Plaistow and Ifold Parish Council Cyber Security Policy

Introduction

Plaistow and Ifold Parish Council (the council) cyber security policy outlines our guidelines and provisions for preserving the security of our data and technology infrastructure.

The council has a collective responsibility to see that suitable cyber security measures are implemented and supported, and all members of the council must follow good practices to keep their own systems safe.

Everyone, from our staff, Councillors, and residents, should feel that their data is safe. The only way to gain their trust is to proactively protect our systems and databases. We can all contribute to this by being vigilant and keeping cyber security top of mind.

For this reason, we have implemented several security measures. We have also prepared instructions that may help mitigate security risks. We have outlined both provisions in this policy.

This policy applies to all our employees, Councillors, volunteers, and anyone who has permanent or temporary access to our systems and hardware.

Parish Councils are not required to have their own Data Protection Officer. xxxxxx acts as the Data Protection officer for Plaistow and Ifold Parish Council.

Understanding Cyber Security

Cyber security is the protection of computer systems including phones and other digital devices from unauthorised access, theft, damage or being made inaccessible from digital attacks.

Also known as information technology (IT) security. Cyber security measures are designed to combat threats against network systems and applications, whether those threats originate from inside or outside of an organization.

Information Security is defined as the preservation of:

- Confidentiality: protecting information from unauthorised access and disclosure.
- Integrity: safeguarding its accuracy and completeness.
- Availability: ensuring that information is available to authorised users when required

Information exists in many forms. It may be on paper, stored electronically, transmitted over a network, viewed in videos or films, or spoken in conversation. Whatever its form, or medium, appropriate protection is required to ensure its continuity and to avoid breaches of the law, statutory, regulatory, or contractual obligations.

Policy elements

Digital Devices

When staff/Councillors etc. use their digital devices to access council emails, software, or accounts, they introduce security risk to our data. We advise our staff and Councillors to keep both their personal and company-issued computer, tablet, and cell phone secure. They can do this if they:

- Keep all devices password protected.
- Choose and upgrade a complete antivirus software.
- Ensure they do not leave their devices exposed or unattended.
- Install security updates of browsers and systems monthly or as soon as updates are available.
- Log into Council accounts, software, and systems through secure and private networks only.

We also advise our staff and Councillors to avoid accessing internal systems and accounts from other people's devices or lending their own devices to others.

Members and staff conducting Council business on their own personal equipment have a responsibility to follow established Good Practice to protect against malicious software and unauthorised external access to networks and systems. Information should be regularly backed up. They should follow these instructions to protect their devices and refer to WSALC via the Clerk if they have any questions.

Email safety

Emails often host scams and malicious software. To avoid virus infection or data theft, we instruct staff/Councillors to:

- Avoid opening attachments and clicking on links when the content is not adequately explained.
- Be suspicious of clickbait titles (e.g., offering prizes, advice.)
- Check email and names of people they received a message from to ensure they are legitimate.
- Look for inconsistencies or give-aways (e.g., grammar mistakes, capital letters, excessive number of exclamation marks.)

If you are not sure that an email you received is safe, they can refer to our Clerk or Chair for advice.

Password security

Password leaks are dangerous since they can compromise our entire infrastructure. Not only should passwords be secure so they won't be easily hacked, but they should also remain secret. For this reason, we advise our staff, Councillors and volunteers and others covered by this policy and guidance to:

- Choose passwords with at least eight characters (including capital and lower-case letters, numbers and symbols) and avoid information that can be easily guessed (e.g. birthdays.)
- Remember passwords instead of writing them down. If they need to write down a password, they are obliged to keep the paper or digital document confidential and destroy it when their work is done.
- Exchange credentials only when necessary. When exchanging them in-person isn't possible, employees should prefer the phone instead of email, and only if they personally recognize the person they are talking to.

Users must take full responsibility for updating their Council email and other council login passwords and take immediate action by changing their all passwords if they suspect any has been compromised.

Transfer data

Transferring data introduces security risk. Staff and Councillors must:

- Avoid transferring sensitive data (e.g. staff records) to other devices or accounts unless absolutely necessary.
- Only share confidential data over a secure network and not over public Wi-Fi.
- Ensure that the recipients of the data are properly authorised people or organisations and that they have adequate security policies.
- Report scams, privacy breaches and hacking attempts

Local councils are responsible for the information they hold, whether in electronic form, on paper, or in any other format. Stored information must be protected from unauthorised access, accidental deletion, and malicious hacking attempts, so we need to know about scams, so we can better protect our infrastructure. All Council members should report immediately to the Clerk, or to the Chair any observed or suspected security incidents where a breach of the Council's security policies has occurred or any security weaknesses or threats to, systems or services, and any Software malfunctions.

Remote Working

Staff working remotely must follow this policy's instructions too. Since they will be accessing our council accounts and systems from a distance, they are obliged to follow all data encryption, protection standards and settings, and ensure their private network is secure.

Privacy of Information

Protection of Personal Information

The council is a public body and will seek to carry out its business in a public and transparent way. Much of its business is conducted in meetings open to the public. All information given at a public meeting of the council is in the public domain, and is likely to appear in the minutes and may be reported by the press. The Council publishes many of its documents on its website. Although the Council owns some IT equipment, this is limited, and much business (principally by email) is conducted on Members' personal devices.

The council may hold and use information about employees, Councillors, members of the public, and other data subjects for essential administrative and business purposes. When handling such information, the Council, must comply with the Data Protection Principles which are set out in the General Data Protection Regulation (GDPR).

Confidential Data

Confidential data is secret and valuable. The council is committed in ensuring that it is safe and secure. This will be done by safeguarding the confidentiality and integrity of Parish council records and data, and by protecting the services we provided to the residents, so we can always maintain them.

Additional measures

To reduce the likelihood of security breaches, we also instruct all persons with access to our systems to:

- Turn off their screens and lock their devices when leaving their desks.
- Report stolen or damaged equipment as soon as possible.
- Change all account passwords at once when a device is stolen.
- Report to the Communications Advisory Group and Clerk a perceived threat or possible security weakness in any software systems. The Clerk will report to xxxxx who acts as our Data Protection Officer
- Refrain from downloading suspicious, unauthorized, or illegal software on their equipment.
- Avoid accessing suspicious websites.

The Council will:

- Install firewalls, anti-malware software and access authentication systems.
- Arrange for security training to all office employees.
- Inform staff/Councillors regularly about new scam emails or viruses and ways to

combat them.

- Investigate security breaches thoroughly.
- Follow this policy's provisions.