Bring Your Own Device Policy

1. Introduction
Heath Hayes & Wimblebury Parish Council recognises that Councillors will use personal devices such as smartphones, tablets, and laptops to conduct Council business. This policy ensures compliance with UK GDPR and the Data Protection Act 2018 and protects council information accessed on personal devices.

2. Scope
This policy applies to all Councillors, the Clerk, employees, volunteers, and authorised third parties who access Council information on personally owned devices.

3. Responsibilities of Councillors
Councillors must protect their devices, ensure appropriate security features are enabled, prevent unauthorised access, and follow all Council data protection policies.

4. Security Requirements
- Devices must use strong passwords, PINs, or biometrics.
- Devices must auto-lock and have up to date security patches.
- Antivirus or built-in security tools must be active.
- Only secure, approved apps or portals may be used to access council data.
- Public Wi-Fi must not be used unless secured via VPN.

5. Data Protection Requirements
Councillors must maintain confidentiality, avoid backing up Council data to personal cloud accounts, keep personal and Council data separate, and delete Council data when no longer required.

6. Loss, Theft, or Breach
Any loss, theft, or suspected breach involving a device that may contain Council data must be reported immediately to the Clerk. Remote wipe or deletion must be carried out if required.

7. Leaving Office
Councillors must permanently delete all Council data from personal devices and ensure access to Council systems is revoked.

8. Compliance and Monitoring
The Council may require confirmation that devices meet security standards. Non-compliance may result in the withdrawal of BYOD permissions.

Signed: L Wilson

Dated: 4th March 2026

Minute Reference: 03/26/192.5