HIGHDOWN SCHOOL AND SIXTH FORM CENTRE

CYBER SECURITY POLICY

Aspiration – Respect – Excellence

Monitoring, Evaluation and Review

Author	Mr M A Grantham [Head of School]	Review Period	2 years
Version	1	Status	Approved
Committee	Finances, Staffing and Premises Committee	Date Approved	November 2023
Link Governor	Mrs M Miller	Review Date	November 2025

HIGHDOWN SCHOOL AND SIXTH FORM CENTRE
CYBER SECURITY POLICY

This policy should be read in conjunction with the following policies:

- ICT and Internet Responsible Use Policy
- Personal Laptop Use Agreement
- BYoD Policy
- Data Protection/GDPR Policy
- Cyber-Attack Response Plan [Internal]

Introduction

This cyber security policy outlines our guidelines and provisions for preserving the security of our data and technology infrastructure.

The more we rely on technology to collect, store and manage information, the more vulnerable we become to severe security breaches. Human error, hacker attacks and system malfunctions could cause great damage and may jeopardise our academy's reputation or threaten our finances.

A cyber-attack is an attack launched from one or more computers against another computer or network of computers. It can maliciously deactivate computers, steal data, or use a compromised computer as a launch point to further aggravate the attack. The two aims of cyber-attacks are to either disable the system or gain illegal access to the target computer or network. There are different types of cyber-attacks based on their specific method and intention.

A cyberattack is a malicious and deliberate attempt by an individual or organisation to breach the information system of another individual or organisation. Usually the attacker seeks some type of benefit from disrupting the victim's network. The complexity and variety of cyberattacks is ever increasing. While cybersecurity prevention measures differ for each type of attack, good security practices and basic IT hygiene are generally good at mitigating these attacks.

The purpose of this policy is to outline measures taken to prevent and/or minimise the impact of cyber-attacks, and to highlight what is regarded as basic principles of good cyber security, e.g. based on guidance from National Cyber Security Centre (NCSC)[1].

Roles and responsibilities

This policy applies to all our staff, governors, students, contractors, volunteers and anyone who has permanent or temporary access to our systems and hardware.

[1] https://www.ncsc.gov.uk/files/NCSC_NEN%20cards_PRINT-2.pdf

The named ICT and e-safety co-ordinators in our academy are:

- Ms R E Cave (Executive Headteacher)
- Mr M A Grantham (Head of School)
- Dr S Capaldi (Associate Deputy Headteacher and Designated Safeguarding Lead)
- Mrs L Holt (School Business Manager and Data Protection Officer)
- Mr K Crosby (Network Manager)
- Mr D Stephenson (Curriculum Leader for Computing and ICT)
- Mrs P Larbey (TLR ICT Across the Curriculum)
- Miss A Morten (Data Manager)

All stakeholders are expected to adhere to this policy and guidance to maintain cyber security.

Common threats and risks

- **Phishing:** a technique used to deceive a target into taking harmful action such as downloading malware disguised as an important document or contain a link that goes to a website designed to look like a familiar website and trick the user into entering their credentials. An attack could be used to gain access to a user's account that has important information or a user with administrative privileges to the network. Phishing is usually in the form of an email sent to either a list of users or targeted at a single user
- **Malware:** malicious software that includes viruses, Trojans, worms or any code or content that could have an adverse impact on organisations or individuals
- **Ransomware:** a kind of malware that locks victims out of their data or systems and only allows access once money is paid
- **Password attack:** an attempt to gain access to systems by cracking the user's password
- **Brute force:** an attempt to gain access to systems by trying different passwords to eventually guess the correct one
- **Denial of service (DDoS):** sending so much traffic to a computer or network such that its resources are overwhelmed and are made unavailable to everyone. This will result from a successful malware attack

The following are all potential consequences of cyber-crime which could affect individuals and/or our Academy:

- Cost
- confidentiality and data protection
- potential for regulatory breach
- reputational damage
- business interruption
- structural and financial instability

Management of risks

We implement a wide range of actions to minimise the risks of deliberate or accidental cyber-crime. These controls are proportionate, multi-layered, up-to-date and regularly reviewed.

- Internet security and filtering blocks access to malicious, hacked, and inappropriate websites. Internet filtering is the first line of defence against web-based attacks. Malicious or hacked websites are a primary source of initiating attacks, triggering download of malware, spyware or risky content
- Firewall services protects against malware, exploits and malicious websites in both encrypted and non-encrypted traffic
- Antivirus software protects against malware and ransomware
- Frequent installation of security patches
- USB storage devices are not permitted. Staff and students are encouraged to use OneDrive to share data between devices
- Laptop devices must be password protected and/or include a passcode
- Microsoft is used for emails and is encrypted and includes authentication filters, e.g. to filter spam
- Routine server backups run
- Disposal of redundant ICT equipment using an authorised agency (R3)
- All staff complete training from National Cyber Security Centre (NCSC) regarding cyber security and identification of suspicious emails, e.g. poor quality images, grammatical errors, impersonalised salutation, request for urgent action, etc.
- 'Powerful Password' protocols are in place for all stakeholders
- Separate wifi network outside of core network for external device connection
- Sensitive data is transferred via secure and encrypted means
- IT infrastructure, e.g. routers, switches, wireless access points, etc., are only handled by authorised personnel
- Regular forced password reset protocols in place
- Remote Apps security: limited user permissions only
- System penetration tests conducted by an external agency
- Routine deletion/disabling of unused/unnecessary user accounts
- Cyber-attack response plan: includes 4 main stages – (1) containment and recovery, (2) assessment of ongoing risk, (3) Notification, and (4) evaluation and response

Monitoring, evaluation and review

It is the responsibility of the Governing Body to facilitate the review of this policy on a regular basis, and at least every 2 years or if new technologies are introduced.

The Network Manager and Senior Leader with responsibility for Whole School ICT will continue to review the effectiveness of this policy.