Iwerne Minster Parish Council

Data and Cyber Security Policy

(Amended 9th January 2023)

This document specified the steps that must be taken by councillors, officers and employees to limit the risk and impact of a data or cyber security breach.

Failure to abide by the provisions of this policy will be considered as a breach of the Code of Conduct for Councillors.

1. Council's data processing facilities:

Iwerne Minster Parish Council owns the following IT systems.

- Acer laptop used by the Clerk.
- Hard drive and USB stick, which are used for back up.

There is no internal network or server, or remote access.

Email and office app facilities are provided using Microsoft Office / Outlook 365, to which the clerk has administrative access. The login details are kept in a locked cabinet and a copy will also be held by the Chairman.

2. Councillors' IT systems

- Councillors are recommended to use Microsoft 365, or other appropriate systems but do not use cloud software for private and confidential information.
- Councillors to be issued email addresses, which are to be used just for Parish Council communications.
- Councillors are recommended to save their works on a separate USB or Hard Drive and have these in a secure place. Once saved all originals will be deleted from personal systems.
- Councillors' devices should be protected by antivirus software systems.

2.a Physical Media.

The following are stored at the Parish Council's Clerks office/home.

- Signed copies of minutes.
- Signed bank reconciliations.
- Signed declarations of office.
- Clerk's contract.
- Bank statements.

(All of the above are kept in a locked filing cabinet)

Councillors may print council document for their own personal use.

3. Policy for use of IT devices.

The following applies to all devices used to store council files and/or emails, whether owned by councillors, officers or employees, unless otherwise stated:

- Passwords – all devices shall be protected by a password containing up to eight characters, including an uppercase letter, lowercase letter and a number. (Some computer systems only require number logins); OR
- A local PIN that is not easily guessable; OR
- Fingerprint, retina or face recognition.
- Beware of using any open wi-fi system, ensure it is secure.

Council-owned device storage.

When not in use, such devices must be kept in either:
- A locked building where there is no public access (e.g. the clerk's home); and
- Where there is public access, in a locked container (e.g. a filing cabinet) in a room locked when not in use.

3.a Microsoft 365 password:

- All Microsoft accounts must be protected by a password conforming to the rules specified in 3.1 above.

3.b Updates:

- All updates to operating systems, security software, and applications used for council work must be updated as soon as reasonably practical after they are made available by the manufacturer once the Parish Clerk confirms the new software is secure.

3.c Security software:

- Firewalls must be used where available. For Windows 10 devices Defender must be used, and for all devices with Windows operating systems earlier than Windows 10, effective antivirus software must be installed and used.
- Should any Parish Councillor wish to use an alternative anti-virus program this must be approved by the Clerk first.

3.d Encryption:

- Unless permanently stored in a dwelling that is locked when not in use (e.g. a councillor's or officer's home), all devices used to store council files and/or emails must as a minimum have this data encrypted.

Android devices:

- Those running v4.4 or above are automatically encrypted
- Those running below v4.4 must not be used for council data unless they are shown to be encrypted.

Apple devices:

- Encryption is standard in all versions.
- For Mac devices File Vault disk encryption must be turned on as detailed in the Appendix of the Apple Mac document.

Windows devices

- Devices running Windows XP or below must not be used for council data.

- Devices running versions of Windows with BitLocker available (e.g. Windows 8 or 10 Pro and Enterprise) must be encrypted using BitLocker.
- Devices running versions of Windows without BitLocker must use VeraCrypt or a similar third party package to encrypt ideally the whole device but as a minimum all council files and emails.

If in any doubt, councillors and officers must ask the clerk for advice.

3.e Data held on Microsoft 365:

- When a councillor ceases to be member of the council, the Councillor's council email account will be immediately suspended and then deleted when no further access to the data is required by the council, usually within 30 days.
- When an officer ceases to be employed by the council, access to the Parish Council's email account will be removed. Access to the account will usually be given to their replacement or another officer.

3.f Removing council data from devices:

- When a councillor ceases to be a member or an officer ceases to be employed, they must remove all council data from all their devices. Similarly, when a councillor or officer no longer uses a device for council business, all council data on that device must be removed.

Data removal must be by either:

- physical destruction of the data storage, or
- wiping with a suitable utility.
- In addition, council data must be permanently deleted on any associated cloud storage (other than the council's Microsoft 365 system).
- If required by the council or the clerk, the councillor or officer must inform the Clerk in writing that all data has been removed from their personal device and hard copies passed over to the Clerk or the new officer responsible for the relevant role.

4. HR documents.

- All current HR documents must be stored in a secure folder or USB/Hard Drive to which only the Clerk and Chairman have access. Any HR documents that must be maintained on paper must be stored securely by the Clerk as described in paragraph 5 below.

5. Physical media.

Any physical media concerning council business (e.g. paper documents printed by or in the possession of councillors or officers) other than public documents must be:

- When not stored in a dwelling that is locked when not in use (e.g. a councillor's or officer's home), kept in a locked container, e.g. a filing cabinet, and
- Must be shredded as soon as they have been used for the purpose for which they were produced.

Note: Theft or loss of any IT device containing council files and/or emails, or any loss of physical media concerning council business must be reported as a Data Breach.