website, social media channels and communication platforms will present accurate and appropriate information.

The following principles apply:

- Personal contact details will not be published.
- Children's full names will generally not be used alongside photographs.
- Consent arrangements will be followed.
- Published content will be reviewed before release.
- Appropriate privacy settings will be applied to school accounts.

Staff are expected to maintain professional standards online and:

- Must not communicate with pupils through personal social media accounts.
- Must not accept social media requests from current pupils.
- Should regularly review privacy settings.
- Should maintain professional boundaries online.
- Must avoid content that may bring the school into disrepute.

Images, Video and Live Streaming

Photographs and videos of pupils will only be used in accordance with school consent procedures and data protection requirements.

The school will:

- Store images securely.
- Use images appropriately.
- Ensure consent arrangements are followed.
- Remove content when required.
- Risk assess any live-streaming activities.

Parents and carers will be informed where appropriate.

Filtering and Monitoring

The Board of Trustees will ensure appropriate filtering and monitoring systems are in place and meet DfE standards.

The school will:

- Monitor the effectiveness of filtering systems regularly.
- Review filtering and monitoring arrangements annually.
- Ensure users are aware that systems may be monitored.
- Maintain clear escalation processes.
- Ensure safeguarding concerns identified through monitoring are referred immediately to the DSL.

Any attempt to bypass filtering systems will be treated seriously and investigated appropriately.

Illegal content identified through monitoring will be reported to relevant agencies, including where appropriate:

- Internet Watch Foundation (IWF).
- CEOP.
- Police.

Emerging Technologies

New technologies will be subject to review and risk assessment before implementation.

Consideration will include:

- Safeguarding implications.
- Data protection requirements.
- Educational value.
- Security risks.

- Accessibility and inclusion.

Reporting Online Safety Concerns

All online safety concerns must be reported immediately.

Examples include:

- Cyberbullying.
- Online grooming.
- Exposure to inappropriate content.
- Online sexual harassment.
- Sharing of nude or semi-nude images.
- Sextortion.
- Radicalisation concerns.
- Hate incidents.
- AI misuse.
- Data breaches.
- Online scams and fraud.
- Phishing attacks.
- Illegal content.
- Misuse of school systems.

Staff must:

1. Record the concern on CPOMS.
2. Inform the DSL where required.
3. Preserve evidence where appropriate.
4. Avoid investigating independently.
5. Follow safeguarding guidance.

Misuse of Technology

All users are expected to follow acceptable use expectations.

Breaches may result in:

- Restriction of technology access.
- Behaviour sanctions.
- Safeguarding referrals.
- Disciplinary procedures.
- Police involvement where appropriate.

Mobile Devices

Pupils are not permitted to use mobile phones during the school day unless agreed by the school for exceptional circumstances.

Any approved mobile phone:

- Must remain switched off.
- Must be handed to staff for secure storage.
- Is brought into school at the owner's risk.

Unauthorised mobile phone use may result in confiscation and sanctions in line with school procedures.

Incidents Outside School

Where online incidents occurring outside school impact pupils' wellbeing, relationships or safety within school, staff will respond appropriately in accordance with safeguarding and behaviour procedures.

Support may include:

- Safeguarding intervention.
- Parent meetings.
- Anti-bullying procedures.
- Referral to external agencies.
- Emotional wellbeing support.

Educational Visits and Outdoor Learning

Where mobile devices are carried by staff during visits, they will be used solely for professional and emergency purposes.

School equipment should always be used to capture images wherever possible.

Parental Engagement

The school recognises the importance of working in partnership with parents and carers.

The school will:

- Share online safety guidance.
- Promote online safety resources.
- Raise awareness of emerging risks.
- Provide regular communication through newsletters and school platforms.
- Encourage parents to report concerns and seek support.

Monitoring and Review

The effectiveness of this policy will be reviewed annually or sooner if significant changes occur in legislation, guidance or technology.

Filtering and monitoring arrangements will be reviewed regularly and safeguarding incidents analysed to identify trends, lessons learned and areas for improvement.

Online safety is everyone's responsibility. Ribbon Academy Trust is committed to creating a culture in which technology is used safely, responsibly and positively to support learning, wellbeing and safeguarding.