Guilsborough Academy
Guilsborough Multi Academy Trust

GUILSBOROUGH MULTI ACADEMY TRUST

CYBER SECURITY POLICY

Policy Name	Cyber Security Policy
Committee	Finance Audit and Risk
Owner	Chief Finance Officer
Statutory	N
Finance Audit and Risk to Ratify	

Date Ratified	Review Date
March 2023	March 2024

Contents

This Policy has been written with reference to the following guidance:

Schools Financial Value Statement
https://www.gov.uk/government/publications/schools-financial-value-standard-sfvs/2019-to-2020-checklist-guidance

Asset Fraud Guidance
https://www.actionfraud.police.uk/guide-to-reporting

ESFA Academy Trust Handbook part 6
https://www.gov.uk/guidance/academy-trust-handbook/part-6-the-regulator-and-intervention

ICO Requirements for Reporting Data Breaches
https://cy.ico.org.uk/for-organisations/guide-to-data-protection/guide-to-le-processing/personal-data-breaches/

ICT Advice on how data encryption should be used
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/encryption/

ICO Template for Data Protection Impact Assessment
https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/annex-d-dpia-template/

Account access standard technical requirements
https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/cyber-security-standards-for-schools-and-colleges#accounts-should-only-have-the-access-they-require-to-perform-their-role-and-should-be-authenticated-to-access-data-and-services
National Cyber Security Centre training for school staff
https://www.ncsc.gov.uk/information/cyber-security-training-schools

Infographics at the National Cyber Security Centre
https://www.ncsc.gov.uk/information/infographics-ncsc

School cyber security questions for governors
https://www.ncsc.gov.uk/information/school-governor-questions

1. Overview

The purpose of the cyber security policy adopted by Guilsborough Academy is to reduce the likelihood of cyber attacks occurring, and to minimise the impact to the school when incidents do occur.

2. Protection for all devices

Guilsborough Academy will:

- protect every school device with a correctly configured boundary, or software firewall, or a device that performs the same function
- change the default administrator password, or disable remote access on each firewall
- protect access to the firewall's administrative interface with multi-factor authentication (MFA), or a small, specified IP-allow list combined with a managed password, or prevent access from the internet entirely
- keep firewall firmware up to date
- check monitoring logs as they can be useful in detecting suspicious activity and will subscribe to CyberAlarm to keep the Police informed
- block inbound unauthenticated connections by default
- document reasons why particular inbound traffic has been permitted through the firewall
- review reasons why any particular inbound traffic has been permitted through the firewall, and change the rules when access is no longer needed
- If necessary, enable a software firewall for devices used on untrusted networks, like public wi-fi
- Ensure users who work from home have MFA enabled and are part of a secure VPN security group

3. Registration of Network devices

Guilsborough Academy will:

- keep a register, list, or diagram of all the network devices
- avoid leaving network devices in unlocked or unattended locations
- remove or disable unused user accounts, including guest and unused administrator accounts
- Remove company data from all devices enrolled to Intune for users that have left the organisation
- change default device passwords
- require authentication for users to access sensitive school data or network data
- remove or disable all unnecessary software according to the school's need
- disable any auto-run features that allow file execution
- set up filtering and monitoring services to work with the network's security features enabled
- immediately change passwords which have been compromised or suspected of compromise
- protect against a brute-force attack on all passwords by allowing no more than 10 guesses in 5 minutes, or locking devices after no more than 10 unsuccessful attempts

4. Controlling access to accounts and services

Users should have a separate account for school business, including internet access, if their main account:

- is an administrative account
- enables the execution of software that makes significant system or security changes
- can make changes to the operating system
- can create new accounts
- can change the privileges of existing accounts

Users must be authenticated with unique credentials before they access devices or services. This includes using passwords.

Password strength will be enforced at the system level.

For younger children or users with special educational needs:

- authentication methods other than passwords may be used
- a separate account accessed by the teacher rather than the student may be used
- the network is segmented so such accounts cannot reach sensitive data
- Consideration may be made if the data or service being accessed requires authentication

5. Use of Multi-Factor authentication

Multi-factor authentication will include at least 2 of the following:

- Complex or three-word password
- a managed device, that will belong to the school
- an application on a trusted device
- a device with a trusted network IP address. The school will not use this in MFA for accounts with administrator rights or for accessing sensitive data
- a physically separate token
- a known/trusted account, where a second party authenticates another's credentials
- a biometric test

6. Use of Malware software

The anti-malware software will :

- be set up to scan files upon access, when downloaded, opened, or accessed from a network folder
- scan web pages as they are accessed
- prevents access to potentially malicious websites, unless risk-assessed, authorised and documented against a specific business requirement

Applications will not be run nor data accessed which have been identified as malware. The anti-malware software will be used to eliminate the problem.

7. Security of all applications downloaded

The IT service provider will approve all code and applications that are deployed and make sure they do not pose a security risk. They should do this in the best way possible given available resources.

Best practice is to maintain a current list of approved applications. Applications with invalid or no digital signatures should not be installed or used.

The network's anti-malware service will scan all downloaded applications.

8. Licensing and update services

The IT service provider will ensure that all devices and software are licensed, supported and set up to meet the technical requirements.

Subscribing to services as Software as a Service (SaaS) rather than buying items will be default method.

So that appropriate risk assessment and mitigation can take place, the IT service provider will tell leadership and trustees at the school and alter the network accordingly when devices or software:

- have become unsupported
- are about to become unsupported

9. Backups and stores of information / data

The school will have at least 3 backup copies of important data, on at least 2 separate devices. At least 1 of these copies must be off-site and far enough away to avoid dangers from fire, flood, theft and similar risks.

The school will schedule backups regularly depending on:

- how often the data changes
- how difficult the information would be to replace if the backups failed

At least 1 of the backups must be offline at all times.

A cloud backup is an off-site backup. Cloud data held in separated cloud services are held in separate devices.

If the offline backup is in the cloud, access must be:

- by a secure account identity
- impossible from any device unless an authorised user has logged on in person

Off-site means in an alternative physical or digital location, offline means that is not connected to the network.

The number of devices with these access permissions must be kept to an absolute minimum.

A secure account identity is defined as a specified account secured with a username and multi-factor authentication.

A device which cannot access the backup is defined as a device that has no valid credentials.

Where the cloud services allow it, controls will be set up to:

- only allow authorised devices to create new or appended backups
- deny connection requests when backup is not in use

The school will regularly check that the backups work.

10. Business continuity plan and Disaster Recovery

The school will include a contingency plan for loss of some or all IT systems in their business continuity and disaster recovery plan. This is required by the schools financial value standard.

This plan must include:

- staff responsibilities
- out of hours contacts and procedures
- internal and external reporting and communications plans
- priorities for service restoration
- the minimum operational IT requirements
- where you can find additional help and resources

Hard copies of key information will be kept in case of total system failure.

Plans will be tested and reviewed regularly.

11. Reporting of Cyber Attacks

Guilsborough Academy will report cyber attacks to:

- Action Fraud
- DfE

Where applicable the school will report cyber attacks to ICO.

The school will act in accordance with:

- Action Fraud guidance for reporting fraud and cyber crime
- ESFA Academy Trust Handbook Part 6
- ICO requirements for reporting personal data breaches

12. Data Protection Impact Assessment by statute for personal data it holds as required by GDPR

The school will incorporate the risk assessment into the risk register.

The school uses encryption to protect data, which is:

- strong encryption
- using encryption systems that are still supported
- with a life appropriate to the sensitivity of the data being stored

The school follows the ICO advice on how data encryption should be used.

The school uses the ICO template for DPIA.

Additional protection and password protection meets the technical requirements in the account access standard.

Access is limited to those staff with a specific need. This is done by specific content area, and not blanket permissions.

By achieving all the cyber standards Guilsborough Academy strives to meet the additional requirements for:

- confidentiality
- integrity
- availability
- Restoration

13. Training for all staff in relation to cyber security

Staff who require access to the IT network will take basic cyber security training every year. The training will be part of the induction training for new staff

This training will focus on:

- phishing
- password security
- social engineering
- the use of approved online storage instead of removable storage media

The National Cyber Security Centre has published suitable training materials which Guilsborough Academy will use:

- cyber security training for school staff
- infographics at the NCSC
- Annual Certificate in Online Reputation for Staff | The National College

At least one current trustee will complete the same basic cyber security training. All governors will read the NCSC publication school cyber security questions for governors.

14. Additional mitigation measures are in place for cyber security

- Digital safeguarding and filtering tools are in place along with firewalls on servers.
- SSO authentication is achieved through Microsoft Azure

Data on old and decommissioned storage devices will be securely destroyed and the devices themselves disposed of in a secure and environment