

BURY PARISH COUNCIL

ACCEPTABLE USE POLICY

This Acceptable Usage Policy covers the security and use of all Bury Parish Council information and IT equipment. It also includes the use of email, internet, voice and mobile IT equipment. This policy applies to all Bury Parish Council councillors (hereafter referred to as ‘individuals’).

This policy applies to all information, in whatever form, relating to Bury Parish Council business activities global, and to all information handled by Bury Parish Council relating to other organisations with whom it deals. It also covers all Information Technology (IT) and information communications facilities operated by Bury Parish Council or on its behalf.

Contents

Computer Access Control – Individual’s Responsibility	1
Internet and email Conditions of Use.....	2
Clear Desk and Clear Screen Policy	3
Mobile Storage Devices	3
Software	3
Viruses.....	3
Monitoring and Filtering	4

Computer Access Control – Individual’s Responsibility

Access to the Bury Parish Council IT system is controlled using User IDs and passwords. Each Councillor and employee is responsible for securely password protecting laptop(s).

Individuals must not:

- Allow anyone else to use their user ID and password on any Bury Parish Council IT system.
- Leave their user accounts logged in at an unattended and unlocked computer.
- Leave their password unprotected (for example writing it down).
- Perform any unauthorised changes to Bury Parish Council IT systems or information.
- Attempt to access data that they are not authorised to use or access.
- Exceed the limits of their authorisation or specific business need to interrogate the system or data.
- Connect any non-Bury Parish Council authorised device to the Bury Parish Council IT equipment.

- Give or transfer Bury Parish Council data or software to any person or organisation.
- outside Bury Parish Council without the authority of Bury Parish Council.

Internet and email Conditions of Use

Use of Bury Parish Council internet and email is intended for business use. Personal use is permitted where such use does not affect the individual's business performance, is not detrimental to Bury Parish Council in any way, not in breach of any term and condition of employment and does not place the individual or Bury Parish Council in breach of statutory or other legal obligations.

All individuals are accountable for their actions on the internet and email systems.

Individuals must not:

- Use the internet or email for the purposes of harassment or abuse.
- Use profanity, obscenities, or derogatory remarks in communications.
- Access, download, send or receive any data (including images), which Bury Parish Council considers offensive in any way, including sexually explicit, discriminatory, defamatory or libellous material.
- Use the internet or email to make personal gains or conduct a personal business.
- Use the internet or email to gamble.
- Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam.
- Place any information on the Internet that relates to Bury Parish Council, alter any information about it, or express any opinion about Bury Parish Council, unless they are specifically authorised to do this.
- Send unprotected sensitive or confidential information externally.
- Make official commitments through the internet or email on behalf of Bury Parish Council unless authorised to do so.
- Download copyrighted material such as music media (MP3) files, film and video files (not an exhaustive list) without appropriate approval.
- In any way infringe any copyright, database rights, trademarks or other intellectual property.
- Download any software from the internet without prior approval.
- Connect Bury Parish Council devices to the internet using non-standard connections.

Clear Desk and Clear Screen Policy

To reduce the risk of unauthorised access or loss of information, Bury Parish Council enforces a clear desk and screen policy as follows:

- Personal or confidential business information must be protected.
- IT equipment must be logged off/locked or protected with a screen locking mechanism controlled by a password when unattended.
- Care must be taken to not leave confidential material on printers or photocopiers.
- All business-related printed matter must be disposed of using shredders.

Mobile Storage Devices

Mobile devices such as memory sticks, CDs, DVDs and removable hard drives must be used only in situations when network connectivity is unavailable or there is no other secure method of transferring data. Only Bury Parish Council authorised mobile storage devices with encryption such as Microsoft Bitlocker enabled must be used by the clerk, when transferring sensitive or confidential data.

Software

Employees / Councillors must use only software that is authorised by Bury Parish Council on Bury Parish Council computers. Authorised software must be used in accordance with the software supplier's licensing agreements. All software on Bury Parish Council computers must be approved and installed by the Bury Parish Council.

Viruses

It is important to keep virus software up-to-date and doing this is the responsibility of the user(s). Any downloaded or copied files must be virus checked first. Do not download any material that you suspect may contain a virus. All files should be downloaded using a PC with virus checking software installed.

Actions upon Termination of Contract / Resignation

All Bury Parish Council equipment and data, for example laptops, USB memory devices and CDs/DVDs, must be returned to Bury Parish Council at termination of contract/ resignation. All Bury Parish Council data or intellectual property developed or gained during the period of employment / as a councillor/clerk remains the property of Bury Parish Council and must not be retained beyond termination or reused for any other purpose.

Monitoring and Filtering

All data that is created and stored on Bury Parish Council computers is the property of Bury Parish Council and there is no official provision for individual data privacy, however wherever possible Bury Parish Council will avoid opening personal emails.

Any monitoring will be carried out in accordance with audited, controlled internal processes, the UK Data Protection Act 1998, the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice Interception of Communications) Regulations 2000.

This policy must be read in conjunction with:

- Computer Misuse Act 1990
- Data Protection Act 1998

All breaches of information security policies will be investigated. Where investigations reveal misconduct, disciplinary action may follow in line with Bury Parish Council disciplinary procedures.