



GAMLINGAY PARISH COUNCIL
The Eco Hub
Stocks Lane
Gamlingay
Beds
SG19 3JR
Telephone: 01767 650310
Email: clerk@gamlingay-pc.gov.uk

Gamlingay Parish Council INFORMATION TECHNOLOGY POLICY

PURPOSE OF THE IT POLICY	2
MONITORING OF IT USE	2
SCOPE OF THIS POLICY	2
COMPUTER USE	2
2. EQUIPMENT	2
3. HEALTH AND SAFETY	4
4.PASSWORD AND AUTHENTICATION POLICY	4
5. MONITORING	5
6. REMOTE WORKING	5
7. EMAIL	6
8. USE OF THE INTERNET	6
9. MISUSE	7

Purpose of the IT Policy

The purpose of an IT policy is to establish clear parameters for how councillors, staff, and other authorised users use 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.

Monitoring of IT Use

As an IT provider, the council has the right to monitor the use of its IT equipment and systems, provided there is a legitimate reason for doing so and councillors, employees and other authorised users are informed that such monitoring may take place. Any monitoring must be proportionate and comply with relevant data protection and privacy laws.

Scope of this policy

This policy applies to all councillors, staff, and other authorised users. It sets out the expectations for the appropriate use of IT equipment and systems provided by the council.

Computer use

1. Hardware

Council computer equipment is provided for council purposes, however reasonable personal use is permitted. Any personal use should not interrupt council work in any way.

All computer and other electronic equipment supplied should be treated with good care at all times.

Councillors and staff are not to purchase any computer or mobile equipment (including software) unless previously authorised.

2. Equipment

2.1 Equipment

Equipment includes laptop and desktop computers, netbooks, tablets, mobile and smart phones with email capability and access to the internet etc.

All devices must be stored safely and securely when not in use.

It is important to ensure all 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. Any security set on these devices must not be disabled or removed.

If an item of equipment is lost or damaged this should be reported to the Council.

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).

2.2 Use of own devices

The Council recognises that some councillors, staff, and other authorised users may wish to use their own smartphones, tablets, laptops etc for normal council purposes. Any such use 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 updated.

The same security precautions apply to personal devices as to the council's desktop equipment. Telephone calls made on an official basis must be made on council landlines or mobile phone numbers to ensure that only these numbers are used and/or stored by the recipient, rather than personal numbers. Any official emails sent from own devices should be sent from a council email account and should not identify the individual's personal email address.

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). This is irrespective of the ownership of the device used. An example would be downloading copyright music illegally or accessing pornographic material.

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, 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.

Councillors, staff, and other authorised users who intend to use their own devices via the council's infrastructure must ensure that they:

- use a security feature to protect their device(s) from unauthorised access.
- always password protect any documents containing confidential information
- ensure secure WiFi networks are used;

- ensure that work-related data cannot be viewed or retrieved by family or friends who may use the device;
- 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, and other authorised users, associates, residents, 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, or if the service permits councillors, staff, and other authorised users to remain logged in between sessions.

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 or CDs), the user must also securely delete the data on the media once the transfer is complete.

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, staff, and other authorised users may be required to allow the clerk and/or IT provider access to the device to ensure that all passwords, user access shortcuts and any identifiable data are removed from the device.

Councillors, staff, and other authorised users must take responsibility for understanding how their device(s) work in respect to the above rules if they are accessing council servers/services via their own IT equipment. Risks to the user's personal device(s) include data loss as a result of a crash of the operating system, bugs and viruses, software or hardware failures and programming errors rendering a device inoperable. The council will use reasonable endeavours to assist, but councillors, staff, and other authorised users are personally liable for their own device(s) and for any costs incurred as a result of the above.

3. Health and safety

Councillors, staff, and other authorised users who work in council offices 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 employees using display screen equipment.

4.Password and Authentication Policy

All user accounts must be protected by strong, secure passwords.

In addition to strong passwords, Multi-Factor Authentication (MFA) should be enabled wherever possible. This significantly reduces the risk of unauthorised access to systems and personal data.

To further strengthen account security:

- Initial user account passwords must be generated by the IT provider.
- Default passwords provided by vendors or the IT provider must be changed immediately upon installation or setup.
- Service or System (e.g. Website) account passwords are generated and managed by the IT provider.
- The council recommends these practices as part of its commitment to robust information security and to support compliance with the UK GDPR and the Data Protection Act 2018.

Access to Passwords

- 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 from the IT provider with appropriate approvals and logging.
- Administrative credentials must be stored securely and only accessible to authorised personnel with a copy provided to the chair of council in a sealed envelope, only to be accessed in an emergency.

Password Storage and Management

- 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.

5. Monitoring

The council reserves the right to monitor computer usage and inspect any files stored on its network, servers, computers, or associated technology to ensure compliance with this policy as well as relevant legislation.

Such monitoring and the retrieval of the content of any messages may be for the purposes of checking whether the use of the system is legitimate, to find lost messages or to retrieve messages lost due to computer failure, to assist in the investigation of wrongful acts, or to comply with any legal obligation.

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.

6. Remote working

Increased IT security measures apply to those who work away from their normal place of work as follows:

- 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 device does not clearly support these actions (for example at an internet café), council services should not be accessed from that device;

- the location and direction of the screen should be checked to ensure confidential information is out of view. Steps should be taken to avoid messages being read by other people, including other travellers on public transport etc;
- any data printed should be collected and stored securely;
- papers, files or computer equipment must not be left unattended at any premises
- 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.
- where possible the ability to remotely wipe any mobile devices that process sensitive information should be retained in the case of loss or theft

7. Email

All councillors, staff, and other authorised users 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.

Email messages sent on the council's account are for council use only. Personal use is not permitted.

8. Use of the Internet

8.1 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 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.

The council's policy is to comply with copyright laws.

8.2 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, unless authorised to do so. Nor should they add links from any of the council's web pages to any other external sites without checking first with the clerk.

Special rules apply to the processing of personal and sensitive personal data. For further guidance on this, see the council's data protection policy.

9. 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.

Adopted 14.4.2026