The Canoe Association of Northern Ireland (CANI)

Cyber Security Policy

CANI CYBER SECURITY POLICY

The purpose of this Cyber Security policy is to:

- Outline the processes and measures in place for cyber security.

Training

All CANI staff have cyber security training during induction. This includes any system access relevant for their role. It covers all aspects of cyber security from the password policy to awareness training for smishing, phishing,

CANI staff receive tips and hints for using IT assets more securely periodically throughout the year.

Security Update emails are sent to create a better security culture, containing trends and examples of recent activity from malicious actors.

Email Security

CANI uses the Office 365 system. All accounts use Multi-Factor Authentication (MFA) as well as passwords protected by an enforced password policy. MFA means that, as well as a password to enter, a message is also sent to a user's phone for further authentication before accessing the account, for example. In other cases, it is an email address or third-party authentication.

All CANI staff have a report phishing button on Outlook. If an email has made it through Microsoft's filters and the user thinks it is malicious, they can report it using the phishing button. The email is then passed to the NCSC and reviewed by the IT Team to determine if it is malicious, and the user advised of action.

Device and Internal Network Security

All CANI devices are encrypted, while patch management automatically applies patches and minimizes the risk of out-of-date devices.

All devices have commercial anti-virus installed. Benefits include blocking malicious apps, data loss prevention, exploits prevention and malicious traffic detection.

All device-based content is backed up in the cloud.

Internet Systems Security

At installation level, all sites are 'https'

Back-end users of our websites have limited access defined by role.