AEM Sutherland House School | Braithwell

Cyber Security Policy

Document Control

Title: SHS Cyber Security Policy

Applicable to: All school staff

Date Reviewed: May 2026

Policy Owner: H&S/ LC

1. Aim

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

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 school's reputation or threaten our finances.

For this reason, we have implemented a number of security measures. We have also prepared instructions that may help mitigate security risks. We have outlined both provisions in this policy.

2. Scope

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

- This also applies to all information gathered about all pupils and this is supported by GDPR procedures.
- To provide a clear and auditable process
- Confidential data is private and valuable, we must ensure that all staff are obliged to protect this data, we will give our staff instructions on how to avoid security breaches. Common examples include but not limited to:
    1. Data of pupils/parents/carers/staff
    2. Financial data
    3. Personal information

3. Roles and Responsibilities

As managing ICT and e-safety are important aspects of strategic leadership within the school. The Headteacher and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored at regular intervals.

The named ICT and e-safety coordinators in this school are:

- Gillian Fotheringham (Head Teacher)

4. Threats to our security

A threat if left unchecked, could disrupt the day-to-day operations of Sutherland House School Braithwell and AEM as a whole, the delivery of education and ultimately has the potential to compromise local and national security.

Types of Threats

- Cybercriminals and cybercrime – are generally working for financial gain. Most commonly, for the purposes of fraud, by either selling illegally obtained information to a third party and/or using directly for criminal intentions. The key tools and modus operandi of cybercriminals includes:

    - Phishing – emails purporting to originate from a public agency to extract sensitive and personal information from members of the public.

    - Ransomware – a type of malware that locks victims out of their data or systems and may only allow access once again when money is paid.

    - Malware – malicious software that includes viruses, trojans, worms or any code or content that could have an adverse impact on AEM as a whole or on a particular individual.

- Hacking – Hackers will generally take over public websites or social media accounts to raise the profile of a particular cause. When targets are against local government or school websites and networks these attacks can cause reputational damage locally and nationally. If online services are regularly disrupted by cyber-attacks this could lead to the loss of public confidence. Hacker groups have successfully used distributed denial of service (DDoS – when a system, service or network is burdened to such an extent by an electronic attack that it becomes unavailable) attacks to disrupt the websites of a number of councils already in the UK.

- Insiders – Staff may intentionally or unintentionally release sensitive information or data into the public domain. This may be for the purpose of sabotage or to sell to another party, but more often than not is due to simple human error or a lack of awareness about the particular risks involved.

- Zero-day threats – A zero-day exploit is a cyber-attack that occurs on the same day a weakness is discovered in software. At this point, it's exploited before a fix becomes available from its creator. This is an attack that exploits a previously unknown security vulnerability. This poses a risk to any computer or system that has not had the relevant patch applied or updated its antivirus software.

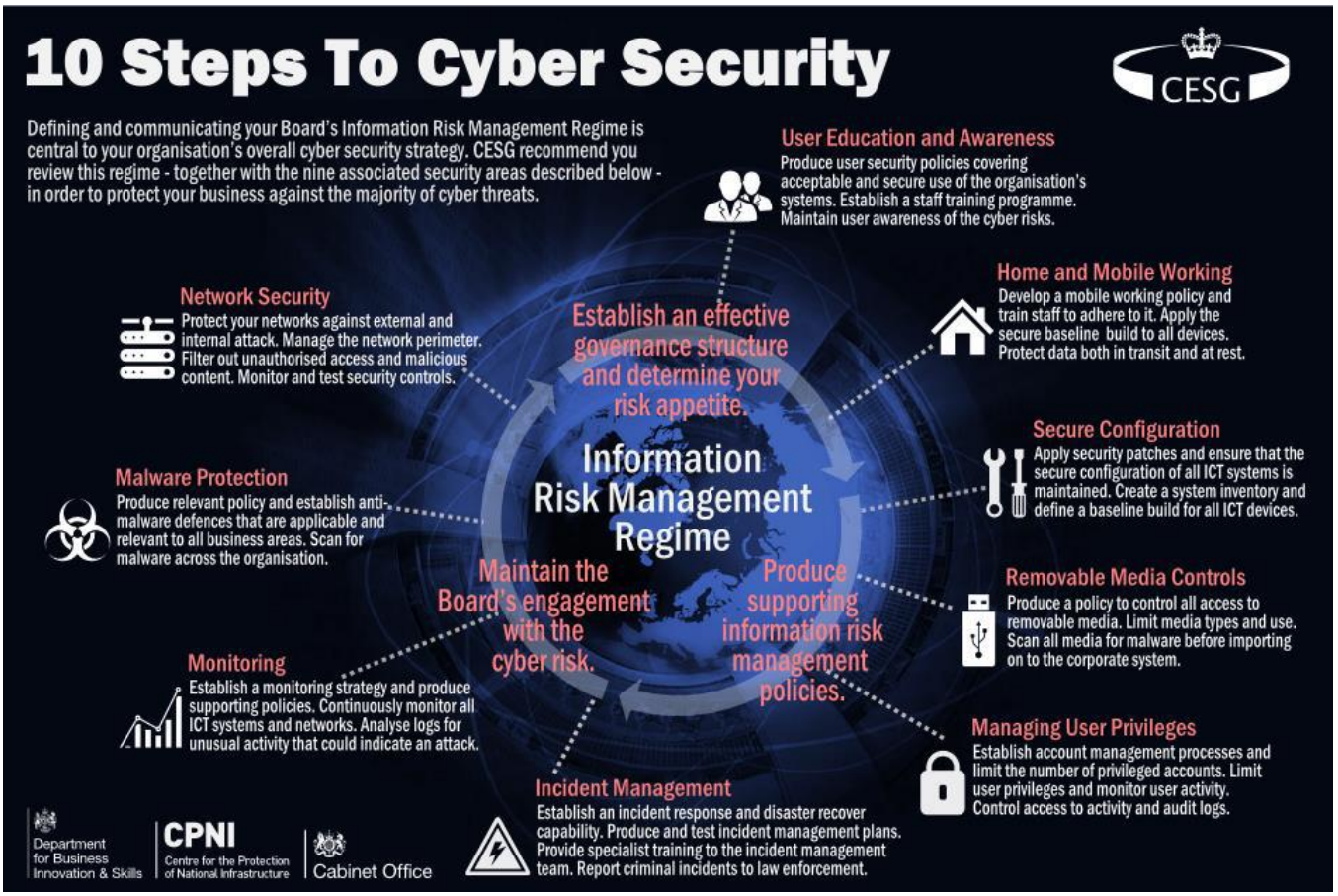
- Physical threats – The increasing reliance on digital services brings with it an increased vulnerability in the event of a fire, flood, power cut or other disaster, natural or otherwise, that could impact upon our IT systems.

- Espionage – Several of the most sophisticated and hostile foreign intelligence agencies target UK government and public sector networks to steal sensitive information. This could ultimately disadvantage the UK in diplomatic or trade negotiations, or in a military way.

- Terrorists – Some terrorist groups demonstrate intent to conduct cyber-attacks, but fortunately have limited technical capability. Terrorist groups could obtain improved capability in a number of ways, chiefly through the sharing of expertise in online forums providing a significant opportunity for terrorists to escalate their capability.

5. Steps to Cyber Security

At AEM and Sutherland House School Braithwell, we aim to implement the National Cyber Security Centre's advice for keeping our data secure:



Data and information used:

- Pupil and staff information in our management information systems (iPlanit, Cascade, Arbor, Myconcerns, Evolve and shared internal drive)
- Child protection information (MyConcerns, iPlanit)
- Communication – emails, School mobile phones and messages through TEAMS
- Curriculum and Teaching materials
- Records of information (meetings, presentations and so forth)

Protection of Personal and School Devices:

Staff must only use school-issued devices to access school emails, accounts and/or folders. When/If staff use personal digital devices to access school emails or accounts, they introduce a security risk to our data. We advise our staff to keep both their personal and school-issued computer, tablet and mobile phone secure. They can do this if they:

- Keep all devices password protected (in the case of school laptops these have a 12-digit password that requires updating regularly)
- Ensure that the school's installed antivirus software is installed on their school issued laptop and that they have antivirus software installed on home computers/devices
- Ensure they do not leave their devices exposed or unattended (locked when not in attendance with their laptop)
- Ensure that school-wide security updates of browsers and systems have taken place.
- Log on to school accounts and systems through secure and private networks only.

We also advise our staff to avoid accessing internal systems and accounts from other people's devices or lending their own devices to others.

When new staff receive school-issued equipment they will receive instructions for: Password management set-up, and to update their password at predefined time intervals.

Antivirus and anti-malware software is installed on all school-owned laptops/devices, and we advise all staff to have antivirus software installed on their own devices.

Staff must follow instructions to protect their devices and refer to our IT Provider (Addooco, 0333 8806088, helpdesk@addooco.it) if they have any questions.

Keep emails safe:

Emails often can host scams and malicious software (trojans, worms, viruses), to avoid virus infection or data theft of from our systems, we instruct staff to:

- Avoid opening attachments and clicking on links when the content has not been adequately explained (for example, “watch this video, it’s incredible”)
- Have suspicion of clickbait titles (for example, offering free items, prizes, money)
- Check email and names of people they received a message from to ensure they are legitimate.
- Look for inconsistencies or give-aways (for example, grammar mistakes, capital letters, excessive use of exclamation marks)
- If a member of staff isn’t sure that an email, they received is safe they can refer to LMG.

Manage passwords responsibly and effectively:

Password leaks are dangerous since they can compromise our entire infrastructure. Not only should passwords be secure thus making them harder to hack, but they should also remain secret and confidential. For this reason, we advise our staff to do the following:

- Choose passwords with at least 12 characters (an AEM system set-up) (including any three from the following options: capital and lower-case letters, numbers and symbols) and to avoid information that can be easily guessed (for example, birthdays, addresses). General guidance on creating a password is to take three random words and to add a number and a special character (Such as, TrinityRainbowEarth143!%)
- Remember passwords instead of writing them down. If staff need to write their passwords, please keep passwords and identifiers separate or, at the very least, secure.
- Exchange credentials only when absolutely necessary. When exchanging them in-person isn’t possible, staff should prefer the phone instead of email, and only if they personally recognize the person they are talking to.
- Whilst some providers and organizations with whom we work advise and expect passwords to be changed regularly, the AEM protocol is for passwords to be updated every six-weeks and our IT systems enforce this change on all employees.

Transfer Data Securely:

Transferring data introduces a potential serious security risk, with this in mind, staff must:

- Avoid transferring sensitive data (staff and pupil information and/or records) to other devices or accounts unless absolutely necessary. Should any form of mass transfer be required then the permission of the Headteacher must be sought before proceeding with the activity.
- Share confidential data over the school network/system and not over public Wi- Fi or private connection.
- Ensure that the recipients of the data are properly authorised people or organisations and have adequate security policies.
- Ensure that data is sent to the correct email addresses/contacts and take particular precautions/care when sending mass emails.
- Our IT support, Addooco need to know about scams, breaches and malware so they can better effectively protect our infrastructure. For this reason, we require our staff to report perceived attacks, suspicious emails or phishing attempts as soon as possible to Addooco. Addooco should then investigate promptly.
- Our IT support, Addooco are responsible for advising staff on how to detect scam emails. We encourage our staff to contact them and ask any questions should they have any concerns relating to this.

Additional measures:

To reduce the likelihood of security breaches when leaving your desk/workstation, we also instruct staff to:

- Either turn off screens or lock devices when not working on them
- Report stolen or damaged equipment as soon as possible to their line manager and/or Addooco depending on the nature of the damage or theft.
- Change all account passwords immediately should a device be stolen.
- Report a perceived threat or possible security risk/weakness in school systems.
- Refrain from downloading suspicious, unauthorised or illegal software onto school equipment.
- Avoid accessing suspicious websites.

We also expect staff to comply with our social media and acceptable use of ICT. Our

Security specialists/Network administrators (Addooco) will:

- Install firewalls, antivirus, anti-malware software and access authentication

systems.

- Arrange for security training for all staff where necessary.
- Inform staff regularly about new scam emails or viruses and ways to combat them.
- Investigate security breaches thoroughly and promptly.
- Follow the provisions set out in this policy.
- Our school will have all physical and digital shields to protect information.

When working remotely:

Anyone working remotely for whatever reason, must follow this policy's instructions too. When staff are accessing our school's systems from a distance, they are obliged to follow all data encryption, protection standards and settings, and also ensure their private network(s) are secure.

At all times should staff be ensure please encourage them to contact LMG for all support in IT matters.

6. Reporting Incidents

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must immediately be reported to the Headteacher. Additionally, all security breaches, lost and/or stolen equipment or data, virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other non- compliance with this policy must be reported to both the Headteacher and the Designated safeguarding lead.

Disciplinary action:

We expect all our staff to always follow this policy and those who cause security breaches may face disciplinary action:

- First-time, unintentional, small-scale security breach: we may issue a verbal or written warning and provide further training to the staff on security.
- Intentional, repeated or large-scale breach(es)(which cause severe financial or other damage): we will invoke more severe disciplinary action up to and including termination of employment after investigation
- We will investigate each incident on a case-by-case basis

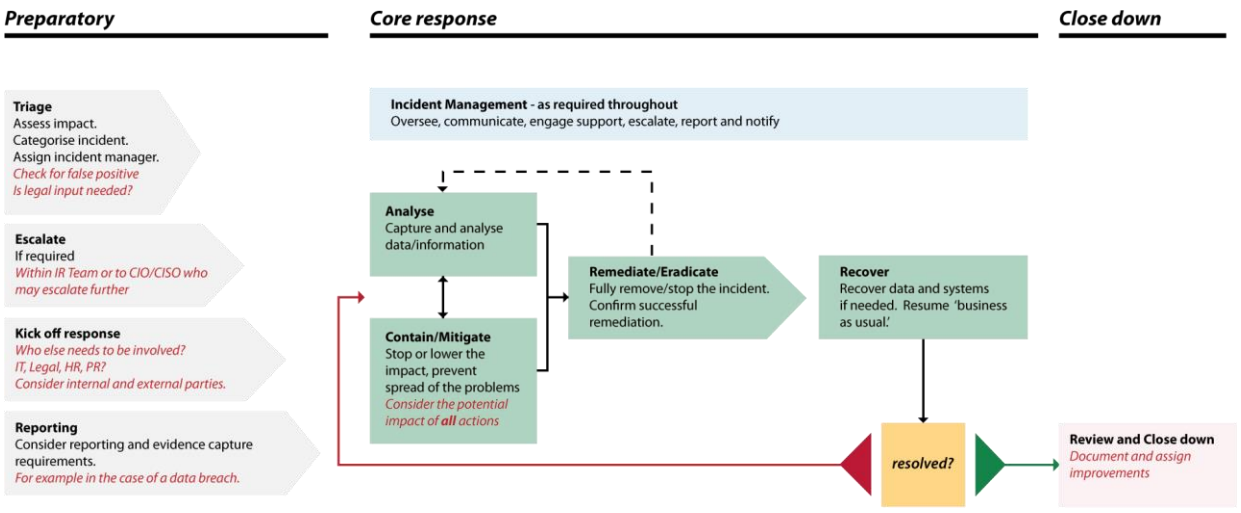
Additionally, staff who are observed to disregard our security instructions will face progressive disciplinary action, even if their behaviour hasn't resulted in a security breach.

Take Security Seriously:

Everyone who works for AEM or who is a pupil should feel that their data is safe. The only way to gain their trust is to proactively protect our systems and databases. We all can and should contribute to this by being vigilant and keeping cyber security at the forefront of our minds when we carry out our roles for AEM.

7. Cyber Security Incident Management Plan

Below is an outline guide of how to successfully manage a security breach:



8. Further Information and References

National Cyber Security Centre https://report.ncsc.gov.uk Action

Fraud http://www.actionfraud.police.uk

Department for Education Safeguarding devices - GOV.UK (www.gov.uk)