Empowering Minds Cyber Policy

The Empowering Minds Cyber and Information Management Policy has been created to ensure all data and systems are kept safe, along with providing guiding principles towards content management, retention, and acceptable actions representatives of Empowering Minds can take with available content. It is a **requirement** to follow this Policy if you have access to any Empowering Minds documents, files, systems, hardware, and/or email.

1. Password Requirements

The following information outlines the expectations for:

A. Storing Passwords
B. Creating Strong Passwords and Password Requirements
C. When to Update Passwords
D. Importance of Having Unique Passwords for Different Logins

A. Storing Passwords

- Use a password manager – this will create and securely store unique passwords for you. Examples of password managers include Google Password Manager or Dashlane. *For extra security, add a log-in password for your computer. Then to see your passwords saved in Google Password Manager you have to enter your log-in password adding another level of security.*
- Don't write passwords down on paper or store a list in a word document – they can be stolen and used to access your accounts.
- Select 'no' when a computer offers to automatically remember your password when logging onto a website.

B. Creating Strong Passwords and Password Requirements

Tips to create a strong password – and remember it. It can help if you:

- Make your passwords have meaning.
- Use the letters of a song, musical or movie title and change some of the characters to make a strong password. For example: Casino Royal 007 = C@s!n0r0y@Le7 or Les Miserable= L3$m!s3r@bLe

Passwords MUST:

- Be at least 8 - 10 characters long
- Not contain a complete word which easily links to you including your name, company name, family member or pet(s)
- Include a mix of upper-and lower-case letters, numbers and symbols
- Be different from each other and from previous passwords
- Be changed every 12 Months
- Be kept private
- Be unique and very hard to guess

C. When to Update Passwords

Passwords should be changed every 12 Months. New information outlines that there is a problem that comes with frequent password changes. The key is to make passwords strong so they do not have to be changed every 30 – 60 Days.

D. Importance of Having Unique Passwords for Different Logins

If passwords are too simple, hackers can easily guess or gather them, giving cybercriminals free access to your system. Once they're in, you have a major problem. The stronger and more complex your passwords, the safer your network will be from a cyber-attack.

2. Email Security Measures

This section includes:

A. Opening Email Attachments and Links from Trusted Sources
B. Blocking Junk, Spam, and Scam Emails
C. Deleting and Reporting Suspicious Emails
D. Accessing Email or Business Apps on Devices

A. Opening Email Attachments and Links from Trusted Sources

- Only open email attachments and links from TRUSTED sources.
- Never open links from contacts that are not work related. (Example – Funny Cat Videos.)
- If you are not sure about the link or attachment, DO NOT OPEN. Reach out to the Operations Manager and ask.
- Trust your gut! If it does not look right or feel right, then DO NOT OPEN and reach out to the Operations Manager and ask.

B. Blocking Junk, Spam, and Scam Emails

Empowering Minds uses Microsoft Exchange Online so we are automatically protected against spam by EOP. EOP uses anti-spam policies (also known as spam filter policies or content filter policies) as part of our overall defense against spam.

It is still up to users to block or unsubscribe to junk, spam, and/or scam emails if one lands in their inbox (gets past the Microsoft Firewall).

Additional security on a user's computer is up to the individual user. The individual user is responsible for the additional costs incurred for extra security. (Example adding Trend Security.)

It is expected that users run Security Scans a minimum of once/week.

C. Deleting and Reporting Suspicious Emails

If an email is suspicious, share the information with the Empowering Minds team members in a new email so they are aware. We want to protect our team and make sure no one 'falls into a trap'!
NEVER FORWARD THE EMAIL!

Next, mark the email as junk and then permanently delete from your junk file.

When prompted to report this information to Microsoft, click 'report' so Microsoft is made aware and has a reference log.

D. Accessing Email or Business Apps on Devices

It is up to individual users to set-up their email or other apps (example – Asana) used by Empowering Minds. It is not mandatory to have access to email or the other apps on your devices. If the user chooses to be able to access email and business apps, the user must PROVE they have security on their device and they must comply with the Empowering Minds Cyber Policy and Information Management Policy.

3. How to Handle Sensitive Data

This section includes:

A. Sharing Sensitive Data with Others
B. Ways to Store Physical Files and How Long to Store Files
C. Ways to Identify Sensitive Data
D. Ways to Destroy Sensitive Data When it is No Longer Needed

A. Sharing Sensitive Data with Others

- Never directly email or text credit card information or banking information.
- If you are required to pay by credit card or provide banking information, here are the options available to you:
  1. Complete the secured form on vendor's secure website.
  2. Complete manual form and mail it in or send an email with the form attached (scanned pdf) via a secure internet connection. (Secure internet connection is your home office connection. Unsecured internet connections include public shared networks.)
  3. Call the vendor and provide the information over the phone.
- Be professional! If your computer is provided by Empowering Minds, we have the right to review ALL your computer files and programs at any time. If you don't want Empowering Minds to see something on your computer, then it should not be on your computer.

B. Ways to Store Physical Files and How Long to Store Files

Hard copies of data (physical files) are to be stored in the following manner:

- All student registration forms, data, information, etc., will be stored in a locked filing cabinet in the Program Manager's office for a maximum of 1 year.
- All accounting forms, data, statements, etc., will be stored in a locked filing cabinet in the acting bookkeeper's office for a maximum of 18 months.
- All operational documents, miscellaneous and otherwise, will be stored in a locked filing cabinet in the Operations Manager's office for a maximum of 1 year.

C. Ways to Identify Sensitive Data

The following is a list of items that fall under 'sensitive data'.

- Intellectual Property
- Information not widely distributed or known to the public
- Product, process, program, or service information
- Specifications and requirements
- Strategy documents
- Inventions, designs, and formulae
- Reports

- Source and object code
- Databases
- Trade secrets
- Supplier lists
- Customer and prospect lists
- Contact lists
- Marketing techniques
- Pricing and cost policies
- Financial information
- Internal operations documents

If you are not sure, ask! In this case it is better to ask rather than assume.

D. How to Destroy Sensitive Data When it is No Longer Needed

If the Sensitive Data is in Hard Copy it should be destroyed on an annual basis.

- Scan and save document into Empowering Minds One-Drive if it should be held onto for future reference.
- Once document is saved, shred document(s). Access to a shredder will be made available annually to ensure safe disposal of all sensitive data in hard copy form.

If the Sensitive Data is Electronic it will be destroyed on an annual basis.

- Data will be reviewed and confirmed for disposal.
- Documents deleted from files to be deleted from Recycle Bin(s) to ensure there can be no access to the document is the future.

4. How to Handle Technology

This section includes:

A. Accessing Devices away from the Workplace
B. Storing Devices When Not in Use
C. Reporting a Theft or Loss of a Work Device
D. Maintaining Systems
E. When to Shut Down Computers and Cell Phones
F. Locking Screens When Devices are Unattended
G. Protecting Data Stored on External Devices
H. Removable Device Restrictions

A. Accessing Devices away from the Workplace

Devices such as lap tops can be used anywhere as long as proper security is on the device and the security has been verified by Empowering Minds. It is preferred that employees use a dedicated/secured network to access the internet. If using a public network, we request that all applications are properly signed out of and the applications are closed.

B. Storing Devices When Not in Use

When not in use, it is expected that devices that have access to the Empowering Minds digital network are turned off and are securely stored.

C. Reporting a Theft or Loss of a Work Device

If a device has been stolen or it is lost, report the loss to the Empowering Minds Operations Manager IMMEDIATELY. This will ensure a quick response to 'lock-up' the system. In the absence of the Operations Manager, please contact the President.

D. Maintaining Systems

Current Empowering Minds digital systems use the Cloud as a result all updates related to Empowering Minds will be automatic.

Individual users will be responsible for installing other updates related to their hardware, operating systems, and/or additional security.

E. When to Shut Down Computers or Cell Phones

When not in use for over 1-Hour, it is expected that devices that have access to the Empowering Minds digital network are turned off and are securely stored.

F. Locking Screens When Device is Unattended

When stepping away from your computer for more than 30 minutes, it is expected that devices that have access to the Empowering Minds digital network be locked or turned off.

G. Protecting Data Stored on External Devices

When not in use or in transport, USB sticks or other external storage devices with Empowering Minds data is stored in a locked and secured draw.

When in transport, the USB sticks or other external storage devices with Empowering Minds data is kept on the person in a secure fashion.

H. Removable Device Restrictions

As each user at Empowering Minds is responsible for their own computer. It is up to them to maintain their security and ensure no malware is installed.

If a removable device is provided, we highly recommend not opening those files unless they come from a trusted source and if they do come from a trusted source, we recommend scanning the files before opening the files.

5. Standards for Social Media and Internet Access

This section includes:

A. Appropriate Information for Sharing on Social Media Channels
B. Appropriate Use of Empowering Minds Email Account

A. Appropriate Information for Sharing on Social Media Channels

All information posted on social media channels must be approved before posting by the President or the Operations Manager. Potential content includes but is not limited to:

- Donation Requests
- Live & Unsigned Requests (Auditions, Auction Items, Sponsors)
- Announcing New Team Members (Directors, Contractors)
- Available Sessions

- Program Updates
- Celebrating Successes

B. Appropriate Use of Empowering Minds Email Account

It is very important that Empowering Minds looks professional. When using an Empowering Minds email account or when representing the organization, it is critical to use proper English.

Empowering Minds has a zero tolerance for profanity, prejudice language, or harassing language. Anyone representing the organization that uses inappropriate language will be immediately dismissed.

6. If An Incident Occurs (Security Incident Response Plan)

This section includes:

A. How to Respond to a Cyber Incident and Actions to Take
B. Empowering Minds User Responsibilities for Dealing with a Cyber-Attack
C. Identify Lessons Learned

A. How to Respond to a Cyber Incident and Actions to Take

The key to avoiding having to respond to an incident is to be proactive! Monitor your computer weekly – sometimes daily as needed. Check and identify any unusual activities that may damage your business information and systems. Unusual activity may include:

- Accounts and your network not accessible
- Passwords no longer working
- Data is missing or altered
- Your hard drive runs out of space
- Your computer keeps crashing
- Your customers receive spam from your business account
- You receive numerous pop-up ads

B. Empowering Minds User Responsibilities for Dealing with a Cyber-Attack

If a cyber-attack occurs, here are the steps to follow:

- Find the initial cause of the incident and assess the impact so you can contain it quickly.
- Determine the impact the incident has had on the business.
- Determine its effects on the business and assets if not immediately contained.
- Limit further damage of the cyber incident by isolating the affected systems. If necessary, disconnect from the network and turn off your computer to stop the threat from spreading.
- Eliminate the problem with the removal of the threat.
- Recover from the incident by repairing and restoring your systems to business as usual.
- Identify if any systems and processes need improving and make those changes.
- Evaluate the incident before and after, and any lessons learnt.
- Update your cyber security incident response plan based on the lessons learnt so you can improve your business response.

C. Identify Lessons Learned

This step is to be performed no later than one week from the end of the incident, to ensure information is fresh. In this stage, identify the following and submit to the President or Operations Manager:

- What happened?
- When did it happen?
- How was it contained and eradicated?
- What was done to recover the attacked systems?
- Identify the areas where the response team was effective.
- Identify the areas that require improvement moving forward.

Internet usage has grown so quickly over the last two decades that technology now touches almost every aspect of our everyday lives. The importance of cybersecurity has thus never been greater.

This Cyber and Information Management policy regulates all aspects of the Empowering Minds digital and paper data exchange, including the Internet, data privacy and network usage as well as cyber defense.