Carn Brea Parish Council
Consel Plu Carn Bre

PROVISION OF IT EQUIPMENT AND ACCEPTABLE IT USAGE POLICY

Adopted: **16th February 2023**

Minute Ref: **23/02/19**

Carn Brea Parish Council
Consel Plu Carn Bre

PROVISION OF IT EQUIPMENT AND ACCEPTABLE IT USAGE POLICY

Context:

Carn Brea Parish Council (CBPC) provides IT equipment to both staff and councillors to enable them to carry out their duties effectively whilst at work, attending Council meetings, when working from home or in the community. This policy is in two parts – the provision of IT equipment and the individual's responsibilities when using IT.

Scope:

This policy sets out the correct, appropriate, and expected use of Carn Brea Parish Council computing and networking facilities to ensure safe and reliable operation. This extends to all IT facilities including software, hardware, laptops & devices and telephones (mobile and internal) provided and maintained by Carn Brea Parish Council.

Ownership of Electronic Files:

All electronic files created, sent, received, or stored on Council owned, leased or administered equipment or otherwise under the control of the Council are the property of the Council. These files may be accessed by the Council's IT Provider at the request of the Council or Proper Officer.

Part 1

Provision of IT Equipment

Virus detection is installed and managed centrally by the IT Provider. Individuals must not remove or disable anti-virus software or attempt to remove virus infected files. Any issues should be immediately referred to the IT Provider via the helpdesk.

All IT equipment issued is owned by and insured by Carn Brea Parish.

a. Employees

All employees are issued with appropriate IT equipment on commencement of employment with the Council. This may include a laptop, tablet, mobile phone and memory devices (e.g., USB) according to the requirements of the role.

A unique email account, Microsoft user ID and password are also issued along with authentication devices if appropriate. Access levels to systems and information will be authorised appropriate to the users' job role.

Upon termination of your contract, all Council owned property should be returned. The Line Manager will ensure all authorised access is promptly removed.

b. Councillors

On joining the Council, Members will be offered a laptop to facilitate their day-to-day duties. The laptop will run a supported operating system, with the capability for joining virtual meetings and accessing Council emails and information via a shared drive. The laptop is on a long-term loan for the length of their tenure as a Parish Councillor. The laptop will be procured by the Council and will be preloaded with software which will be licensed and managed by the Council IT Provider.

The Council will provide all Councillors with a unique Microsoft user ID and password with access to selected areas of the shared drives on the IT system.

On cessation of service as a Parish Councillor the laptop should immediately be returned to the Clerk's Office and all access rights will be rescinded.

c. Loss/Damage

a. Employees

Employees have a responsibility to take reasonable care of any device they are allocated, particularly when taking off site. Any loss or damage should be immediately reported to the Clerk.

b. Councillors

It is accepted that these devices will be taken off site and Councillors have a responsibility to take reasonable care of the device. Any loss or damage should be immediately reported to the Clerk. Where a device has to be sent for repair it may be possible to provide a loan device but this cannot be guaranteed.

At the end of the useful life of the laptop, it will be securely wiped of all data and donated to a suitable individual or organisation.

Part 2

Acceptable IT usage and user responsibilities

a. All authorised users of CBPC computing facilities and network must ensure that:

- Any breaches or suspected security incidents concerning the Council network or computing facilities must be reported immediately.
- Passwords, PINs or any other unique authentication credentials should not be disclosed to anyone under any circumstances.
- Passwords, PINs or any other unique authentication credentials should not be written down anywhere.
- Passwords should be unique and not contain any personal references such as birthdays, family or pet names etc.
- You should change your password immediately if you believe it may have been compromised.
- Always 'screen lock' any device when leaving it unattended.
- Never attempt to perform any unauthorised changes to CBPC IT systems. (such as installation of printers or devices)
- All data held on CBPC systems may be subject to Freedom of Information or Subject Access Requests. For this reason, personal use of CBPC computing and network facilities cannot be deemed to be private.
- Do not use or attempt to use another individual's account.

- Never exceed the limits of your authorisation or specific business need by attempting to access systems or information that you do not need in order to carry out your role. A deliberate and intentional attempt to access unauthorised resources breaches the Computer Misuse Act 1990.
- If you believe you have mistakenly been granted access to IT systems, information or resources which are not appropriate or authorised by you, this should be immediately reported as a possible incident to the Clerk. Under no circumstances should you attempt to further access the information/resources.
- Do not facilitate or attempt to facilitate access for anyone who is not authorised to access specific information or systems.
- Never copy, store or transfer data or software owned by CBPC to any unmanaged device without the explicit written consent of the Council as asset owners.
- Your login ID identifies you as an individual and holds you directly accountable for all actions which take place under your credentials. A logged in session should not be shared with anyone else.

b. Working off site

- Equipment and media taken off site must not be left unattended in public places and not left in sight in a car.
- Information must be protected against loss or compromise when working remotely.
- Particular care should be taken with the use of mobile devices such as mobile phones, laptops and tablets.

c. Internet and Email Conditions of Use

Employees

Use of CBPC internet and email is intended for business use. You should normally only access the internet for the purpose of carrying out Council related business, however limited and reasonable personal use is permitted as long as it does not interfere with the performance of your duties.

All data on the device may be subject to release under the Freedom of Information Act 2000 and UK GDPR. It is the responsibility of the registered user of the device to ensure that personal data is only processed, collected, or retained on the device within the guidance laid out in the Information and Data Protection Policy.

Email and data must not be opened or accessed on a non CBPC device without prior permission from your Line Manager.

All employees are accountable for their actions on the internet and email systems and inappropriate use may result in disciplinary action being taken.

d. Laptops issued to Councillors.

Laptops issued to Councillors are primarily for Council business related purposes. Limited and reasonable personal use is permitted, however the device must not be shared with other family members or loaned to other individuals.

All data on the device may be subject to release under the Freedom of Information Act 2000 and UK GDPR. It is the responsibility of the registered user of the device to ensure that personal data is only processed, collected, or retained on the device within the guidance laid out in the Information and Data Protection Policy.

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

Where requested, the device should immediately be returned to Carn Brea Parish Council.

Councillors and Employees must not:

- Use the internet or email for purposes of harassment or abuse.
- Use profanity, obscenities or derogatory remarks in communications.
- Access, download, view, send or receive any data (including images), which you have reason to suspect are illegal or that could be considered 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 emails 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 CBPC, alter any information about it, or express any opinion about CBPC, unless they are specifically authorised to do this.

- Send unprotected sensitive or confidential information externally.
- Forward CBPC emails and documentation to personal (non-CBPC) email accounts without prior permission and agreement.
- Make official commitments through the internet or email on behalf of CBPC 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 of the IT Consultant. (printers / external devices).

This policy should be read in conjunction with the following:

- CBPC Equality and Diversity Policy
- CBPC Data Protection Policy

For further information please refer to:

- UK GDPR and Freedom of Information Act 2000
- Data Protection Act 2018
- Computer Misuse Act 1990

Employees:

- Employees should also refer to the Employee Handbook