South Willesborough and Newtown Community Council

Use Your Own Device Policy

1. Use of Councillors' own personal devices

A Council Member ("member") may use their own personal device **provided they comply with this policy.**

2. Legal Requirements

Using one's own device raises several data protection concerns as the device is owned by the user rather than the data controller (SWAN CC). It is crucial that the data controller ensures that all processing of personal data remains in compliance with the General Data Protection Regulation 2018.

Inappropriate use of personally-owned devices or unsatisfactory procedures could involve a breach of the Code of Conduct, the Data Protection Act 2018, and the General Data Protection Regulation ("GDPR").

3. Purpose

To ensure so far as possible that:

- personally-owned devices used by members are used in a manner which protects confidentiality, personal data and the confidentiality of council communications.
- members may use personally-owned computers, smartphone and tablet computers for purposes related to council business.
- individual Councillors are responsible for their device at all times. The Council is not responsible for the loss, theft of, or damage to the device or storage media on the device (e.g. removable memory card).
- the Council takes no responsibility for supporting councillors' own devices; nor has the council a responsibility for conducting PAT testing of personally-owned devices.
- personal devices must be secured by a password or a biometric access control (e.g. fingerprint scanner or facial recognition). Passwords should be sufficiently memorable that the user can avoid writing them down, but not obvious or easily guessed.
- care must be taken to avoid using personal devices in a manner which could pose a risk to confidentiality, whether by clicking on links in suspicious emails, accessing potentially harmful websites, using potentially harmful application software, using wi-fi facilities in public places (e.g. coffee shops or airports), or otherwise.
- if a personal device is lost or stolen, or is suspected of having been lost or stolen, the Clerk must be informed as soon as possible such that steps can be taken quickly to protect the council members email account.
- passwords to personal devices must be kept confidential and must not be shared with family members or third parties.

- personal devices must not be used/shared by family members or other persons unless the device has been configured for separate profiles and logins to ensure restricted access to files.
- except in the case of an emergency, members must not copy data from personal devices to other personally-owned devices. The data must be securely deleted when the emergency has passed.
- Councillors may view council information via their mobile devices but must not store the information on their devices, or on cloud servers linked to their mobile devices. In some cases, it may be necessary for councillors to download council information to their mobile devices in order to view it (for example, to view an email attachment). Members must delete this information from their devices as soon as it is appropriate and reasonable to do so. Council information accessed through these services is confidential, in particular information about Members or the Clerk.
- in the event that a personal device needs to be disposed of, confidential material must be destroyed or wiped using a recognised method to put the data beyond recovery, to the satisfaction of The Data Controller. Merely deleting the files, single-pass overwriting, or reformatting the disk is insufficient.
- in the event of a member leaving the council, appropriate steps must be taken to remove the members email account and other data belonging to the Parish Council, from personal devices and cloud storage services used by that member.

Author – Cllr Nirosha Thilagarajan
Adopted by Council 2nd March 2020
Review by March 2022