Mount Bures Parish Council Information Technology Policy (IT Policy)

Introduction

Mount Bures Parish Council (the council) does not have its own IT equipment or servers. All councillors and staff use their own IT equipment to carry out council work. It does manage a website and council email service.

Purpose of the IT Policy

The purpose of this IT policy is to establish clear parameters for how councillors, staff, and other authorised users use the council-provided technology in the course of their duties. A well-defined policy helps to:

- Set expectations for appropriate use;
- 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.

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, work on a flexible or part-time basis or are unpaid volunteers. It sets out the expectations for the appropriate use of IT systems in general and those provided by the council. IT equipment includes anything that can connect to email services and websites e.g. computers, laptops, tablets, smart TV's and mobile phones.

1.0 General Computer use

a. Councillors, staff, and other authorised users must lock their IT equipment that they use for council duties when leaving them unattended to prevent unauthorised access. Failure to comply may lead to disciplinary action.

b. Councillors, staff, and other authorised are not to purchase any computer or mobile equipment (including software), unless previously authorised at an Mount Bures Parish Council Meeting

c. In cases of legal proceedings, the council may need to temporarily take possession of a device to retrieve the relevant data.

d. 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.

e. Councillors, staff, and other authorised users who intend to use their own devices must ensure that they:
   i. use a strong password (see section 2.0)
   ii. configure their device(s) to automatically prompt for a password after a period of inactivity of more than 15 minutes for laptops and 1 minute for mobile devices.

<ol type="i" start="3">
always password protect any documents containing confidential information that are sent as attachments to an email, and notify the password separately (preferably by a means other than email e.g. text or WhatsApp).
ensure secure Wi-Fi networks are used and not use public Wi-Fi where possible.
ensure that council-related data cannot be viewed or retrieved by family or friends who may use the device.
inform the Mount Bures Parish Chair or Vice Chair if their device(s) is/are lost, stolen, or inappropriately accessed where there is risk of access to council data or resources. To prevent phones being used to access confidential data, they will need to retain the details of their IMEI number and the SIM number of the device as their provider will require this to deactivate it.

<ol type="a" start="6">
Personal data relating to Councillors, Clerk or Residents 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.
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.
Any work done on user's own equipment should be stored securely and password protected and should always be backed up in accordance with the council's standard backup procedures.
If transferring data, either by email or by other means, this should be done through an encrypted channel, such as a virtual private network (VPN) or a secure web protocol (https://). 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, staff, and other authorised users are required to allow the council 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 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.

2.0 Password and Authentication Policy
<ol type="a">
All user accounts must be protected by strong, secure passwords. The council follows the National Cyber Security Centre (NCSC) recommendations for creating passwords using three random words (e.g. PurpleCandleRiver). This method helps create passwords that are both strong and easy to remember, while offering effective protection against common cyber threats such as brute-force attacks. This approach is endorsed in NALC guidance.
Fingerprint and/ or face recognition is acceptable forms of securing IT equipment as long as the above password requirements are met.
In addition to strong passwords, Multi-Factor Authentication (MFA) should be enabled wherever possible. MFA requires users to provide two or more independent forms of

verification—for example, a password (something you know) and a code sent to your phone (something you have). This significantly reduces the risk of unauthorised access to systems and personal data.

d. To further strengthen account security:
    i.   Initial user account passwords must be generated by the IT provider.
    ii.   Default passwords provided by the IT provider must be changed immediately upon installation or setup.
    iii. Service or System (e.g. Website) account passwords are generated and managed by the IT provider.
    iv.   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.

e. Access to Passwords
    i.   Passwords are personal and must not be shared under any circumstances.
    ii.   Only the assigned user of an account may access or use the associated password.
    iii. 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.
    iv.   Administrative credentials must be stored securely and only accessible to authorised personnel with a copy provided to Adham Parish Chair, in a sealed envelope, only to be accessed in an emergency.

f. Password Storage and Management
    i.   Passwords must not be stored in plain text or written down in insecure locations.

g. Password Change Requirements
    i.   Immediately change password if compromise is suspected.

h. Password Access Control and Logging
    i.   All access to administrative or shared credentials must be logged and auditable.
    ii.   Attempts to access unauthorized passwords will be treated as a security incident.

i. Responsibility
    i.   Users are responsible for creating and maintaining secure passwords for their accounts.
    ii.   The IT provider is responsible for managing system/service credentials.

3.0 Monitoring

a. The council reserves the right to monitor and maintain logs of 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. Email usage is continually monitored as part of the council's protection against computer viruses, ongoing maintenance of the system, and when investigating faults.

b. The council will monitor the use of electronic communications and use of the internet in line with the Investigatory Powers (Interception by Councils etc for Monitoring and Record-keeping Purposes) Regulations 2018.

c. Monitoring of email and council website use will be conducted in accordance with an impact assessment that the council has carried out to ensure that monitoring is necessary and

proportionate. Monitoring is in the council's legitimate interests and is to ensure that this policy is being complied with.

d. The information obtained through monitoring may be shared internally, including with relevant councillors and IT staff if access to the data is necessary for performance of their roles. The information may also be shared with external HR or legal advisers for the purposes of seeking professional advice. Any external advisers will have appropriate data protection policies and protocols in place.

e. The information gathered through monitoring will be retained only long enough for any breach of this policy to come to light and for any investigation to be conducted.

f. Councillors, staff, and other authorised users have a number of rights in relation to their data, including the right to make a subject access request and the right to have data rectified or erased in some circumstances. You can find further details of these rights and how to exercise them in the council's data protection policy available on the council's website.

g. 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.

h. 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.

i. All computers will be periodically checked and scanned for unauthorised programmes and viruses.

4.0 Remote working

a. Increased IT security measures apply to those who work away from their normal place of work (e.g. whilst travelling, working from home), as follows:
    i. 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), council services should not be accessed from that device.
    ii. 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.
    iii. any data printed should be collected and stored securely.
    iv. all electronic files should be password protected.
    v. papers, files or computer equipment must not be left unattended at any time.
    vi. any data should be kept safely and should only be disposed of securely.
    vii. 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 out of sight in the boot of the car. If staying away overnight, council data should be taken into the accommodation, care being taken that it will not be interfered with by others or inadvertently destroyed.

viii.   where possible the ability to remotely wipe any mobile devices that process sensitive information should be retained in the case of loss or theft.

5.0 Email

a. 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. Councillors, staff, and other authorised users need to be careful not to introduce viruses onto council systems and should take proper account of the security advice below.

b. These rules are designed to minimise the legal risks run when using email and to guide councillors, staff, and other authorised users as to what may and may not be done. If there is something which is not covered in the policy, councillors, staff, and other authorised users should ask an IT competent councillor rather than assuming they know the right answer.

c. 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.

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

6.0 Trademarks, links and data protection

a. 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.

b. Special rules apply to the processing of personal and sensitive personal data. For further guidance on this, see the council's general data protection policy and privacy policy, copies of which are available on the council's website.

7.0 Use of social media

a. Social media includes blogs; Wikipedia and other similar sites where text can be posted; multimedia or user generated media sites (YouTube); social networking sites (such as Facebook, LinkedIn, X (formerly known as Twitter), Instagram, TikTok, etc.); text messaging and mobile device communications and more traditional forms of media such as TV and newspapers. Care should be taken when using social media at any time.

b. The council has a separate policy for media and communication and is available on the council website.

8.0 Misuse

a. 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.