Cyber Security Policy

Like businesses, charities are increasingly reliant on IT and technology and are falling victim to a range of malicious cyber activity. Losing access to this technology, having funds stolen or suffering a data breach through a cyber-attack can be devastating, both financially and reputationally. This policy has been developed using guidance from The National Cyber Security Centre (NCSC) for small charities.

Backing up data

It is vital to prevent loss of data following flood, fire, physical damage or theft by regularly backing up data, this will also make ELH NM more resilient to cyber-crime.

- ELH NM stores all its files on a server, this is backed up on a daily basis.
- Backups are made to an external hard drive, which is removed from the office overnight.
- The Finance and Office Manager is generally responsible for this, but can delegate this responsibility to other members of the team in anticipation of being away from the office.
- Staff email accounts are stored in the cloud which means this data is physically separate from the ELH NM office.

Keeping smartphones and tablets safe

Smartphones and tablets which are used away from the safety of the office need more protection than desktop equipment.

- All mobile devices are pin or password protected.
- All mobile devices are configured so that if lost or stolen, can be tracked, remotely wiped or locked.
- All mobile devices are kept up to date using the 'automatically update' option.
- When sending sensitive data, staff do not connect to public Wi-Fi spots, using only 3g or 4g connections via the device.

- Devices that are no longer supported by the manufacturers are replaced with up to date alternatives.
- Only approved software is downloaded to mobile devices.

Preventing malware damage

Malicious software (also known as 'malware') is software or web content that can harm desktop equipment. The most well-known form of malware are viruses, which are self-copying programs that infect legitimate software.

- Use antivirus software to protect electronic equipment from viruses

All of ELH NMs' computers and laptops are protected by antivirus software, our IT support company administer the software to ensure it cannot be turned off.

- Restrict threats from software and downloads

Staff have restricted permissions which do not allow them to install or download software. Our IT support company and the Finance and Office Manager have administrative permission to install software where needed.

- Patch all software and firmware

The latest software updates are set to automatically update.

- Switch on firewall

Our antivirus software also includes firewall protection. Our server is also protected under a separate firewall with additional security.

Avoid phishing attacks

In phishing attacks, scammers send fake emails asking for sensitive information, such as bank details or containing links to bad websites

- Ensure staff don't browse the web or check emails from an administrator user, this will reduce the impact of successful phishing attacks.
- Scan for malware and change passwords as soon as possible if you suspect a successful attack has occurred.
- Check for obvious signs of phishing, like poor spelling and grammar, or low quality versions of recognisable logos. Does the senders email look legitimate, or is it trying to mimic someone you know?

Using passwords to protect data

Passwords, when used correctly, are a free, easy and effective way to prevent unauthorised people from accessing your devices and data.

- All desktop computers and laptops use encryption products that require a password to boot. Switch on pin/password protection or fingerprint recognition on mobile phones.
- Use two factor authentication from important websites such as banking and email, if you're given the option.
- Avoid using predictable passwords such as family or pet names, or the most common passwords that criminals can guess, like passw0rd. A strong password contains a combination of upper and lower case characters, numbers and symbols.
- Do not enforce regular password changes, they only need to be changed when you suspect a compromise.
- Change the manufacturers default passwords that devices are issued with, before they are distributed to staff.
- Provide secure storage so staff can write down passwords and keep them safe, but not with the device. Ensure staff can reset their own passwords easily.