CAISTER-ON-SEA PARISH COUNCIL
The Council Hall
1 Yarmouth Road
Caister-On-Sea
Norfolk
NR30 5DL

Cyber Security Policy

Policy Brief and Purpose

Caister-On-Sea Parish Council cyber security policy outlines the guidelines and provisions for preserving the security of it's data and technology infrastructure.

The Council has a collective responsibility to ensure 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, including 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. Everyone can contribute to this by being vigilant and keeping cyber security in mind.

For this reason, Caister-On-Sea Parish Council have implemented security measures and prepared advice which may help mitigate security risks. These are outlined in this policy.

Scope

This policy applies to all staff, councillors, volunteers, and anyone who has permanent or temporary access to Council systems and hardware.

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 organisation.

Information Security is defined as the preservation of:

- Confidentiality: protecting information from unauthorised access and disclosure;
- Integrity: safeguarding its accuracy and completeness; and
- 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.

Protect Personal and Company Devices

When staff and councillors use their digital devices to access Council emails or accounts, they introduce a security risk to the Council's data.

Caister-On-Sea Parish Council advise their staff and councillors to keep both their personal and company-issued computer/mobile phone secure. This can be achieved by:

- Keeping all devices password protected;
- Choosing and updating antivirus software;
- Ensuring devices are not left exposed or unattended;
- Installing security updates as soon as updates are available; and
- Logging into Council accounts, software, and systems through secure and private networks only.

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

Keeping Emails Safe

Emails often host host scams and malicious software. To avoid virus infection or data theft, Caister-On-Sea Parish Council advises staff 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 the email address and name of the sender to ensure they are legitimate; and
- Look for inconsistencies or giveaways (e.g. grammar mistakes, capital letters, excessive number of exclamation marks.)

Manage Passwords Properly

Password leaks are dangerous as they can compromise Caister-On-Sea Parish Council's entire infrastructure. Not only should passwords be secure, so they won't be easily hacked, but they should also remain confidential.

For this reason, the Council advise staff and councillors 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 staff 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, staff should prefer the phone instead of email, and only if they personally recognise the person they are talking to; and
- Change their passwords every two months.

Users must take full responsibility for updating their password and take immediate action by changing their password if they suspect it has been compromised.

Transfer Data Securely

Transferring data introduces security risk. Staff and councillors must:

- Avoid transferring sensitive data (e.g. personal information, staff records) to other devices or accounts unless absolutely necessary;
- Share confidential data over the Council network/ system and not over public Wi-Fi or private connection;
- Ensure that the recipients of the data are properly authorised people or organisations and have adequate security policies; and
- Report scams, privacy breaches and hacking attempts.

Caister-On-Sea Parish Council is 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. All staff and Council members should report immediately to the Clerk or 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 also follow the guidance laid out in this policy. Since they will be accessing Council accounts and systems remotely, they are obliged to follow all data encryption, protection standards and settings, and ensure their private network is secure.

Additional Measures

To reduce the likelihood of security breaches, Caister-On-Sea Parish Council also advise staff 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 if a device is stolen;
- Report a perceived threat or possible security weakness in company systems;
- Refrain from downloading suspicious, unauthorised or illegal software on their company equipment; and
- Avoid accessing suspicious websites.

Review

Within 3 years, or as appropriate, the Council will review and update this policy.

Date of Policy	March 2025
Approving Committee	Full Council
Date of Committee Meeting	31 March 2025
Date of Adoption by Full Council	31 March 2025
Policy Version Number	1

Date of Next Review	March 2028

Signed: _____ Chair, Caister-On-Sea Parish Council

Date: _____