GOOD PRACTICE GUIDE
PART 6

CYBER SECURITY POLICY

1. INTRODUCTION

1.1 This policy provides guidelines and provisions for preserving the security of the organisation's data and technology infrastructure.

1.2 The more the organisation relies on technology to collect, store, and manage information, the more vulnerable the organisation is to security breaches. Human errors, hacker attacks, and system malfunctions have the potential to cause financial damage and jeopardise the organisation's reputation with stakeholders and members.

1.3 The security measures within this policy aim to help mitigate security risks and ensure compliance with data protection.

2. SCOPE

2.1 This policy applies to all staff, volunteers, contractors, and anyone who has permanent or temporary access to the IT systems and hardware.

3. ROLES AND RESPONSIBILITIES

3.1 The CEO and DCEO shall:

- Contract suitably competent IT cyber security specialists to install firewalls, anti-malware software, suspicious activity monitoring and an access authentication system.
- Ensure provision of regular training for all staff and contractors.
- Investigate security breaches thoroughly and record incidents.
- Control and review administrative rights to relevant personnel.
- Ensure policy compliance.

3.2 All staff and contractors shall:

- Follow the cyber security guidelines and policies, including those contained within the staff handbook.
- Regularly undertake training and keep up to date.
- Report any suspicious activity.

4. ACCESS CONTROL

4.1 It is important to manage access to the organisation's data platform through the following controls:

- **Unique access** – each staff member shall have unique credentials for access to the system and use Multi-Factor Authentication.
- **Least privilege** – grant only the permissions necessary for users to perform their role. For example, volunteers may only have access to the Teams Groups they are part of.
- **Just-in-time access** – allow access only when needed and revoke access when it is no longer required.
- **Review** – access levels for staff and volunteers shall be defined and permissions regularly reviewed.
- **Visibility** – ensure all access is visible and tracked to avoid unauthorised access and prevent data breaches.
- **Separate libraries** – place sensitive files in separate libraries or new sites and avoid overusing unique permissions.
- **Governance** – implement a framework to manage permissions and ensure compliance with policies that balance collaboration and security.

5. DATA TRANSFER AND STORAGE

5.1 The transferring of data introduces security risks. Staff shall:

- Avoid transferring sensitive data (e.g., member information, staff records) to other devices or accounts unless absolutely necessary.
- Ensure sensitive data is encrypted or password protected if shared outside of the organisation.
- Share confidential data over the company network/system and not over public Wi-Fi or private connections.
- Ensure that the recipients of the data are properly authorised people or organisations and have adequate security policies.
- Report scams, privacy breaches, and hacking attempts.

5.2 The storage of the organisation's data should only be on approved cloud platforms like OneDrive, SharePoint, and Teams.

6. DEVICE SECURITY

6.1 When staff use digital devices to access company emails or accounts, they introduce security risks. Staff devices shall have disk encryption, have remote wipe capability, patch management policy.

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

- Keep all devices password protected.
- Turn off their screens and lock devices when away from their desk.
- Ensure they do not leave their devices exposed or unattended outside of the office.

- Report stolen or damaged equipment as soon as possible to their line manager and SLT.
- Mobile devices that shall have security apps for remote wipe capability like Find My Phone, activated.
- Change all account passwords at once when a device is stolen.
- Ensure all devices have antivirus software and are set up with automatic updates.
- Install security and software updates as soon as updates are available.
- Log into company accounts and systems through secure and private Wi-Fi networks only.

6.3 The use of personal devices to access organisational systems should be kept to a minimum and only with authorised permission from the CEO, and where device security standards are met.

6.4 Staff shall avoid accessing internal systems and accounts from other people's devices or lending their own devices to others.

7. EMAIL AND COMMUNICATION

7.1 Emails often host scams and malicious software (e.g., worms). To avoid virus infection or data theft, staff are instructed to:

- Avoid opening attachments and clicking on links when the content is not adequately explained (e.g., "watch this video, it's amazing").
- Be suspicious of clickbait titles (e.g., offering prizes, advice).
- Check email addresses and names of people they receive messages from to ensure they are legitimate.
- Look for inconsistencies or giveaways (e.g., grammar mistakes, excessive capital letters, excessive exclamation marks).
- Report any phishing attempts immediately.

7.2 The organisation's IT contractors are knowledgeable in detecting scam emails. Staff are encouraged to reach out to them and their line manager with any questions or concerns.

8. PASSWORD POLICY

8.1 Password leaks are a risk as they can compromise the entire infrastructure. Not only should passwords be secure so they are difficult to hack, but they should also remain secret. For this reason, staff are advised to:

- Choose passwords with at least eight characters (including capital and lowercase letters, numbers, and symbols) and avoid information that can be easily guessed (e.g., birthdays).
- Do not use the same password across different accounts and platforms.
- Where available, make use of PINs or biometric options.
- Remember passwords instead of writing them down. If employees need to write their passwords, they are obliged to keep the paper or digital document confidential and destroy it when their work is done.

- Exchange credentials only when absolutely necessary. When exchanging them in person isn't possible, employees should use the phone or WhatsApp instead of email.
- If a password has been shared, update it as soon as reasonably possible.
- Use a password management tool that generates and stores passwords. Staff are obliged to create a secure password for the tool itself.

Additional measures

8.2 To reduce the likelihood of security breaches, we also instruct staff to:

- Report a perceived threat or possible security weakness in company systems.
- Refrain from downloading suspicious, unauthorised, or illegal software on their company equipment.
- Avoid accessing suspicious websites.
- When working away from the office, at home, or at competition venues, staff are obliged to follow all data encryption, protection standards, and settings, and ensure their home network or venue network is secure.
- Comply with the social media policy and IT and communications systems policy, which can be found in the Staff Handbook.
- Comply with the organisation's privacy policy and data protection and retention policies.

9. INCIDENT RESPONSE

9.1 A cyber incident or attack is often an intentional and unauthorised attempt to access, change, or damage data and digital technology.

9.2 As soon as a potential incident or attack has been reported, the following steps should be considered:

- Contain the risk and make sure systems are safe and secure.
- Notify the CEO, DCEO, and Data Protection Officer.
- Capture information on the risk.
- The CEO will approve a formal investigation and escalate as required.
- The organisation's IT contractors will investigate the risk and advise on the next course of action.
- Report the potential incident or attack to the Chair of the Board.
- CEO and DPO will establish whether a data breach has occurred and inform the ICO if appropriate. See GDPR Policy.
- The event shall be recorded and lessons learnt.

9.3 The organisation's IT contractors need to know about scams, breaches, and malware to better protect the organisations infrastructure. For this reason, staff need to report perceived attacks, suspicious emails, or phishing attempts as soon as possible to DCEO and the IT contractors. The organisation's IT contractors, when appropriate, will investigate promptly, resolve the issue, and send an organisation wide alert when necessary.

10. TRAINING AND AWARENESS

10.1 Staff need to have appropriate cyber security awareness, knowledge, and skills to operate securely.

- All staff shall undertake appropriate cyber security training annually, and this shall be tracked.
- Cyber security information is easily available to staff; concerns are readily shared, owned, and taken seriously.

11. COMPLIANCE

11.1 Non-compliance may result in disciplinary action and loss of access.

12. POLICY REVIEW

12.1 This policy shall be reviewed by the Board every three years. Outside of this the DCEO may call for more frequent review as required, especially after any significant incident or changes in technology.