PAKENHAM PARISH COUNCIL

INFORMATION TECHNOLOGY POLICY

Adopted: February 2026

Reviewed: February 2027

Purpose of the IT Policy

The purpose of this IT policy is to establish clear parameters for how Councillors and the Parish Clerk use of council-provided technology or equipment in the course of their duties. A well-defined policy helps to:

- Set expectations for appropriate use of equipment and systems;
- Raise awareness of risks associated with IT use;
- Safeguard the council's data and digital assets;
- Clarify what constitutes acceptable and unacceptable use;
- Outline the consequences of policy breaches.

IT Use

As an IT provider for the Parish Clerk, the Council has the right to monitor the use of its IT equipment provided there is a legitimate reason for doing so and they are informed that such monitoring may take place. Any monitoring must be proportionate and comply with relevant data protection and privacy laws. Councillors may be included if they have access or use council systems e.g. if they have a council e-mail address.

Scope of this policy

This policy applies to the Parish Clerk and Councillors accessing the .gov.uk email address. It sets out the expectations for the appropriate use of IT equipment provided by the Council.

Computer Use

Hardware

- Council computer equipment is provided for Council purposes only. Any personal use of the computer and systems should not interrupt the daily Council work in any way.

- The Parish Clerk must lock the computer when leaving their desk to prevent unauthorised access. This applies to all Council and personal devices used for work. Failure to comply may lead to disciplinary action.

- The Parish Clerk's computer and electronic hardware should be kept clean, and every precaution taken to prevent food and drink being dropped or spilled onto it.

- Equipment should not be dismantled or reassembled without seeking advice and any faults or necessary repairs must be reported to the Council.

- Personal disks, USB stick, CDs, DVDs, data storage devices etc cannot be used on Council computers.

Equipment

Portable equipment

- Portable equipment includes laptop computers, netbooks, tablets, mobile and smart phones with email capability and access to the internet.

- Council back-up procedures specific to portable equipment should be followed at all times.

- All portable computers must be stored safely and securely when working from home.

- It is important to ensure all portable devices are protected with encryption in case they are lost or stolen. All smartphones or tablets that hold Council data, including emails and files, must be protected with a pin code. Where possible, these devices should also be programmed to erase all content after several unsuccessful attempts to break in. Any security set on these devices must not be disenabled or removed.

- If the Clerk's laptop is lost or damaged this should be reported to the Chairman.

- Under no circumstances should any non public meeting or conversation be recorded without the permission of those present. This does not affect statutory rights (under The Openness of Local Government Regulations 2014).

- The Council does not permit webcams (which may be pre-installed on many laptops) to be used in the workplace, other than for conference calls for Council purposes.

Use of own devices

- The Council recognises that some Councillors or the Parish Clerk may wish to use their own smartphones, tablets, laptops etc to read their emails, access documents or access data. Any such use of personal devices will be at their discretion. Such devices should be kept up to date so that any vulnerabilities in the operating system or other software on the device are appropriate or updated.

- Any emails sent from own devices should be sent from a council email account and should not identify the individual's personal email address.

- In cases of legal proceedings against the Council, the Council may need to temporarily take possession of a device, whether Council-owned or personal to retrieve the relevant data.

- Wherever possible the user should maintain a clear separation between the personal data processed on the Council's behalf and that processed for their own personal

use. If the device supports both work and personal profiles, the work profile must always be used for work-related purposes.

- If Councillors or the Parish Clerk intend to use their own devices they must ensure that they use a strong password and Councillors must inform the Clerk if their device(s) is/are lost, stolen, or inappropriately accessed where there is risk of access to Council data or resources.

- Personal data relating to Councillors, staff, associates, residents and external stakeholders should not be saved to any personal accounts with third-party storage cloud service providers as this may breach data protection legislation or create a security risk if the device is lost or stolen. This applies especially if the passwords used to store/access data are saved onto the device.

- Personal information and sensitive data should never be saved on Councillors or the Parish Clerk's own devices as this may breach confidentiality agreements.

- If removable media are used to transfer data (e.g. USB drives or CDs), the user must also securely delete the data on the media once the transfer is complete.

- If transferring data, either by email or by other means, this should be done securely. Unsecured wireless networks should not be used.

- Prior to the disposal of any device that has work data stored on it, and in the event of a user leaving the Council, Councillors should ensure that all passwords, user access shortcuts and any identifiable data are removed from the device.

Health and safety

The Parish Clerk will be provided with an appropriate workstation.

The Council has a duty to ensure that regular appropriate eye tests, carried out by a competent person, are offered to the Parish Clerk using display screen equipment.

If the Parish Clerk's workstation requires changes to make it compliant they must speak to the Chairman.

If any hazards are detected at a workstation, including 'noises' from the laptop, this should be reported immediately to the Chairman.

Passwords – Parish Clerk

- Passwords are personal and must not be shared under any circumstances.
- Only the assigned user of an account may access or use the associated password.
- Administrative credentials must be stored securely and only accessible to authorised personnel with a copy provided to the Chairman, in a sealed envelope, only to be accessed in an emergency.
- Passwords must not be stored in plain text or written down in insecure locations.
- Immediately change a password if compromise is suspected.

- All access to administrative or shared credentials must be logged and auditable.
- Attempts to access unauthorised passwords will be treated as a security incident.
- The Parish Clerk is responsible for creating and maintaining secure passwords for the Council accounts.

Monitoring of Council Laptop

Internet, email, and computer usage is continually monitored by the Parish Clerk as part of the Council's protection against computer viruses, ongoing maintenance of the system, and when investigating faults.

Remote Working

- If logging into the Council's systems or services remotely, using computers that either do not belong to the Council or are not owned by the user, any passwords must not be saved, and the user must log out at the end of the session deleting all logs and history records within the browser used. If the configuration of the devise does not clearly support these actions (for example at an internet café), these should not be accessed from that device.
- Any data printed should be collected and stored securely.
- Papers, files or computer equipment must not be left unattended at a premises unless arrangements have been made with a responsible person at a premises for them to be kept in a locked room or cabinet if they are to be left unattended at any time.
- Any data should be kept safely and should only be disposed of securely.
- Papers, files, data sticks/storage, flash drive or backup hard drives should not be left unattended in cars, except where it is entirely unavoidable for short periods, in which case they must be locked in the boot of the car.
- The use of paid for Wi-Fi access, for example at airports should be carefully monitored and restricted to essential Council use.

Email

Council email facilities are intended to promote effective and speedy communication on work-related matters. Although we encourage the use of email, it can be risky and to be careful not to introduce viruses.

All Councillors who need to use email as part of their role will normally be given their own Council email address and account. The Council may, at any time, withdraw email access, should it feel that this is no longer necessary for the role or that the system is being abused.

Copyright

Much of what appears on the Internet is protected by copyright. Any copying without permission, including electronic copying, is illegal and therefore prohibited. The Copyright, Designs and Patents Act 1988 sets out the rules.

Councillors and the Parish Clerk should not assume that because a document or file is on the Internet, it can be freely copied. There is a difference between information in the 'public

domain' (which is no longer confidential or secret information but is still copyright protected) and information which is not protected by copyright (such as where the author has been dead for more than 70 years).

Usually, a website will contain copyright conditions; these warnings should be read before downloading or copying.

Trademarks, links and data protection

The Council does not permit the registration of any new domain names or trademarks relating to the Council's names or products anywhere in the world. Only the Parish Clerk will add links from any of the Council's web pages to any other external sites.