CYBERSECURITY POLICY

REVIEWED, APPROVED

& ADOPTED BY

FLINT TOWN COUNCIL

ON 19th JUNE 2023

CYBERSECURITY POLICY

Why is cybersecurity so important?

The world we inhabit is changing rapidly. Many people rely on the internet for everyday interactions and transactions. Local Councils are using an increasing range of technology, from apps and the cloud, to multiple devices and gadgets.
The level of threat varies across Councils, but all possess information or infrastructure of interest to malicious cyber attackers. Cybersecurity is crucial to ensure that services are kept up and running. It is also vital in ensuring the public trust Councils with their information. A cyber attack can have very serious consequences both in terms of disrupting services and damaging a Council's reputation.

Types of threat

Cybercriminals are generally working for financial gain. Key tools and methods include:
* Malware – malicious software that includes, viruses, trojans, worms or code that could have an adverse impact on an organisation.
* Ransomware – these lock victims out of their data or systems and only allow access once money is paid.
* Phishing – emails purporting to come from a public agency to extract sensitive information from members of the public.
* Hacktivism – hacktivists will generally take over websites or social media accounts to raise the profile of a particular cause.
* Insiders – staff may intentionally or unintentionally release sensitive information or data into the public domain. This may not always be malicious, and more often than not is down to human error or a lack of awareness of the risks involved.
* Other threats – physical e.g.fire or water damage to equipment, terrorists, and espionage.

Protection Measures

The Council's response to cybersecurity should be appropriate and proportionate to its size and scale and the type of information it holds.
The Council has introduced the following protection measures designed to mitigate its risk from its systems being subjected to a potential attack:
Antivirus, antimalware, and encryption software.

Device and network firewalls to block unauthorised external access to systems.
Password protection on all devices.
* Back up facility for the Council's data.
* Enhanced email spam filters / anti-spoofing controls.
* Council staff machines run Windows 11 and the council is subscribed to Microsoft 365 Business Standard, including Azure Active directory for user management.

Automatic software updates of key applications are enabled, and regular servicing of ICT equipment covers any other updates.

* Multiple wireless networks providing, each providing access only to what is required.
* Staff keep laptops securely locked when away from their desks.

Staff and Councillor responsibilities

Employees of the council and serving councillors are not to divulge their user credentials to anyone, including family members, unless with the strict approval from the Town Clerk.

Employees of the Council and serving Councillors are not to leave unlocked devices unattended.

Employees of the Council and serving Councillors should be mindful of the risks involved with cybersecurity and should not share any private data or information to any third party. They should be satisfied that any websites visited while browsing the internet on Council devices are legal and safe to use.

The Town Clerk will routinely remind staff about never leaving their computers unlocked and will share on cybersecurity awareness information as appropriate to keep abreast of the latest advice and guidelines.

Professional Support

This policy has been reviewed and endorsed by the Council's third party ICT support provider.