Trust-wide cyber security policy

For: All Schools within the Rivermead Inclusive Trust.

Aligned with: DfE Cyber Security Standards, KCSIE, GDPR, and Microsoft Security Frameworks

1. Purpose and Scope

This policy outlines the technical and procedural controls in place to protect the confidentiality, integrity, and availability of digital systems and data across all schools in the Trust. It applies to all staff, pupils, contractors, and third-party users accessing Trust-managed systems.

2. Policy Foundations

This policy is grounded in:
- DfE's Cyber Security Standards for Schools and Colleges
- The statutory guidance in Keeping Children Safe in Education (KCSIE)
- GDPR and UK Data Protection Act 2018
- Microsoft Endpoint Security and Azure best practices

3. Core Security Principles

a. Device and Endpoint Protection

- All devices are enrolled in Microsoft Endpoint Manager (Intune) and protected by Defender for Endpoint.
- Devices must be encrypted, regularly patched, and centrally monitored.

b. User Access Control

- Azure Active Directory (AAD) governs user identity and access.
- Multi-Factor Authentication (MFA) is mandatory for all staff accounts.
- Role-based access control (RBAC) is enforced for administrative privileges.

c. Data Protection and Backup

- All data is stored in Microsoft 365 with automated daily backups.
- Sensitive data is classified and access is restricted.
- Data loss prevention (DLP) policies are applied to prevent unauthorised sharing.

d. Network and Cloud Security

- All schools operate behind firewalls with web filtering and threat detection.
- Microsoft Defender for Cloud Apps monitors cloud usage and anomalies.

4. Cyber Awareness and Training

- All staff must complete annual NCSC Cyber Security Training and GDPR certification.
- DSLs and senior leaders must complete advanced safeguarding and online safety training.
- Pupils receive age-appropriate online safety education as outlined in the Online Safety Policy.

5. Incident Response and Reporting

- All cyber incidents must be reported to the Trust I.T. Lead and logged in the central incident register.
- The Trust follows the DfE's guidance to report serious breaches and notifies the ICO where applicable.

6. Monitoring and Compliance

- Regular audits are conducted in collaboration with school leadership.
- Filtering and monitoring systems are reviewed termly.
- Policy compliance is reviewed annually and updated in line with DfE updates.