

Bomere Heath and District Parish Council

IT Policy



Version History			
Version	Date	Detail	Author
V0.1	03 Nov 2025	Adopted at Nov 25 PC Meeting	D Harmer

November 2025

Contents

Bomere Heath and District Parish Council.....	1
IT Policy.....	1
Bomere Heath & District INFORMATION TECHNOLOGY POLICY	3
Guidelines and Background.....	3
BHPC IT Policy.....	4
The Basics;	4
Monitoring.....	4
Passwords & rules around accessing IT systems	4
Computer usage	4
Data Protection.....	4
Mobile phone texting	4
Email communication	4
Internet.....	5
Software.....	5
Training	5
Misuse.....	5
Important notice.....	5

Bomere Heath & District INFORMATION TECHNOLOGY POLICY

Guidelines and Background

Each council will have their own IT provision and a 'fit-for-all' policy is not possible. Some small Parish councils, such as Bomere Heath, will have minimal equipment whilst others may have multiple devices linked to a server. These guidelines are designed to help councils consider some of the factors that may need to go into a policy.

The purpose of an IT policy is to set out the parameters on how council staff should use the technology that you provide them with in order to do their job.

A clear policy will also help to raise awareness of the risks associated with using IT and can protect the council from loss of data. Councils will need to take a view on whether staff are permitted to use IT equipment for personal use (i.e. accessing webmail or online shopping at lunchtimes). The policy needs to clarify acceptable and non-acceptable use and what will happen if the policy is breached.

As an employer, BHDPC have the right to monitor / review work use of IT equipment provided the Parish Council have a legitimate reason and that BHDPC tell staff that you might do this.

Bomere Heath & District has limited IT equipment and basic access & software needs; therefore the policy is designed to be simple and appropriate for our considered needs. For the most part, councillors use their personal computers & phones to carry out their work.

It is proposed that the policy is reviewed every 3 years

BHPC IT Policy

The Basics;

Who does the policy apply to?

- All Councillors & Employed Staff

What communications and IT equipment does the policy cover?

- Computers, Shared server (Hugo Fox Members Site) Emails, Website & Social Media.

Who is responsible for monitoring and reviewing the policy?

- The Chair of the PC shall have overall responsibility. This person should help staff understand the policy and enforce it as appropriate.

Related policies

- BHPC has other policies which set out standards of behaviour that apply equally to online behaviour? Include Disciplinary Rules, Data Protection Policy, Equality and Diversity Policy, Social Media. GDPR etc.

Monitoring - BHPC don't passively monitor how staff use the internet or email;

Passwords & rules around accessing IT systems - Do not disclose passwords, Do you transmit confidential or personal sensitive information

It is recommended that the length and form must passwords could include being long, complex (using a mix of uppercase and lowercase letters, numbers, and symbols), and unique to each account. Avoid using personal information, common words, or predictable patterns to increase security.

If councillors or employee think someone else knows their password, take steps to update and change it as soon as possible.

Computer usage – the PC do not issue computer hardware to councillors.

Computers/Laptops are councillors' personal hardware with access to PC portals.

The Clerk is the only employee that has PC owned & provided hardware. Computers should be shut down at the end of every day. Should employees log out of their systems.

Documents be saved in a location accessible for back up or update to the server.

Clerk hardware is primarily to be used at home and for PC meetings or works at venues.

Data Protection – ensure you reference the requirements when processing personal data in accordance with the six data protection principles.

Collecting, Storing, Retaining, Using, Disclosing and Disposing of personal information is covered in the GDPR Policy.

It covers how the council protects data and prevents unauthorised or unlawful processing or disclosure.

Mobile phone texting – Mobile Phones are not issued as part of the PC. Texting is permitted as part of PC work on personal phones, but if for PC business it is expected to be polite & professional at all times.

Email communication - Email is the most common communication method for the PC.

Note as a casual way to communicate and this may present a reputational risk.

The PC members are encouraged to utilise a dedicated email for PC communication such as a free Gmail account.

The email format is xxbomereheathpc@gmail.com the xx replaced by councillors' initials.

The PC has 3 dedicated "gov.uk" PC emails that are restricted to general enquiries, Chair & Clerk.

Most communication from the PC will be via the clerk and the clerk will manage the flow of day to day information.

Internet – The PC has no internet access other than the clerks. This is funded by the PC and for the sole use of the clerk at the clerks home address.

The PC uses Hugo-Fox as its website holder and storage manager. This will be regularly updated and managed (set out in the social media policy)

Software – The clerk is the only employee with a computer and software is to be limited to the general Microsoft suite, with a security function. The clerk is able to contact the PC IT Support to annually review and update as needed. (Funds for this should be allocated in the budget and made available as needed)

Training – It is encouraged that members that do not have IT training, especially surrounding IT security, that they review free online training for awareness

Misuse – Misuse of IT facilities can potentially result in disciplinary proceedings.

Examples of misuse include;

1. Not adhering to the policy;
2. Attempting to discover a user's password;
3. Using the computer systems to act abusively;
4. Attempting to circumvent the network's security;
5. Knowingly running and installing programmes intended to damage the computer systems;
6. Deliberately wasting computer resources;
7. Leaving laptops unattended in a public place etc.

Important notice

This document was adapted from the National Association of Local Councils (NALC) template for the purpose of its member councils and county associations.