Melrose Education
LIMITED

Cyber Security Policy

Reviewed by:	Andrew Patterson, Compliance Manager and Lauren Mansfield, IT Manager
Date:	1 September 2024
Last reviewed on:	1 August 2023
Next review due by:	31 August 2025
Version control:	2
Approved by:	Tracey Storey, CEO

Contents

- Current Cyber Security Threats
- Types of Cyber Attacks
- Phishing (and Smishing)
- Help Your Staff to Spot Unusual Requests
- Cyber Security Measures
- User Information and Education
- Reporting Culture and Processes
- Cyber Security and Data Breaches
- Third Party Applications
- Passwords
- Employee Responsibilities
- Further Information and Reading
- Online Safety Advice

Melrose Education and its subsidiaries (schools) recognises that Cyber Security is an essential function to protect not only our own Company's assets and functions, but also to safeguard and protect the sensitive data we may hold and process about our stakeholders.

Cyber security is the process by which individuals and organisations reduce the risk of a cyber-attack. Cyber security's core function is to protect the devices we all use (smartphones, laptops, tablets, and computers), and the services we access - both online and at work - from theft or damage. It is also about preventing unauthorised access to the vast amounts of personal information stored on these devices, and online.

Melrose Education is aware of the growth of Cyber Crime activities and has procedures and processes in place to minimise both the opportunities for an attack taking place, and to minimise any resulting damage arising out of a malicious attack.

We take the potential threat of Cyber Attack seriously, and all staff must abide by this policy, and its associated policies, including:

- Clear Desk and Screen Policy
- Online Safety - Acceptable Use of Technology
- Online Safety - Use of Computers, Internet, and Email
- GDPR Policy
- Melrose Education Privacy Management Programme
- Safeguarding Online Safety Audit
- Social Media Policy
- Social Networking Guide for Staff
- Staff Acceptable Use of Technology Declaration

Current Cyber Security Threats

A Cyber Threat Actor (CTA) is a participant (person or group) in an action or process that is characterized by malice or hostile action, using computers, devices, systems, or networks. CTAs are classified based on their motivations and affiliations and include:

- ***Cybercriminals*** - profit-driven and represent a long-term, global, and common threat. They target data to sell, hold for ransom, or otherwise exploit for monetary gain.
- ***Insiders*** - current or former employees, contractors, or other partners who have access to an organisation's networks, systems, or data. Malicious insiders intentionally misuse their access in a manner that negatively affects the confidentiality, integrity, or availability of the organisation's information or information systems. This is distinct and separate from employees who unintentionally cause damage to their organisation's information systems through their actions, such as clicking on malicious links in a phishing email, which is the number one cause of cyber-attacks.
- ***Foreign Government*** - aggressively target and gain persistent access to public and private sector networks to compromise, steal, change, or destroy information.
- ***Hacktivists*** (Ideologically Motivated Criminal Hackers) are politically, socially, or ideologically motivated and target victims for publicity or to effect change.
- ***Terrorist Organisations*** – activity is typically disruptive or harassing in nature.

Types of Cyber-Attack
Common types of cyber-attack include:

- ***Malware*** - Malware is a term used to describe malicious software, including spyware, ransomware, viruses, and worms. Malware breaches a network through a vulnerability, typically when a user clicks a dangerous link or email attachment that then installs risky software. Once inside the system, malware can do the following:
    - Block access to key components of the network (ransomware)
    - Installs malware or additional harmful software.
    - Covertly obtains information by transmitting data from the hard drive (spyware)
    - Disrupt certain components and renders the system inoperable.
- ***Phishing*** - Phishing is the practice of sending fraudulent communications that appear to come from a reputable source, usually through email. The goal is to steal sensitive data like credit card and login information or to install malware on the victim's machine. Phishing is an increasingly common cyberthreat. A Cyber-attack made via text message or SMS is known as Smishing.
- ***Man-in-the-middle attack*** - Man-in-the-middle (MitM) attacks, also known as eavesdropping attacks, occur when attackers insert themselves into a two-party transaction. Once the attackers interrupt the traffic, they can filter and steal data. Two common points of entry for MitM attacks are:
    - 1. On unsecure public Wi-Fi, attackers can insert themselves between a visitor's device and the network. Without knowing, the visitor passes all information through the attacker.
    - 2. Once malware has breached a device, an attacker can install software to process all the victim's information.
- ***Denial-of-service attack*** - A denial-of-service attack floods systems, servers, or networks with traffic to exhaust resources and bandwidth. As a result, the system is unable to fulfill legitimate requests. Attackers can also use multiple compromised devices to launch this attack.
- ***SQL Injection*** - A Structured Query Language (SQL) injection occurs when an attacker inserts malicious code into a server that uses SQL and forces the server to reveal information it normally would not. An attacker could carry out a SQL injection simply by submitting malicious code into a vulnerable website search box.
- ***Zero-day exploit*** - A zero-day exploit hits after a network vulnerability is announced but before a patch or solution is implemented. Attackers target the disclosed vulnerability during this window of time.

Phishing (and Smishing)
Whilst cyber-attacks can come in many forms, the number one cause of cyber security breaches is Phishing or Multi-Layered Phishing (Social Engineering).

Phishing emails are designed to trick an individual into divulging sensitive information or will include a malicious link or attachment which if clicked on or opened will download Malware on to your computer and/or network.

Whilst some Phishing emails may contain obvious spelling or grammar mistakes, Cyber Criminals are becoming more sophisticated and may include personal information to give their appearance validity.

Phishing emails will often include ‘urgency’ and ‘authority’ cues to pressure you to act quickly and without thinking, for example, your payment has been declined, ‘click here to avoid further action,’ or claim to be from a person in authority, for example a CEO.

Melrose Education’s employees are expected to be familiar with the organisation’s policies and procedures and to double check the validity of an email or instruction if something seems unusual. This checking must not be undertaken by responding to the email - you should telephone a trusted contact.

‘Phishers’ will use publicly available information to make their emails more convincing so employees should consider reviewing privacy settings on social media settings.

Employees are not permitted to post online about any Company or organisational activity which is not already in the public domain or provided or approved by the Company.

Spotting scam emails is tricky, but things to look out for include:

- official-sounding messages about ‘resetting passwords,’ ‘receiving compensation,’ ‘scanning devices’ or ‘missed deliveries.’
- emails full of ‘tech speak,’ designed to sound more convincing.
- being urged to act immediately or within a limited time. The message will often claim to be from an authority figure (like a bank, or power company).

Remember, your bank (or any other official organisation) will **never** ask you to supply personal information.

If you have any doubts:

- contact the organisation directly using their official website or social media channels. Do not use the links or contact details in any messages you have been sent.
- Hover over the recipient to see the full originating email address; an email address can be set to appear as something like “Lloyds Bank” in the settings, but if you hover over this name, it could be from ‘clicktogetphished@scammer.com’.
- If a suspicious email arrives which is from someone within your organisation, call them to check.
- Always contact our Internal IT Department to advise them of your concerns.

Help Your Staff to Spot Unusual Requests

Do colleagues and staff at your school know what to do with unusual emails or phone calls, and where to get help? Ask yourself whether someone impersonating an important individual (a parent, member of staff, or member of the local authority) would be challenged by everyone in your school. Think about how you can encourage and support your staff to question suspicious or just unusual requests, even if they are from important individuals. Having the confidence to ask, ‘is this genuine?’ can be the difference between staying safe, or a costly mishap.

Cyber Security Measures

Melrose Education Limited and its subsidiaries has the following protective measures in place to minimise the risk of a cyber-attack:

- Firewalls installed at all sites.
- Endpoint detection and response installed on all sites.
- Advanced email security and phishing detection.
- Automatic patch updates (to ensure security updates are installed without delay)
- Secure document sharing and storage – SharePoint.
- System for the updating of passwords and removal of access when an employee leaves our employment.
- Regular IT incident and problem reviews for a proactive approach to IT and Cyber Security.
- Change Management
- Security Awareness Training and Phishing Simulation
- Websites built with protection from SQL injections and SSL certificates for all sites, plus automated vulnerability scans regularly conducted.
- Limitation of, and removal of unnecessary email addresses.

User Information and Education

Melrose Education advocates a User Information and Education approach to Cyber Security in addition to the measures outlined in this policy, and ensures all relevant users have access to training courses to support this.

Reporting Culture and Processes

Melrose Education and its subsidiaries understand that a reporting culture in which errors are identified and reported as soon as possible can minimise the impact of any potential breach and highlight areas for additional training and/or improvement in our processes. Any employee who believes they have accidentally clicked on a suspicious link, opened a malicious attachment or in any other way potentially breached or allowed the breach of our internal systems, must report this immediately to both our internal IT Department and to the Compliance Manager.

If a member of staff receives a suspicious email, and have not been able to check it's validity with a trusted contact within the organisation, or they have confirmed it has not originated from them, this must be reported internally using the same process as above, and also to the Suspicious Emails Reporting Service (SERS) on report@phishing.gov.uk

Suspicious SMS should be reported internally, as above, and by forwarding the SMS to 7726 (remember 'SPAM' on a telephone keypad). Please note you will be asked to provide the telephone number you have received the suspicious SMS from so do not delete the message before you have completed the reporting process.

If you have been tricked into providing your banking details, contact your bank and let them know.

If you have given out your password, you should change the **passwords** on any of your accounts which use the same password.

Incidents of fraud and cybercrime will be reported to Action Fraud.

Further information can be found here.

Cyber Security and Data Breaches

A cyber security breach may also represent a personal data breach (or put the company or school at risk of one). It is therefore essential that if you believe a cyber breach may have taken place, you report this immediately to your school's DDL, or Principal so that a Personal Data Breach Form can be completed, and a decision taken as to whether the breach is reportable to the Information Commissioner's Office, which will be completed by Andrew Patterson, Compliance Manager, the Company's DPO Lead.

Third Party Applications

As part of its day-to-day operations, Melrose Education Limited and its subsidiaries and employees use a number of third-party applications, including the below. These third-party applications have their own systems for ensuring the security of the data including but not limited to:

- Local Authority Egress and other secure systems
- Sage
- Bright Pay HR
- NatWest Bankline

Passwords

Melrose Education takes the security of its passwords seriously and expects all employees to do the same.

Access to Office365 applications, including email and SharePoint, is via a complex password created and imputed by our Internal IT Department.

Office365 passwords are changed when a user leaves the organisation or will be absent from the organisation for an extended period, for example, on Maternity or Paternity Leave. Authorisation for access to in-active accounts must be approved by the CEO. New email diverts or forwards also require the same authorisation.

Melrose Education Limited follows guidance on Using Passwords from the National Cyber Security Centre, and also requires its employees to adhere to this guidance and the following requirements when using and setting passwords which are not controlled centrally by the Company. Passwords must:

- Use Multi-Factor Authentication (where applicable/available)
- Avoid the most common passwords that criminals can easily guess, for example 'passw0rd'.
- Be made up of 3 random words – these must not be words which are easily guessed (like a pet's name or anything which is linked to school, your hobbies, or your children). Numbers and symbols can be included if you need to, for example, 'OrangeToasterExtension5!'.
- Not be duplicated/used for multiple accounts.
- Not be written down and kept near to your computer. If passwords are written down, they must be kept securely, out of sight.

If more than one person is accessing your computer, you should ideally have different accounts, and different passwords, for each person. Where this is not possible, make sure you know who has access to your devices, who knows the password, and that you are OK with this.

Never write the password on a post-it that is stuck to the computer, where anyone could access your details. For the same reasons, use a **lock screen** when you are not at your desk, and make sure you change your passwords when a member of staff with access to your devices leaves.

Employee Responsibilities

All employees of Melrose Education and its subsidiaries are responsible for ensuring they:

- Undertake all relevant training on Cyber Security issued to them by the company.
- Use only company issued software and hardware, including laptops, computers, mobile phones, mobile phone chargers, tablets, tablet chargers, SD cards or memory sticks. Do **not** use your personal equipment.
- Use SharePoint (and **not** email) to share any information of a sensitive information.
- Include password protection on all documentation coming via emails i.e., safeguarding notifications, contracts of employment, and a host of other email traffic attachments that contain personal data.
- Passwords protect any document which cannot be shared via SharePoint before sending via email. Passwords must never be shared via email and must be given verbally only. The person supplying the password must telephone the recipient, and not provide the password on an incoming call.
- Adhere to the password requirements detailed in this policy.
- Validate any unusual or suspicious request for information made via email or SMS with a trusted contact and report the suspicious activity as per the reporting process detailed in this policy.
- Do not provide information about any member of staff, child, or parent of the school on an incoming call to the school (even to confirm they are at your school or work for the Company). You should never assume a phone call is authentic just because someone knows your basic details such as name and address and you should never confirm a child/learner's attendance at your school as you cannot be sure who you are talking to. Advise you will look into the request, and then you should return the call on a known contact number.
- Always save documents on OneDrive or to SharePoint. Documents should never be saved on your desktop as these are not recoverable.
- Read and are familiar with the NCSC's Staying Safe Online 'Top Tips for Staff'.
- Read and are familiar with the NCSC's 'Business Email Compromise' Fact Sheet.
- Implement safe storage of confidential paperwork in a locked cabinet.
- Never take confidential or sensitive information home.
- Never leave Company hardware in a car or otherwise non-secure location.
- Have face-recognition access enabled on the Company mobile phone, with a PIN code which is not easily guessed, for example birthdays or other memorable dates/number combinations must not be used.
- Will not delay applying updates to apps and your device's software. These updates include protection from viruses and other kinds of malware and will often include improvements and new features. Applying software updates is one of the most important things you can do to protect your devices.
- Update all apps and your device's operating system when you are prompted. You can also turn on 'automatic updates' in your device's settings, if available. This will mean you do not have to remember to apply updates.
- If you think your device contains a virus (or any other type of malware), please contact the internal IT department as soon as possible and disconnect your device from any network.

Further Information and Reading

https://www.ncsc.gov.uk/guidance/hacked-device-action-to-take
https://www.ncsc.gov.uk/files/Recovering-hacked-online-accounts-infographic.pdf

Online Safety Advice:

- https://www.getsafeonline.org/
  UK's leading awareness resource helping to protect people from online fraud and other issues.
- https://www.cyberaware.gov.uk/
  Government advice about cyber security
- https://www.cyberessentials.ncsc.gov.uk/advice/
  Government advice for Businesses
- https://takefive-stopfraud.org.uk/
  Advice regarding online fraud (**Take Five campaign toolkit**)
- https://www.saferinternet.org.uk/
  Online safety tips, advice, and resources
- https://www.ageuk.org.uk/information-advice/work-learning/technology-internet/internet-security/
  Age UK advice and tips to stay safe online.
- https://www.ncsc.gov.uk/information/report-suspicious-emails
  If you have received an email which you are not sure about, forward it to the Suspicious Email Reporting Service (SERS).
- https://www.ncsc.gov.uk/guidance/video-conferencing-services-using-them-securely
  Video conferencing guidance from the NCSC (**Individuals**)
- https://www.ncsc.gov.uk/guidance/video-conferencing-services-security-guidance-organisations
  Video conferencing guidance from the NCSC (**Organisations**)
- https://www.actionfraud.police.uk/
  Action Fraud is the UK's national reporting centre for fraud and cybercrime in England, Wales, and Northern Ireland.
- https://www.ncsc.gov.uk/information/mailcheck
  NCSCs mail check assists with email reporting and configuration (DMARC).
- Cyber Aware - NCSC.GOV.UK
  Step-by-step instructions on enabling the free security feature that prevents hackers from accessing your accounts, even if they know your password.
- https://haveibeenpwned.com/
  Check if your accounts have been compromised.
- Social Media: how to use it safely - NCSC.GOV.UK
  Social Media Privacy Settings.
- Police CyberAlarm
  Helping organisations monitor and report malicious activity.

Useful Videos:

https://www.youtube.com/watch?v=sgs3lnemp3g&feature=youtu.be- Threat Actors
https://youtu.be/ZPori-GTI-4 - Ransomware
https://www.getsafeonline.org/fraudstars/ - Impersonation Fraud
https://www.youtube.com/watch?v=yrjT8m0hcKU – Action Fraud (Social Media Settings)

https://www.youtube.com/watch?v=aujUl3yt6nM – Quad9

Cyber Prevent Links :
https://www.westyorkshire.police.uk/advice/online-crime-safety/online-safety/cybercrime/cyber-choices- Cyber Choices (courses/qualifications).
https://www.youtube.com/watch?v=DjYrxzSe3DU- NCA Video.

Learn how to protect yourself online with the Cyber Aware Action Plan Individuals and families Action Plan - NCSC.GOV.UK