**Barkway Parish Council – IT and Information Security Policy**

**1. Purpose**

This policy sets out how Barkway Parish Council will protect its information and IT systems, ensuring that information is:

- kept secure and confidential where appropriate
- accurate and reliable
- available when required

The Council recognises its responsibilities under the UK General Data Protection Regulation and the Data Protection Act 2018.

**2. Scope**

This policy applies to:

- the Clerk
- all councillors
- any devices used to access or process council information

**3. Responsibilities**

- The **Clerk** is responsible for day-to-day management of council information and systems.
- Councillors are responsible for handling council information securely and in accordance with this policy.

**4. Use of IT Systems**

- The Council uses Microsoft 365 as its primary system for storing and managing documents.
- The version of any document held within the Council's official systems is the **authoritative record**.
- Draft documents may be created on personal devices but should be transferred to the Council's systems when they become part of official business.

**5. Use of Personal Devices**

- Councillors may use personal devices for council business.

- Reasonable precautions must be taken, including:
    - use of passwords or device security
    - avoiding use of shared or public computers
    - ensuring devices are not left unattended in public places
- Where personal data is involved, councillors should avoid retaining unnecessary copies on personal devices and should transfer documents to the Council's systems, or to the Clerk, once they form part of official business.

**6. Data Storage and Backup**

- Council data is stored within Microsoft 365 and benefits from its built-in backup and recovery features.
- The Council does not rely on councillors' personal devices for long-term storage of official records.

**7. Data Handling**

- Personal data will be handled in accordance with data protection legislation.
- Only necessary data will be retained, and duplication will be minimised where possible.

**8. Disposal of Equipment and Media**

- All IT equipment will be securely wiped or reset before disposal to ensure that no data can be recovered.
- Equipment will be disposed of through appropriate recycling routes in compliance with WEEE regulations.
- Storage media (e.g. USB drives) will be securely wiped or physically destroyed before disposal and will not be placed in general waste.
- Disposal of equipment will be recorded in the Council's asset register or minutes.

**9. Physical Security**

- Devices containing council information should be kept secure and not left unattended in public places.
- Paper documents containing sensitive information should be stored securely when not in use.

**10. Incident Reporting**

- Any suspected loss of data, breach of security, or unauthorised access must be reported to the Clerk as soon as possible.
- The Clerk will assess whether further action is required.

**11. Review**

This policy will be reviewed annually or when there are significant changes to the Council's systems or legal requirements.

**Adopted: 16th June 2026**

**Review: March 2027**