



GREAT BEDWYN PARISH COUNCIL INFORMATION TECHNOLOGY POLICY.V3

The purpose of this policy is to set out the parameters on how council staff should use the technology that the council provide them with in order to do their job.

It is designed to raise awareness of the risks associated with using IT and can protect the council from loss of data. This policy clarifies acceptable and non-acceptable use and what will happen if the policy is breached.

As an employer the council has the right to monitor work use of IT equipment provided that there is a legitimate reason and that you tell staff that you might do this.

- **Who does the policy apply to.**

This policy applies to all members of staff and all Cllrs, Contractors and volunteers who may have cause to use any council owned IT equipment.

- **What communications and IT equipment does the policy cover.**

All laptops owned by the council, data, software, internet access, email services, smart phones, other devices and mobile phones owned by the council, and printers owned by the council.

- **Who is responsible for monitoring and reviewing the policy.**

The Clerk will review the policy once every 12 months and bring the policy to Full Council for approval. The Clerk is responsible for making sure members of staff understand this policy and adhere to it.

- **Related policies.**

This policy should be used in relation to the Disciplinary Rules, Data Protection Policy, Social Media and Communications and Equality and Diversity Policy.

- **Monitoring.**

The council does not routinely monitor the use of internet, email or work telephones of its employees. If it was felt that this was required due to suspicions of illegal/illicit activity, mis-use of council resources or theft or fraud etc, the council will determine at a council meeting who will monitor the internet, email or work telephone and how this would be administered. The council accepts that occasional personal use of council equipment or IT may be required. Staff will be made aware if any monitoring is to take place.

- **Passwords**

There is no standard requirement for council staff to share passwords or disclose them to others.

If council staff identify a need to share passwords then all parties must ensure that the passwords are securely shared and stored.

Council staff will share access codes to other staff members laptops to cover unexpected illness or holiday lasting over 1 week where there is the need for a laptop to be passed to another member of staff.

If a member of staff believe someone has fraudulently accessed their passwords or other secure council data they should immediately seek to change the passwords.

The Clerk will make sure the council is advised of any such occurrences.

Passwords should be no less than 8 characters in length and include upper and lower case characters and at least 1 number.

Laptop PIN's will be set in length by the manufacturer and so are not subject to change.

If password protected documents are shared then the passwords should be shared via a separate medium such as a phone call.

- **Computer usage**

Laptops should be closed down at the end of every working day and put in a location where they cannot easily be seen or accessed.

All documents should be saved on laptops in a location that is backed up.

There should be no need to bring personal IT equipment and use them for work purposes unless the council does not provide the hardware for your role. Any deviations to this should be discussed with the Clerk, and Chairman of the council.

- **Data Protection**

Council staff will follow the principles of data protection and GDPR when processing personal data. Data is only to be used for the purpose intended and deleted once it is no longer required or relevant. Data will not be disclosed to others unless there is a valid business reason demonstrated.

Council staff will consider the validity of sharing any personal data and check beforehand if there is any doubt. Documents with personal data will be password protected and the password only shared with those who need to access the data.

- **Mobile phone texting/WhatsApp**

Whilst not often used, it will be remembered that text/WhatsApp messages should be treated the same as any other council communication if suppliers or members of the public etc are contacted using one of these methods.

- **Email**

Emails should be friendly but formal and ensure that there is no opportunity for suppliers believing that they have entered into an agreement with the council by staff inadvertently stating as such with a poorly worded email. Any unexpected email attachments or those from unverified sources should be checked prior to opening. If in doubt do not open and contact the sender to verify the validity of the attachment. Information that could be classed as confidential or sensitive should only be transferred to another party with suitable IT protection in place.
- **Internet**

The internet at the council premises should be used for work purposes only. No documents or files should be downloaded from the internet on to staff laptops without determining that the source is reliable and virus free.
- **Software**

Only verified & authorised software should be downloaded onto council owned laptops. Staff should check first if they are unsure.
- **Training**

Staff and Cllrs will be sent information on any major changes or updates to IT security as they occur and will encourage Cllrs and staff to attend relevant industry training that is available.
- **Misuse**

Misuse of IT facilities can potentially result in disciplinary proceedings. This can include not adhering to the policy; attempting to discover a user's password; using the computer systems to act abusively; attempting to circumvent the network's security; knowingly running and installing programmes intended to damage the computer systems; deliberately wasting computer resources; leaving laptops unattended in a public place etc.
- **Use of AI for work purposes.**

Council staff may use AI to assist with writing of documents or emails as part of their work, however all use of AI produced text should first be thoroughly read by the staff member before sending/using. All externally quoted sources or legislation should be checked for accuracy

- **Website compliance.**

The Councils website, www.greatbedwyn-pc.gov.uk should always meet the current compliance levels (Currently WCAG2.2 AA) and the Clerk will ensure that website providers adhere to this and bring the matter to the relevant council meeting should updates be required that need council approval.

- **Actions after a data breach.**

If a Cllr or member of staff discover a breach of council data such as malware, phishing or other scams they must immediately report this to the Parish Clerk. The Clerk will talk to the council Chairman about the required actions to take. The Clerk will contact the councils email provider to change passwords on Cllr and staff email addresses and this will be done straight away if required or the email account will temporarily be suspended from use. Any infected devices whether council or personally owned should not be used until the source of the breach has been identified and resolved. External sources will be brought in to resolve issues if needs be, using the delegated powers for H&S matters to pay for services if required.

- **Using personal email addresses for council business.**

Cllrs and members of staff should NOT use personal email addresses for council business (Google mail, Outlook or Hotmail etc) This type of account is not secure and is vulnerable to attack and is no longer compliant with current legislation.

- **Access to council data rescinded.**

Once a Cllr or member of staff leaves the council the Clerk is responsible for immediately blocking access to their email account. Once a period of 6 months has passed, the Clerk will delete the email account. This is to ensure that important data is not lost that may need to be retrieved.

- Data will be kept in accordance to our Data Protection Policy. Councillors and staff are signposted to this policy for further information.

Created July 2025. V2

Approved at.....July 2025 full council Meeting

Date 10th July 2025

Minute reference...969.25 – 27

AMENDED Oct 25 V2 – “Actions after data breach”, “website compliance”, “Using personal email addresses” and “Access to council data rescinded” sections added.

Approved at.....October 2025 full council Meeting

Date 16th October 2025

Minute reference 1028.25 - 20

Updated and approved at Feb 2026 full council meeting. Minute ref. 1117.25 - 20