



**EAST WOODHAY PARISH COUNCIL
IT/CYBER SECURITY POLICY
Approved October 2025
Next Review Date: May 2027**

Background to this policy:

In order to ensure compliance with all applicable laws and to minimise the potential risk for cyber related issues, East Woodhay Parish Council (the council) has adopted an IT/cyber security policy. This should be read in conjunction with our Data Protection policy and Councillor Code of Conduct. The term 'council member' used in this policy includes staff as well as councillors.

As of April 2025, the Smaller Authorities' Proper Practices Panel (SAPPP) has released the updated [*2025 edition of the Practitioners' Guide*](#) to include, what is referred to as 'Assertion 10'. Parish councils are expected to comply with 'Assertion 10', and to demonstrate compliance it has also been added to the *Annual Governance and Accountability Return (AGAR)* for smaller authorities starting from the 2025/26 financial year. In summary, and relating to this policy, this encompasses the following.

- Council-Owned Domain:

Councils must use their own domain-based email addresses and have an official website with a council-owned domain, not a generic address.

- Website Accessibility:

The council's website must meet accessibility regulations, (WCAG 2.2 AA standards), to ensure it can be used by people with disabilities.

- IT Policy:

Councils need to have an IT policy in place that covers various digital and data-related aspects, ensuring secure and proper data handling and use.

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. Appropriate protection and actions are therefore required to minimise the risk and to avoid breaches of the law, statutory, regulatory, or contractual obligations.

The council's adherence to Assertion 10 and cyber security is described in the detail below.

The council's approach to IT and Cyber Security:

The council does not have its own network. To help to minimise the cyber security risk, the council only uses industry standard internet-based systems.

The systems currently in use are listed below along with their purpose:

- Scribe (financial accounting)
- Online banking systems
- HugoFox (council public website information). The council uses its own domain name (www.eastwoodhay-pc.gov.uk) and its use conforms to WCAG 2.2 AA standards.
- AXIS (CCTV) which is administered by a specialist third party.
- Facebook and Instagram (social media)

Only specified council members are authorised to have either update or read access to the above systems.

In addition, the council uses:

- Dropbox (data storage)
- .gov.uk email (specifically @eastwoodhay-pc.co.uk which is hosted on Spacemail and administered by HugoFox)

Council members and staff use personal devices (phones, PCs, Laptops...) to access all the above, except CCTV. Council members must not store council sensitive, confidential or unique data on personal devices (see Data Protection Policy).

There is also a council-owned computer which is kept at the home of an assigned member of the council. Its sole use is to access the CCTV system.

Cyber Security risks:

1. Financial and banking system is hacked.
Potential issue: Financial loss, access is altered, information is altered, data is lost.
2. Website is hacked.
Potential issue: Access is altered, information is altered, data is lost.
3. Social media is hacked.
Potential issue: Access is altered, information is altered, data is lost.
4. CCTV data is hacked.
Potential Issue: Access is altered, data is lost.
5. Email accounts are hacked.
Potential issue: Email is used for misuse
6. Data storage system.
Potential issue: Information is altered, data is lost,

Actions to minimise cyber risks:

1. Financial and banking systems
 - Two factor access authentication must be used. Passwords must follow rules outlined below.

- More than one person must have access to the systems in case an individual cannot access those systems.
 - Financial data is also stored via paper which would enable emergency recovery.
 - Regular financial reconciliation checks are made including that between the banking system and the financial system.
2. Website:
Telephone support is provided via the system owner. Data is also maintained on the data storage system.
3. Social media:
Support is provided via the system owners. No unique data is contained on social media.
4. CCTV
Telephone and access support is provided by the system owner. The PC is solely used to access CCTV and not used to for any other application. Two factor access security is used. Access recovery is via phone.
5. Email
The hosting platform Spacemail uses a spam filter, which is to protect users from unwanted and malicious emails like phishing, malware, and viruses by utilising the industry standard built in service, Jellyfish.
Council members are instructed to use password rules outlined below. To minimise the potential for the email account to be compromised email safety rules should also be followed (see below). If the email account is compromised, then the council member must inform the Clerk or Chair and the password changed immediately.
6. Data storage facility
Multiple accounts can access the system to prevent a single point of failure. The council uses a system which contains historic backup/recovery whereby any data loss or can be restored.

General:

Email safety

Emails often host scams and malicious software. To avoid virus infection or data theft, staff/councillors should:

- 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.).

Password security rules

- Must be at least eight characters using random sequences (including capital and lower-case letters, numbers and symbols).
- Passwords should not be stored anywhere physical.
- Not shared between individuals.