Potterne Parish Council
Information Technology Protection Policy

Effective date:	June 2026	**Review due:**	June 2027
		Last reviewed:	New Policy
Author & responsible officer:	Clerk to Potterne Parish Council		
Status	Approved	**Version:**	1.0

1. This policy defines the acceptable use of all IT equipment and associated facilities within Potterne Parish Council. Its primary goal is to mitigate risks such as data loss, system outages from malware, financial loss, and legal issues. This policy applies to all staff, contractors, and visitors using Council-owned or leased technology. Failure to comply may lead to the withdrawal of IT facilities or disciplinary action.

2. Individual Responsibility

Access to PPC systems is controlled through User IDs, passwords, and Multi-Factor Authentication (MFA). Individuals are accountable for all actions performed under their unique identity.

·Do not share User IDs, passwords, PINs, or MFA tokens with anyone (except authorised IT support).

·Lock your device whenever it is unattended (Windows Key + L for computers; power button for mobile devices).

·Do not interrogate data or systems beyond your specific business need or authorised role.

·Council data must only be stored on authorised equipment; transferring data to personal cloud accounts or external organisations without authority is prohibited.

3. Information Security & Access Control

Information should be classified to ensure proper handling:

·PUBLIC: Approved for website or public release.

·INTERNAL: Routine business; not for external distribution.

·CONFIDENTIAL: Personal or commercially sensitive data. These must be labelled and encrypted both at rest and in transit.

Access is granted based on the principle of least privilege, ensuring users only see what is necessary for their role. Access reviews will occur annually, with the main user system reviewed every 90 days.

4. Passwords & Authentication

·Passwords must be at least 6 characters long, including at least one number, one symbol, and one capital letter.

·Passwords must be changed every 90 days.

·Multi-Factor Authentication (MFA) or Passkeys must be used if available.

·Passwords must remain confidential and never be written down or displayed when entered.

5. Working Remotely & Flexible Working

When working from home or in public areas:

·Do not access sensitive information in public if the screen is visible to others.
·Keep equipment and files locked out of sight during transit.
·Ensure family members or visitors cannot access Council equipment or data.

6. Prohibited Activities

The following activities are strictly prohibited:
·Sending offensive, pornographic, discriminatory, or illegal material.
·Using Council IT for personal business or personal financial gain.
·Connecting unauthorised devices to Council networks or using unsecured, open Wi-Fi hotspots.
·Downloading or distributing unauthorised software.
·Bypassing security measures or attempting to gain unauthorised access to data.

7. Personal Use of Council IT

While not encouraged, limited and reasonable personal use is permitted at the Council's discretion, provided it does not:
·Waste Council time, money, or resources.
·Involve gaming, gambling, share dealing, or commercial activity.
·Store personal photos or data on Council devices.
·Incur excess data charges (e.g., via video streaming).

8. Asset Management

·Software Updates: Users must update their devices with new security patches as soon as reasonably possible.
·Location: Devices should not be moved or used outside the UK without formal approval; login attempts from abroad may be blocked.
·Lost/Stolen Devices: These must be reported to the IT helpdesk immediately so the device can be remotely wiped.
·Returns: All equipment must be returned upon termination of employment or contract.

9. Bring Your Own Device (BYOD)

Staff may use personal devices for Council apps (e.g., Teams, Outlook) with approval.
·Council data remains Council property and cannot be saved directly to the personal device.
·The Council may remotely wipe Council applications if the device is lost, stolen, or if a policy breach occurs.

10. Reporting Breaches

All suspected security breaches must be reported immediately to line management and the IT helpdesk for investigation.