BARCOMBE PARISH COUNCIL INFORMATION TECHNOLOGY POLICY

Introduction

This IT policy has been designed to meet the needs of Barcombe Parish Council. A small Parish council with no full time staff and a minimal amount of hardware.

Purpose of the IT Policy

- 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.

Other persons may be included in monitoring if they access or use council systems e.g. if they have a council e-mail address

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.

Computer use

1.1 Hardware

1.1.1 Council computer equipment is provided for council purposes, however reasonable personal use is permitted (reasonable interpreted as in the opinion of the council).

1.1.2 When working in an open environment computers must be locked when left. Councillors, staff, and other authorised users must lock their computers when leaving their computers to prevent unauthorised access. This applies to all council and personal devices used for council matters.

1.1.3 All computer and mobile equipment will carry a number which is logged against the current owner of that equipment. A list of hardware is appended to this policy document.

1.1.4 Equipment purchases should be reviewed and approved by the Parish council.

1.1.5 Personal disks, USB stick, CDs, DVDs, data storage devices etc cannot be used on council computers without the prior approval of the Council. Barcombe Parish Council approves the use of an external hard drive for backup purposes.

Equipment

2.1 Portable equipment

2.1.1 Portable equipment includes laptop computers, netbooks, tablets, mobile and smart phones with email capability and access to the internet etc.

2.1.2 Portable equipment should be treated with care.

2.1.3 It is important to ensure all portable 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 appropriate security measures. Eg PIN code or biometrics.

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

2.1.5 To protect confidential information, unless it is a requirement of the job and this has been authorised, it is forbidden for photographs or videos to be taken on council premises, without the prior written permission of the Council This includes mobile telephones with camera function, camcorder, tape or other recording device for sound or pictures - moving or still.

2.1.6 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).

2.1.7 In addition, the council does not permit webcams (which may be pre-installed on many laptops) to be used at Council meetings, other than for conference calls for council purposes. If there is any doubt as to whether a device falls under this clause, advice should be sought from ESALC.

2.2 Use of own devices

2.2.2 The Council recognises that some councillors, staff, and other authorised users may wish to use their own smartphones, tablets, laptops etc to access our servers, private clouds or networks for normal council purposes, including, but not limited to, reading their emails or access data in other services. Any such use of personal devices will be at the discretion of the council, but consent for standard systems (MS Windows, Mac OS X, Linux - in commercial configurations) 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.

2.2.3 However, the same security precautions apply to personal devices as to the council's desktop equipment. For continuity purposes where possible, calls made to external external stakeholders must be made on mobile phone numbers to ensure that only these numbers are used and/or stored by the recipient, rather than personal numbers. Any emails sent from own devices should be sent from a council email account and should not identify the individual's personal email address.

2.2.4 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). For Workers or Contractors, we may terminate the worker agreement. This is irrespective of the ownership of the device used. An example would be downloading copyright music illegally or accessing pornographic material.

2.2.5 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.

2.2.6 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.

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

- use a 4-digit pin and biometrics or strong passwords.

- configure their device(s) to automatically prompt for a password after a period of inactivity of more than ten minutes duration.
- 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 Chairman and Clerk if their device(s) is/are lost, stolen, or inappropriately accessed where there is risk of access to council data or resources.

2.2.8 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.

2.2.9 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.

2.2.10 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.

2.2.11 Any work done on user's own equipment should be stored securely and password protected and should be stored on the council's storage cloud.

2.2.12 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 will be required to ensure that all passwords, user access shortcuts and any identifiable data are removed from the device.

Health and safety

3.1.1 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. Further details are set out in the council's display screen equipment policy.

3.1.2 Any VDU user who feels that their workstation requires changes to make it compliant must speak to the Chairman.

If any hazards are detected at a workstation, including 'noises' from the IT equipment, this should be reported immediately to the Clerk.

Password and Authentication Policy

Note: **Barcombe Parish Council has no IT systems.**

4.1.1 Councillors and employees are required to maintain a password and/or biometric security on any personal/council device containing council related data.

Monitoring

5.1.1 Barcombe Parish Council has no IT systems and will not conduct any routine monitoring of system use.

5.1.2 Barcombe Parish council reserve the right to review personal devices used by councillors and employees for council matters in the event that the council needs such data to satisfy any legal challenges.

Remote working

Note: Barcombe Parish council has no office space.

Barcombe Parish council has no On-line IT services.

6.1.1 Councillors and employees should handle council equipment as if it were their own - with care.

Email

Note: Email addresses will be made available by end of March 2026 at which time the email policy will be enforced.

7.1.1 Council email addresses will be provided to Councillors and employees. These addresses must not be used for personal use. If used in error for personal use then any emails must be deleted as soon as possible.

7.1.2 The code of conduct must be adhered to when communicating via email.

7.1.3 Copies of emails using council addresses should be copied to the clerk.

Use of the Internet

8.1 Copyright

8.1.1 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. It is easy to copy electronically, but this does not make it any less an offence. The council's policy is to comply with copyright laws, and not to bend the rules in any way.

8.1.2 Councillors, staff, and other authorised users should not assume that because a document or file is on the Internet, it can be freely copied. There is a difference between information in the 'public domain' (which is no longer confidential or secret information but is still copyright protected) and information which is not protected by copyright (such as where the author has been dead for more than 70 years).

8.1.3 Usually, a website will contain copyright conditions; these warnings should be read before downloading or copying.

8.1.4 Copyright and database right law can be complicated. Councillors, staff, and other authorised users should check with the Clerk if unsure about anything.

8.2 Trademarks, links and data protection

8.2.1 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 and/or ESALC.

8.2.2 Special rules apply to the processing of personal and sensitive personal data. For further guidance on this, see the council's data protection policy, a copy of which is available from the Clerk or online.

8.3 Accuracy of information

8.3.1 One of the main benefits of the internet is the access it gives to large amounts of information, which is often more up to date than traditional sources such as libraries. Be aware that, as the internet is uncontrolled, much of the information may be less accurate than it appears.

9 Use of social media

9.3.1 The Social Media Policy (December 2025) must be adhered to.

9.3.2 The code of conduct (December 2025) must be adhered to.

9.3.3 Note that the council may, from time to time, monitor external postings on social media sites. Any employee who has a profile (for example on LinkedIn or Facebook) must not misrepresent themselves or their role with the council. Councillors, staff, and other authorised users are also advised that social media sites are not an appropriate place to air council concerns or complaints: these should be raised with the council or formally through the grievance procedure.

9.3.4 It is important to note that external stakeholders contact details and information remain the property of the council. In addition, councillors, staff, and other authorised users

leaving the council will be required to delete all council-related data including external stakeholders contact details from any personal device/equipment.

9.3.5 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.

Important notice .

This document has been adapted by Barcombe Parish Council from an original document written by Worknest HR – a company that provides HR advice and guidance to town and parish Councils. Please contact them on 01403 240 205 for information about their services.

Equipment list:

One x Dell Laptop Inspiron 14 5000 (id/01)