FOOTSTEPS TRUST CYBER SECURITY, FILTERING, MONITORING AND ONLINE SAFETY POLICY

1. Policy Statement

Footsteps Trust recognises that technology is essential to education, communication and safeguarding.

The Academy is committed to maintaining secure digital systems that:

- Protect children and young people from harm.
- Protect personal and sensitive information.
- Support teaching and learning.
- Reduce cyber security risks.
- Enable effective safeguarding and monitoring.
- Promote responsible and safe use of technology.

Cyber security forms part of the Academy's safeguarding responsibilities and contributes to the protection and wellbeing of students, staff and visitors.

2. Aims

This policy aims to:

- Protect Academy networks, systems and devices.
- Prevent unauthorised access to information.
- Support safeguarding through appropriate monitoring.
- Ensure effective filtering of harmful online content.
- Promote safe and responsible technology use.
- Reduce the risk of cyber-attacks.
- Support compliance with legal and regulatory requirements.
- Provide clear procedures for responding to cyber incidents.

3. Scope

This policy applies to:

- Students
- Staff
- Trustees and Governors

Date of Issue: September 2026
Date of Review: September 2027

- Volunteers
- Contractors
- Visitors using Academy systems

It covers:

- Academy-owned devices
- Cloud-based systems
- Email systems
- Internet access
- Mobile devices
- Remote access arrangements
- Third-party digital services

4. Roles and Responsibilities

Proprietor Board / Trustees

Will ensure:

- Appropriate cyber security arrangements are in place.
- Filtering and monitoring systems are effective.
- Risks are reviewed regularly.
- Sufficient resources are available for cyber security.

Principal

Will:

- Oversee implementation of this policy.
- Ensure cyber security forms part of safeguarding arrangements.
- Ensure significant incidents are managed appropriately.

Designated Safeguarding Lead (DSL)

Will:

- Work with IT providers to assess online safeguarding risks.
- Review filtering and monitoring concerns.
- Respond to safeguarding alerts generated by monitoring systems.
- Ensure online safety education is provided.

IT Provider / IT Lead

Will:

- Maintain security infrastructure.
- Implement technical controls.

- Monitor cyber security risks.
- Maintain patching and update schedules.
- Support incident response processes.

Staff

Staff must:

- Follow Academy cyber security procedures.
- Keep passwords secure.
- Report incidents promptly.
- Complete cyber security training.
- Use Academy systems responsibly.

Students

Students must:

- Follow the Acceptable Use Agreement.
- Use technology safely and responsibly.
- Report concerning online content.
- Respect Academy filtering arrangements.

5. Cyber Security Controls

The Academy maintains a layered cyber security approach that includes:

Firewalls

The Academy operates centrally managed firewall technology which:

- Monitors network traffic.
- Restricts unauthorised access.
- Detects suspicious activity.
- Supports filtering arrangements.
- Helps protect Academy systems from external threats.

Device Management

The Academy uses Microsoft Intune or equivalent management systems to:

- Enforce security policies.
- Apply encryption requirements.
- Deploy approved software.
- Restrict unauthorised applications.
- Secure Academy-owned devices.
- Support remote management and device recovery.

Endpoint Protection

All Academy devices will be protected through endpoint security software providing:

- Malware protection.
- Ransomware protection.
- Phishing detection.
- Threat monitoring.
- Security updates and vulnerability protection.

Multi-Factor Authentication

Where available, the Academy will implement Multi-Factor Authentication (MFA) for staff accounts and systems containing sensitive information.

Encryption

Sensitive data will be protected through appropriate encryption measures during storage and transmission.

6. Filtering and Monitoring

The Academy maintains filtering and monitoring systems which are:

- Appropriate to the age and needs of students.
- Proportionate to safeguarding risks.
- Reviewed regularly.
- Managed in partnership with safeguarding leads.

Filtering systems are designed to block access to content including:

- Pornographic material.
- Violent content.
- Extremist material.
- Gambling websites.
- Criminal activity.
- Harmful self-harm or suicide content.
- Illegal content.
- Other categories identified as safeguarding risks.

Monitoring systems may identify:

- Safeguarding concerns.
- Attempts to access blocked content.
- Cyberbullying concerns.
- Potential radicalisation indicators.
- Threats of violence.
- Self-harm indicators.

- Security risks.

7. Online Safety Education

Students are taught how to:

- Stay safe online.
- Manage digital footprints.
- Recognise scams and phishing.
- Report concerns.
- Protect personal information.
- Recognise misinformation and disinformation.
- Understand healthy online relationships.
- Recognise online exploitation risks.

Online safety education is delivered through:

- PSHE
- RSHE
- Assemblies
- Tutor sessions
- Safeguarding workshops

8. Safeguarding and Cyber Security

The Academy recognises that online safety is a safeguarding issue.

Cyber security arrangements support protection from risks including:

- Cyberbullying.
- Grooming.
- Radicalisation.
- Sexual exploitation.
- Criminal exploitation.
- Harmful online challenges.
- Fraud and financial exploitation.
- Identity theft.

Any safeguarding concerns generated through digital monitoring will be managed through the Academy's safeguarding procedures.

9. Data Protection

All processing of personal data will comply with:

- UK GDPR
- Data Protection Act 2018
- Academy Data Protection Policies

Personal data will:

- Be processed lawfully.
- Be stored securely.
- Be retained appropriately.
- Only be shared where lawful and necessary.

Monitoring activities will be proportionate and undertaken for legitimate safeguarding, security and operational purposes.

10. Cyber Incident Response

A cyber incident may include:

- Malware infections.
- Unauthorised access.
- Data breaches.
- Ransomware attacks.
- Account compromise.
- Significant system failures.

Staff must immediately report suspected cyber incidents to:

- The Principal
- DSL (where safeguarding risks exist)
- IT Support Provider

The Academy will:

- Assess risks.
- Contain incidents.
- Investigate causes.
- Take remedial action.
- Notify appropriate authorities where required.

11. Training and Awareness

All staff will receive regular training covering:

- Cyber security awareness.
- Phishing risks.
- Password security.
- Data protection.
- Online safeguarding.
- Reporting cyber incidents.

Training will be refreshed regularly to reflect emerging threats.

12. Monitoring and Review

The effectiveness of cyber security arrangements will be monitored through:

- Security audits.
- Incident reviews.
- Filtering and monitoring reviews.
- Safeguarding audits.
- Staff training records.
- IT provider reports.

The policy will be reviewed annually or sooner where:

- KCSIE is updated.
- Cyber threats change significantly.
- Significant incidents occur.
- Government guidance changes.

Date of Issue: September 2026
Date of Review: September 2027