East Midlands Education Trust

Cyber Security Policy

Spring 2024

Review Date:	Spring 2024	Reviewed & adopted by:	Trustees
Next Review Due:	Spring 2026	Updated by:	ICT Director
Mid-Reviews *(statutory):*			
Document No:	POL-SCH-012	The information contained on this document is considered proprietary to East Midlands Education Trust in that these items and processes were developed at private expense. This information shall not be released, disclosed, or duplicated.	

Contents

1. Policy brief & purpose

1.1 This EMET policy outlines the guidelines and provisions for preserving the data and technology infrastructure.

1.2 The more the Trust relies on technology to collect, store and manage information, the more vulnerable we become, to severe security breaches. Human errors, hacker attacks and system malfunctions could cause great financial damage and may jeopardise the Trust's reputation. For this reason, it is necessary to implement a number of security measures and instructions that may help mitigate security risks. Both provisions are outlined in this policy and employees should also refer to other relevant Trust Policies such as:

- Data Protection (POL-OPS-002)
- Online Safety (POL-SCH-006)

2. Scope

2.1 This policy applies to all our employees, contractors, volunteers and anyone who has permanent or temporary access to the Trust's systems and hardware.

3. Policy elements

3.1 Confidential data

Confidential data is secret and valuable. Common examples are:

- Information concerning staff, students, parents, governors and partners.
- Unpublished financial information and contractual data.

All employees are obliged to protect this data in accordance with GDPR regulation. In this policy, employees are given instructions on how to avoid security breaches.

3.2 Protect personal and company devices.

When employees use their digital devices to access Trust emails or accounts, they introduce a security risk to our data. Employees are strongly advised to keep both their personal and Trust-issued devices secure. They can do this provided that:

- All devices are password protected.
- School IT support ensure all devices are encrypted where possible and recovery keys stored securely.
- In addition to being encrypted, school IT support should ensure ALL staff devices have a start-up PIN enabled (on compatible devices) to further protect against unauthorised access whilst the device is off-site.
    - Unsupported devices should not be used by staff.
- Antivirus software is kept up to date.
- Devices are not left unexposed or unattended.
    - Devices should be locked away and out of site when not in use.

- Security updates of browsers and systems are installed monthly or as soon as updates are available.
- Company accounts and systems are logged into through secure and private networks only.

Employees should avoid accessing internal systems and accounts from other people's devices or lending their own devices to others.

When new staff receive Trust-issued equipment they should review the Trust's Online Safety policy, as it will contain key information relating to the safe and secure use of this equipment. New staff are required to sign an AUP (Acceptable Use Policy) when issued with Trust equipment.

3.3 Email security

Emails often host phishing attacks, scams or malicious software (e.g., trojans and worms.) To avoid virus infection or data theft, employees are instructed to ensure that:

- Chosen email application or browser for accessing emails is kept up to date and latest security fixes applied.
- Opening attachments and clicking on links is avoided when the content is not adequately explained e.g. "watch this video, it's amazing".
- Clickbait titles (e.g., offering prizes, advice) are treated as suspicious.
- The names of people messages are received are checked to ensure they are legitimate.
- Inconsistencies or giveaways e.g. grammar mistakes, capital letters, excessive number of exclamation marks are observed.
- The sender and subject of an email are recognisable.

If an employee isn't sure that an email is safe, they should contact the school IT support. It is strongly recommended that ALL incoming/outgoing emails are scanned for malicious content by a third-party solution prior to entering school systems. Advice on this is available on request from our EMET IT team.

3.4 Password management.

Password leaks are dangerous, since they can compromise the entire infrastructure. Not only should passwords be secure to avoid being easily hacked, but they should also remain secret. For this reason, employees are instructed to:

- Choose passwords with at least 12 characters (including capital and lower-case letters, numbers and symbols) and avoid information that can be easily guessed e.g. birthdays.
    - The Trust recommends using the 'three random words' method when setting a password.
- Remember passwords and DO NOT write them down.
    - The only exception is when issuing a temporary password to a new user for example.

- Password manager apps or browsers are recommended as a way of storing strong passwords for multiple services rather than re-using the same password over and over.
    - MS Edge for example has a built-in password manager which is linked to your O365 account.
    - Only recommended in conjunction with 2FA.
- Never share credentials under any circumstances! Should IT support need to access an account then they can, provided they have the permission to do so.

IT Managers MUST ensure multi-functional authentication or conditional access rules are used for ALL accounts, and passwords must comply with complexity requirements which include not matching against an online database of known common passwords that attackers could use.

Further information regarding password security can be found in the Online Safety policy and also on the National Cyber Security Centre website below.

Top tips for staying secure online - NCSC.GOV.UK

3.5 Transfer data securely

Transferring data introduces security risks. Employees must:

- Avoid transferring sensitive data e.g. customer information, employee records, to other devices or accounts unless absolutely necessary. When mass transfer of such data is needed, employees are requested to seek the support of the school IT support.
- Share confidential data over the company network/ system and not over public Wi-Fi or private connection.
- Avoid the use of USB/external drives. If such drives are used, they must be encrypted and issued by the IT support team.
    - School IT Support should ensure that 'on-access' scanning is enabled via the anti-virus solution installed.
    - School IT Support should ensure 'auto-play' is disabled on ALL devices.
- Ensure that recipients of data are properly authorised people or organisations and have adequate security policies.
- Ensure Confidential data is NOT downloaded and saved to a user's personal device.
- Report scams, privacy breaches and hacking attempts.

School IT support need to know about scams, breaches and malware so they can better protect the infrastructure. For this reason, employees MUST report perceived attacks, suspicious emails or phishing attempts as soon as possible to our specialists. The school IT support will investigate promptly, resolve the issue and send a Trust-wide alert when necessary.

3.6 Additional measures

To reduce the likelihood of security breaches, employees are instructed to:

- Lock their devices when leaving desks and place them out of sight.
    - School IT Support should enforce this with inactivity limits set appropriately.
- Report stolen or damaged equipment as soon as possible to the IT support.
- Change all account passwords at once when a device is stolen.
    - Devices should be wiped remotely where possible by School IT Support. A built-in feature of O365 named MS Endpoint Manager for example has this function.
- Report a perceived threat or possible security weakness in company systems.
- Refrain from downloading suspicious, unauthorised or illegal software on their Trust equipment.
- Avoid accessing known malicious and/or suspicious websites.

Employees are expected to comply with the trust's Online Safety Policy and associated policies.

The Trust and school IT support will:

- Install firewalls, anti-malware software and access authentication systems.
- Arrange security training for all employees as part of an initial induction for new starters and annually for existing staff.
- Upload training materials on the EVERY's e-learning portal for all of our schools, upon request.
    - Additional material is also available at Cyber security training for school staff - NCSC.GOV.UK
- Inform employees regularly about new scam emails or viruses and ways to combat them.
- Investigate security breaches thoroughly.
- Follow this policy's provisions.

Everyone should feel that their data is safe. The only way to gain trust is to proactively protect systems and data. Everyone can contribute to this by being vigilant and keeping cyber security at the top of their minds.

3.7 Remote employees

Remote employees must follow this policy. Since they will be accessing Trust information and systems remotely, they are obliged to follow all data encryption, protection standards and settings, and ensure their private network is secure. Where possible, remote access to information and systems should only be from school issued devices.

Employees are encouraged to seek advice from the school IT support or, if employed centrally, from the Trust IT support.

3.8 WiFi security

Access to school and Trust Wi-Fi networks should only be granted to known corporate devices.

Access codes should be encrypted and deployed through device management procedures and not made public.

An isolated guest Wi-Fi provision should be available for visitors using non-corporate devices and is granted at the school's discretion. Under no circumstances should such devices be permitted to use the corporate Wi-Fi.

A BYOD (bring your own device) agreement is required if schools wish to allow staff and students to use these whilst accessing the network. A BYOD template can be found in ***Appendix A***.

4. Disciplinary Action

4.1 All employees are expected to follow this policy at all times and those who cause security breaches may face disciplinary action.

4.2 Deliberate and serious breach of this policy may lead to the Trust taking disciplinary measures in accordance with the Trust's Disciplinary policy and procedure.

4.3 Misuse of these facilities can have a negative impact on employees' and volunteers' productivity and the reputation of the Trust. In addition, all the Trust's phone, web-based, locally hosted systems and email related resources are provided for business purposes. Therefore, the Trust maintains the right to monitor all internet and local network traffic, together with the email systems. The specific content of any transactions will not be monitored unless there is a suspicion of improper use - see the Safeguarding section below.

4.4 Examples of deliberate or serious breaches of this policy and examples of misuse are, but not limited to:

- Knowingly disclose login information to an unauthorised third party.
- Inappropriate disclosure of personal data.
- Knowingly installing software on Trust devices that hasn't been approved by IT which leads to a breach.
- Allowing the use of Trust devices by unauthorised third parties.
- Storing data on insecure media such as removable media that leads to a breach.

5. Safeguarding

5.1 Schools have a statutory duty to monitor their digital environment to identify any potential threats to pupils' welfare and wellbeing. EMET schools have appropriate filtering and monitoring in place.

5.2 Schools must regularly (at least half-termly) review the logs produced by their filters. Monitoring what is trapped by the filter allows schools to identify individuals using inappropriate search terms, so that they can be given advice/support, and to see any trends, which can be used to inform the school's curriculum/advice to staff, pupils and parents/carers.

5.3 In the case of a specific allegation of misconduct, the safeguarding lead/investigating officer can authorise access to the specific content of transactions in order to investigate the allegation.

6. Reporting and Contact Information

Questions or reports relating to this policy should be sent to: adminoffice@emet.uk.com

Named school contact: _David Newton d.newton@kimberleyschool.co.uk

Appendix A – Bring your own device agreement

BRING YOUR OWN DEVICE AGREEMENT

The East Midlands Education Trust (EMET) will allow personal devices on our guest network and school grounds for staff and Post16 students who follow the responsibilities stated in the Acceptable Use Policy (AUP) and the guidelines stated in this Bring Your Own Device (BYOD) policy.
The East Midlands Education Trust (EMET) strives to provide appropriate and adequate technology to support teaching and learning. The use of personal devices by students and staff is optional, and are used at the owner's risk.

We will review cyber-safety rules with students and staff frequently throughout the course of the school year and will offer reminders and reinforcement about safe online behaviours. In addition to the rules outlined in these guidelines, students and staff will be expected to comply with all class and school rules while using personal devices. The use of technology is not a necessity but a privilege. When abused, privileges will be taken away.

Device Types:
For the purpose of this programme, the word "devices" will include: laptops, netbooks, mobile phones, smart phones, I-pods, I-pads, tablets, and E-readers. Please note that games consoles will not be permitted.

Guidelines:

- Students and staff participating in BYOD must adhere to the Acceptable Use Policy.
- Each teacher has the discretion to allow and regulate the use of personal devices in the classroom and on specific projects.
- Approved devices must be in silent mode while on school campus, unless otherwise allowed by a teacher. Headphones may be used with teacher permission.
- Devices may not be used to cheat on assignments, quizzes, or tests or for non-instructional purposes (such as making personal phone calls and text messaging).
- Students may not use devices to record, transmit, or post photographic images or video of a person or persons on campus during school hours or during school activities, unless otherwise allowed by a teacher.
- Student devices may only be used to access computer files on internet sites which are relevant to the classroom curriculum.

Students and Staff acknowledge that:

- The school's network filters will be applied to a device's connection to the internet and any attempt to bypass the network filters is prohibited.
- Students and staff are prohibited from knowingly:
  - Bringing a device on premises that infects the network with a virus, Trojan, or program designed to damage, alter, destroy, or provide access to unauthorized data or information.
  - Processing or accessing information on school property related to "hacking." Altering or bypassing network security policies.

- EMET is authorised to collect and examine any device that is suspected of causing technology problems or was the source of an attack or virus infection.
- Students should be aware that devices are subject to search by school administrators if the device is suspected of a violation of the AUP. If the device is locked or password protected the student or staff will be required to unlock the device at the request of a school administrator.
- Staff may also be requested to make their devices available for search if the device is suspected of violating the AUP.
- Printing from personal devices will not be possible at school.
- Personal devices must be charged prior to school and run on battery power while at school. Other than in exceptional circumstances the charging of devices will not be permitted at EMET schools.
- EMET administrators have the right to block the use of personal devices if it is deemed necessary.

Lost, Stolen, or Damaged Devices:
Each user is responsible for his/her own device and should use it responsibly and appropriately. EMET schools takes no responsibility for stolen, lost, or damaged devices, including lost or corrupted data on those devices. While school employees will help students identify how to keep personal devices secure, students will have the final responsibility for securing their personal devices. Please check with your homeowner's policy regarding coverage of personal electronic devices, as many insurance policies can cover loss or damage.

Usage Charges:
EMET schools are not responsible for any possible device charges to your account that might be incurred during approved school-related use.

Network Considerations:
Users should strive to maintain appropriate bandwidth for school-related work and communications. All users will use the "BYOD" wireless network to access the internet. EMET does not guarantee connectivity or the quality of the connection with personal devices. EMET IT Support department is not responsible for maintaining or troubleshooting student or staff personal devices.

I understand and will abide by the above policy and guidelines. I further understand that any violation is unethical and may result in the loss of my network and/or device privileges as well as other disciplinary action. During the course of the school year, additional rules regarding the use of personal devices may be added.

_____ _____

Signature of Student/Staff Member Date