DATA SECURITY POLICY

Executive Head:	**Dan Nearney**
Chair of Management Committee:	**Ian Hawkins**
Date of Policy:	**February 2026**
Date of Review:	**February 2027**

Document Control/ Review Sheet

The information in the table below details earlier versions of this document with a brief description of each review and how to distinguish amendments made since the previous version date (if any).

Version Number	Version Description/ changes	Date of Revision
001	New policy created	19-02-26
002		

IT SUPPORT CONTACT DETAILS

- Primary contact name/role: James Brewster
- Telephone (support line): 01992 534841
- Email (support mailbox): helpdesk@riversesc.herts.sch.uk
- Out-of-hours/emergency contact (if available): 07541 001578

DATA SECURITY STATEMENT

Servers and Cloud

The school's servers run Windows Server 2019/2022 in a virtualised environment (Hyper-V or equivalent), with appropriate licensing and security hardening. Active Directory is managed securely and role-based access is enforced through groups. The school increasingly uses hybrid or cloud services (Microsoft 365, Google Workspace) for collaboration and storage, in line with DfE standards and GDPR requirements.

Email and Accounts

The school uses Microsoft 365 for staff and pupil email. Multi-factor authentication (MFA) is enabled for all staff and admin accounts. Legacy access protocols (POP/IMAP) are disabled. Anti-phishing and spam filtering controls are applied, and email traffic is encrypted in transit.

Passwords

Passwords follow NCSC guidance: they must be strong and unique. Staff are required to use long, memorable passphrases. Enforced expiry is not applied unless there is a suspected compromise. MFA provides an additional layer of security. Administrator accounts have unique credentials and are never shared.

Remote Access and Support

Remote access is provided via secure VPN, SSL gateway or equivalent, using encrypted connections and individual staff logins. Remote support tools are restricted to approved IT staff, with logs maintained for accountability.

Backups

The school operates both onsite (NAS) and cloud-based encrypted backups, with daily cycles. Backup data is tested regularly to ensure integrity and recoverability. Cloud backup providers comply with UK GDPR requirements.

Endpoint Security

All staff and pupil devices are protected by centrally managed endpoint protection (e.g. Microsoft Defender and ESET AV). Alerts are monitored by IT support. Firewalls and web filtering are applied to safeguard users and comply with DfE standards.

Device Management
Devices are managed through Microsoft Intune, Google Admin Console, or an equivalent Mobile Device Management (MDM) solution. Encryption (BitLocker, FileVault, ChromeOS encryption) is enabled on all mobile and portable devices. Lost or stolen devices can be remotely locked or wiped.

Updates and Patching
Operating systems, applications and security software are updated regularly. Critical patches are applied as soon as practicable and no later than one month after release, in line with NCSC guidance. As of October 2025, Microsoft will no longer provide security patches for Windows 10 without Extended Security Updates (ESU). The school will ensure all devices are migrated to supported versions of Windows or other platforms before that date.

Monitoring
Automated monitoring is in place to check server status, antivirus alerts, backup success, and disk health. Reports are reviewed by IT support to ensure issues are identified and resolved promptly.

Incident Escalation
Any security incidents or suspected data breaches are escalated immediately to the IT support provider. Confirmed or suspected data breaches are also reported to the school's Data Protection Officer in line with the Data Protection and Breach Response Policy.

Artificial Intelligence (AI)
Where the school or Trust uses artificial intelligence tools or platforms, these are managed in line with the separate AI Policy and the school's Data Protection Policy. Staff and pupils are reminded that no personal data, names or images should ever be entered into AI tools unless the system has been formally approved and privacy controls have been verified.

Review and Updates
This Data Security Statement is updated annually or when significant changes occur to the school's IT infrastructure. It provides governors with oversight of security measures in place. IT support providers may edit this template to reflect the specific solutions implemented at each school.