Information Technology Policy

Bramfield and Thorington Parish Council

Proposed for Adoption March 2026

1. Purpose of this policy

The purpose of this policy is to establish clear parameters for how councillors, staff, and other authorised users use council-provided technology or equipment in the course of their duties.

2. Monitoring of IT Use

As an IT provider, the council has the right to monitor the use of its IT equipment and systems and councillors, employees and other authorised users should be aware that such monitoring may take place without prior notice or consent being sought. Any monitoring will be proportionate and comply with relevant data protection and privacy laws. Other persons may be included if they access or use council systems

3. Scope of this policy

This policy applies to all councillors, staff, and other authorised users, regardless of their working location or pattern, including those who are home-based, office-based, or work on a flexible or part-time basis. It sets out the expectations for the appropriate use of IT equipment and systems provided by the council.

4. Computer use

a. Hardware

- Council computer equipment is provided for council purposes, however reasonable personal use is permitted (with reasonable interpreted as “in the opinion of the Parish Council”). Any personal use of our computers and systems should not interrupt council work in any way.

- All councillors, staff, and other authorised users must secure their computers when working on Council business to prevent unauthorised access. This applies to all council and personal devices used for work.

- All computer and other electronic equipment supplied should be treated with good care at all times. Computer equipment is expensive, and any damage sustained to any equipment will have a financial impact on the council.

- Computer and electronic hardware should be kept clean, and every precaution taken to prevent food and drink being dropped or spilled onto it.
- All computer and mobile equipment will have an entry on the Parish Council Asset Register
- Equipment should not be dismantled or reassembled without seeking advice.
- Councillors, staff, and other authorised are not to purchase any computer or mobile equipment (including software) unless previously authorised.
- External data storage devices should not be used on council computers without the prior approval of the Parish Council.

- Any faults or necessary repairs must be reported to the Chair of the Parish Council.
- All computers must be stored safely and securely
- All devices that hold council data, including emails and files, must be protected, at least with a pin code.
- If an item of computer equipment is lost or damaged this should be reported to the Chair of the Parish Council. If the loss or damage is due to an act of negligence, the individual responsible may be liable to meet some or all of the cost of the loss/damage, as decided by the Parish Council

5. Use of own devices

- The Council recognises that councillors, staff, and other authorised users may be using their own smartphones, tablets, laptops etc to access Council information including, but not limited to, reading their emails, accessing documents stored on the council's website or icloud. Any such use of personal devices will be at the discretion of the council, but consent for standard systems will normally be permitted. Such devices should be kept up to date so that any vulnerabilities in the operating system or other software on the device are appropriately patched or updated.
- The same security precautions apply to personal devices as to the council's desktop equipment. Any emails on Council business sent from own devices should be sent from a council email account
- Councillors, staff, and other authorised persons that use council systems are expected to use all devices in an ethical and respectful manner and in accordance with this policy. Accessing inappropriate websites or services on any device via the IT infrastructure that is paid for or provided by the council carries a high degree of risk, and, for employees, may result in disciplinary action, including summary dismissal (without notice).
- In cases of legal proceedings against the council or Council staff 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, for example, by using different apps for council and personal use. If the device supports both work and personal profiles, the work profile must always be used for work-related purposes.
- Users must inform the Chair of the Parish Council if their device(s) is/are lost, stolen, or inappropriately accessed where there is risk of access to council data or resources.
- Personal information and sensitive data should never be saved on councillors, staff, or other authorised users own devices as this may breach confidentiality agreements, especially if the device is used by other people from time to time.
- If removable media are used to transfer data (e.g. USB drives), the user must also securely delete the data on the media once the transfer is complete.

6. Health and safety

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

7. Password and Authentication Policy

- 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.

- In exceptional cases (e.g., incident response or employee offboarding), access to system credentials may be granted to authorised personnel
- Administrative credentials must be stored securely and only accessible to authorised personnel with a copy provided to the Chair of the Council, 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 password if compromise is suspected.
- Users are responsible for creating and maintaining secure passwords for their accounts.

8. Monitoring

- The council reserves the right to monitor and maintain logs of computer usage and inspect any files stored to ensure compliance with this policy as well as relevant legislation. Internet, email, and computer usage may also be monitored as part of the council's protection against computer viruses, ongoing maintenance of the system, and when investigating faults or complaints
- The council reserves the right to monitor the types of sites being accessed and the extent and frequency of use of the internet at any time, both inside and outside of working hours to ensure that the system is not being abused and to protect the council from potential damage or disrepute.
- Any use that the council considers to be 'improper', either in terms of the content or the amount of time spent on this, may result in disciplinary proceedings.
- All computers will be periodically checked and scanned for unauthorised programmes and viruses.

9. Use of the Internet

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 set out the rules. The copyright laws not only apply to documents but also to software. The infringement of the copyright of another person or organisation could lead to legal action being taken against the council and damages being awarded, as well as disciplinary action, including dismissal, being taken against the perpetrator.

10. Use of social media

Personal use of social networking/media on Council devices should be restricted to breaks during working hours, or after hours with permission

11. Misuse

Misuse of IT systems and equipment is not in line with the council's standards of conduct and will be taken seriously. Any inappropriate or unauthorised use may lead to formal action, including disciplinary proceedings or, in serious cases, dismissal.