Hook Infant School

Cyber Security Policy

Introduction

A cybersecurity incident can have a major impact on any organisation for extended periods of time. For a school, this can range from minor reputational damage and the cost of restoring systems from existing backups, to major incidents such as losing student work or access to learning platforms and safeguarding systems, which could lead to data-protection fines or even failing an inspection.

This Cybersecurity Policy outlines Hook Infant School's guidelines and security provisions which are there to protect our systems, services and data in the event of a cyberattack.

Scope of Policy

This policy applies to all staff, contractors, volunteers and anyone else granted permanent or temporary access to the school's systems and hardware. It also covers the physical and technical elements that are used to deliver IT services for the school.

Risk Management

Hook Infant School will include data and cyber security risks on the "**Data & IT Incident Log**" and will record major system changes and internal cyber security testing in the "**Data & IT Security Change Log**". The Network Manager/DPO will report on the progress and management of these logs to Governors three times a year via the "**Data and IT Security Report to Full Governing Body**". The Network Manager/DPO will also meet with the designated Governor(s) for Data Protection and Filtering and Monitoring prior to the first Full Governing Body meeting of each term to discuss the logs in detail, and at other times as necessary.

Physical Security

Hook Infant School will ensure there is appropriate physical security and environmental controls protecting access to its IT Systems, including but not limited to air conditioning, lockable cabinets, and secure server/communications rooms. The school buildings are protected by an intruder and door entry system.

Asset Management

To ensure that security controls to protect the data and systems are applied effectively, Hook Infant School will maintain asset registers for, files/systems that hold confidential data, and all physical devices (servers, switches, desktops, laptops etc) that make up its IT services.

User Accounts

Users are responsible for the security of their own accounts. If at any time they believe their credentials may have been compromised, for example after a phishing scam, they must change their password and inform the Network Manager immediately! Personal accounts should not be used for work purposes. Hook Infant School will implement multi-factor authentication where it is practicable to do so.

Devices

To ensure the security of all the school's devices, infrastructure and data, users are required to:

- Lock devices that are left unattended (using the 'Windows key' and 'L' or clicking on start/account name/lock)

- Allow system or ESET antivirus updates to install when prompted
- Report lost or stolen equipment as soon as possible to the Network Manager
- Change **all** account passwords at once when a device is lost or stolen (and report immediately to the Network Manager
- Report a suspected threat or security weakness in the school's systems to the Network Manager

Devices will be configured with the following security controls as a minimum:

- Password protection
- Windows firewall on client machines and Fortigate next generation firewall across the network
- ESET Anti-virus / malware software
- Automatic security updates
- Removal of unrequired and unsupported software through Group Policy
- Autorun disabled
- Minimal administrative accounts

Data Security

Hook Infant School will take appropriate measures to reduce the likelihood of the loss of availability to, or the disclosure of, confidential data.

Hook Infant School defines confidential data as:

- Personally identifiable information as defined by the ICO
- Special Category personal data as defined by the ICO
- Unpublished financial information
- CCTV and other closed monitoring systems

Critical data and systems will be backed up on a regular basis following the 3-2-1 backup methodology

- 3 versions of data
- 2 different types of media
- 1 copy offsite backup

To meet this methodology, our backups are:

- Full data back up to the onsite RMB device every day at 17:00hrs
- Offsite backup sent to Agile Vault overnight
- Three shadow copies saved per day at 07:00hrs, 12:00hrs and 19:00hrs

Opening, Sending and Receiving Confidential Data

Hook Infant School recognises the security risks associated with opening, sending and receiving confidential data.

To minimise the chances of a date breach users are required to:

- Always use specific Hook Infant School accounts when engaged in school business
- Consider if an email could be a phishing email or that a colleague's or official looking account could be 'hacked' or faked. If something does not feel right check with the sender by another method, particularly in relation to financial transactions, attachments, or links to websites
- Wherever possible, keeping Hook Infant School's files on school systems: remote access, 365 email/Onedrive, etc
- Not sending school files to personal accounts
- Verifying the recipient of data prior to sending
- Always mark emails containing personal or sensitive data with "***CONFIDENTIAL***" to flag up the potential risk of opening the email in front of others.

- Never open confidential or sensitive emails, accounts or other data sources with the classroom touch panels switched on
- Using file encryption where possible, sending passwords/keys via alternative communication channels
- Alerting the Network Manager/DPO to any breaches, malicious activity or suspected scams immediately

Training

Hook Infant School recognises that it is not possible to maintain a high level of Cybersecurity without appropriate staff training. It will integrate regular Cybersecurity training into Inset days, provide more specialist training to staff responsible for maintaining IT systems and promote a "No Blame" culture towards individuals who may fall victim to sophisticated scams. All staff are responsible for following school policies and procedures and engaging in the training provided.

System Security

Agile ICT and their partners will build security principles into the design of IT services for Hook Infant School. The School Leadership Team will ensure that the school has appropriate plans in place to maintain acceptable cyber security provision.

- Security patching – network hardware, operating systems and software
- Pro-actively plan for the replacement of network hardware, operating systems and software before vendors stop providing security support for them
- Actively manage anti-virus systems
- Actively manage and test backups
- Regularly review and update security controls that are available with existing systems
- Review the security risk of new systems or projects

Major Incident Response Plan

Hook Infant School will develop, maintain, and regularly review a Cybersecurity Major Incident Response Plan. This will include identifying or carrying out:

- Key decision-makers
- Key system impact assessments and restoration priorities (i.e. which backups needs to be restored first for the school to become operational again)
- Emergency plans for the school to function without access to systems or data
- Alternative methods of communication, including copies of contact details
- Emergency budgets and who can access them / how
- Key agencies for support (e.g. IT support company)

Maintaining Security

Hook Infant School understands that the financial cost of recovering from a major cybersecurity Incident can far outweigh the ongoing investment in maintaining secure IT systems. Hook Infant School will budget appropriately to keep cyber related risk to a minimum.

Approved by the Governing Body, Hook Infant School

Reviewed: January 2024

Signed *Alison Collier*
Chairman of Governing Body

Date for next review: January 2025

Appendix 1

Filtering and Monitoring Guide for Staff and Governors

Learn about our school's filtering and monitoring systems and how you can help to keep pupils safe online. Know what to do if you have concerns about the content that pupils are accessing.

What is filtering and monitoring?

Filtering systems:

- Block access to harmful websites and content

Monitoring systems:

- Identify when someone searches for or accesses certain types of harmful online content on school devices
- Identify who is searching for or accessing the harmful content
- Alerts the school about it so we can intervene and respond
- **Don't** block access to harmful content

We are all responsible for filtering and monitoring

No filtering and monitoring software is perfect:

- It might not be aware of all the websites that contain inappropriate content
- Abbreviations or misspellings in a search engine may slip past the software
- Inappropriate content may be found on websites considered 'safe'

You can help to make sure the internet is used appropriately by:

- Monitoring what pupils are accessing on devices during school hours (e.g. by looking at their screens when using computers during lessons)
- Alerting the Network Manager if you become aware that content is not being filtered properly

If you have concerns about what a pupil is accessing online, always raise it with the Safeguarding team.

Inappropriate content includes:

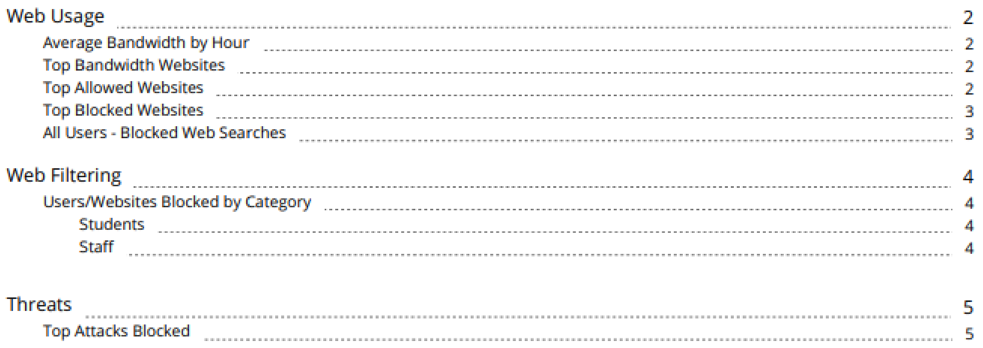
- Illegal content (e.g. child sexual abuse)
- Discriminatory content (e.g. sexist, racist or homophobic content)
- Sites that promote drugs or substance abuse
- Extremist content (e.g. the promotion of terrorism)
- Gambling sites
- Malware and/or hacking software
- Pornography
- Pirated material (copyright theft)
- Sites that promote self-harm, suicide and/or eating disorders
- Violent material

What systems do we use?

Keeping Children Safe in Education 2023 states that all schools should have appropriate filtering and monitoring systems in place.

We use the following systems and processes for filtering and monitoring purposes:

- The schools access to the internet is via AgileInternet
- We use the FortiGate Unified Threat Management (UTM) firewall to police incoming and outgoing internet traffic
- We are subscribed to the global Fortiguard service which is constantly updated with new threats as they are identified
- Agile ICT are the school's IT support provider and they manage and monitor the Fortigate/ Fortiguard setup and maintenance
- The Network Manager receives a weekly automated report on internet use by staff, visitors and pupils, including web use, blocked websites, and any cyber security threats (see screenshot below)



Web Usage 2
Average Bandwidth by Hour 2
Top Bandwidth Websites 2
Top Allowed Websites 2
Top Blocked Websites 3
All Users - Blocked Web Searches 3

Web Filtering 4
Users/Websites Blocked by Category 4
Students 4
Staff 4

Threats 5
Top Attacks Blocked 5

How to raise questions or concerns

Our filtering and monitoring system is designed to protect staff and pupils online. It shouldn't have an impact on teaching and learning or school administration.

Contact the Network Manager, Pete West, if you or pupils:

- Cannot access content that you need to carry out your work
- Have access to content that should be blocked

If you become aware of pupils accessing concerning content at any time, report this to the Safeguarding Team as soon as possible.

Sources

- Keeping Children Safe in Education, GOV.UK – Department for Education
  https://www.gov.uk/government/publications/keeping-children-safe-in-education--2
- Filtering and monitoring standards for schools and colleges, GOV.UK – Department for Education
  https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-standards-for-schools-and-colleges
- Appropriate filtering, UK Safer Internet Centre
  https://saferinternet.org.uk/guide-and-resource/teachers-and-school-staff/appropriate-filtering-and-monitoring/appropriate-filtering
- Appropriate monitoring, UK Safer Internet Centre
  https://saferinternet.org.uk/guide-and-resource/teachers-and-school-staff/appropriate-filtering-and-monitoring/appropriate-monitoring