

LEWKNOR PARISH COUNCIL — IT AND DATA SECURITY POLICY

1. Purpose

1.1 This policy protects the Council's information and equipment, and sets out acceptable use. It is deliberately proportionate to a small council whose IT is provided and secured mainly by established suppliers.

2. How the Council's IT is provided

2.1 **Devices.** *One Parish Council laptop, managed by the Clerk*

2.2 **Data storage and email.** *Microsoft 365 on Council laptop, all email addresses managed by Parish Online and are @lewknorparishcouncil.gov.uk*

2.3 **Accounting.** *Scribe*

2.4 **Website.** *Parish Online*

2.5 *Parish mobile under a Tesco contract*

3. Responsibilities

3.1 **LEWKNOR** maintains device security (updates, anti-virus) and provides support.

3.2 **The Clerk/RFO** operates the Council's systems day to day, controls access, and is the point of contact with the IT provider, the cloud service and the website provider.

3.3 **The website provider** maintains the security and accessibility of the website.

3.4 **Councillors and the Clerk** follow this policy when using Council systems and data.

4. Access and passwords

4.1 Accounts are individual to each user; passwords are strong and are **not shared**.

4.2 **Multi-factor authentication** is enabled on the Council's email and document systems, and on other systems where it is available.

4.3 Access is granted on a least-privilege basis and is removed promptly when a person leaves office or employment.

5. Acceptable use

5.1 Council equipment and accounts are used for Council business. Reasonable incidental personal use is permitted provided it does not compromise security or bring the Council into disrepute.

5.2 Users do not install unauthorised software, disable security controls, or open suspicious links or attachments; anything suspicious is reported to the Clerk (and the IT provider) promptly.

5.3 Council data is not stored on personal devices or personal accounts except where necessary and secured; where a Council laptop is kept at the Clerk's home, it is recorded in the asset register and remains subject to this policy.

6. Data security and back-up

6.1 Personal and sensitive information is held within the Council's cloud services, which provide access control and back-up; it is not left on unsecured local storage or removable media.

6.2 The Council relies on the cloud providers' back-up, supplemented by device management, so that records can be recovered after loss or hardware failure.

6.3 Paper records containing personal data are held securely and disposed of by shredding.

7. Loss, theft or breach

7.1 A lost or stolen device, or a suspected security incident, is reported **immediately** to the Clerk and to the IT provider so that access can be revoked and the device remotely secured where possible.

7.2 Any incident involving personal data is handled under the Data Protection Policy (including the 72-hour reporting duty where the breach is reportable).

8. Leaving office or employment

8.1 On leaving, a person returns Council equipment, and their access to email, document storage, the accounting system and any other system is removed promptly.

9. Review

9.1 This policy is reviewed by the Council at least every two years, and whenever the Council's IT arrangements change materially.

Adopted by Lewknor Parish Council on: _____ 14th September 2026 _____ (date)

Minute reference: _____ 7(c) _____

This IT and Data Security Policy will be reviewed in two years, unless circumstances dictate otherwise.