EASTBURY FARM PRIMARY SCHOOL

Data Security Statement

Spring 2026

Date of Governor Approval: 04.03.26

Data Security

Server setup

The school uses a physical server running Microsoft Server and several virtual servers running under Hyper-V. The physical server BIOS is password protected. Access to the server console is password protected with a password unique to the school.

Each individual virtual server is password protected using passwords unique to the school.

Virtual servers are part of a Microsoft domain and are kept up-to-date with Microsoft patches, keeping them at the highest current security level provided by Microsoft.

Virtual servers run the school's chosen antimalware solution.

Access to data on the server is controlled via NTFS permissions. These are applied in a way that allow access, based on the user's role. The default is to be more restrictive and allow access as authorised by school leadership.

Host OS: Windows Server 2019
Virtual OS: Windows Server 2016
Antimalware: McAfee

Hard disk health is constantly monitored and reported/flagged to the helpdesk allowing drive failures to be predicted and replaced in advance of failure.

The schools' shares are on Microsoft Cloud (SharePoint\OneDrive) and access to these shares are set by group permissions. All users have their own unique username and password.

Remote Server Management

The server uses a Dell iDRAC management portal for out of band management. Connection requires SSL and a school specific password is required for access.

Staff Passwords

Staff passwords are required to meet Microsoft password complexity standards. Passwords are not required to be changed periodically, in accordance with best practice guidance from GCHQ and Microsoft.

Onsite Backup

The school uses a Microsoft's Windows Server Backup technology. The destination is a NAS unit located on site in a different physical location from the server. The NAS unit is connected via an iSCSI connection authenticated through CHAP, using a school specific password. Access to the NAS unit management portal is through a school specific password.

Backups are reported to the help desk.

Offsite Backup

To augment the school's onsite backup, critical data is also backed using Microsoft Azure Remote Backup. Data is stored securely in Microsoft data centres in an encrypted format (AES, 256-bit). All communications between the backup agents and Microsoft cloud storage are via 256-bit SSL (Secure Socket Layer) channel using TLS (Transport Layer Security) v1.2.

Backups to the off-site location are automated. Manual tasks require a school specific password to access the console.

Backups are reported to the help desk.

School Email

The school uses Microsoft 365 for email. Accounts are provisioned manually, and passwords are subject to Microsoft complexity requirements. Passwords do not expire, in accordance with best practice guidance from GCHQ and Microsoft.

We scan the email system daily for a number of security indicators, including suspicious geographical logins, unauthorised protocol use, forwarding to external accounts and inactive accounts.

System Updates

The school uses WSUS to update their Windows workstation. This is carried out at termly intervals to ensure that Windows or other operating systems are current and up to date with the latest and appropriate vulnerability protection. At less frequent intervals, but at least annually, other devices such as port/switches will have firmware updates to enhance data security.