Downend and Bromley Heath Parish Council
IT Usage Policy – Workplace and Remote Use

1. Purpose

This policy sets out the responsibilities and expectations for all users of IT equipment provided by Downend and Bromley Heath Parish Council ("the Council") for both workplace and remote use, including home working. It aims to ensure equipment is used securely, responsibly, and only for its intended purpose.

2. Scope

This policy applies to all employees, councillors, and contractors who use Council-issued IT equipment in the workplace and/or in any other location, including at home or while in transit.

3. Permitted Use of IT Equipment

• All IT equipment provided by the Council is strictly for official Council business only.
• Personal use is not permitted.
• Users must not:
o Install unauthorised software or hardware.
o Modify system settings without prior authorisation.
o Share access credentials with others, including family members.

4. Use in the Workplace

When using Council IT equipment on-site:
• Equipment must be stored in a secure location (e.g. lockable drawer or office) when not in use.
• Users must lock their screens if leaving a workstation unattended, even briefly.
• At the end of each working day, devices must be logged out or shut down securely.
• Confidential data must not be left visible on screens or in printed format.
• If equipment is to be shared (e.g. between staff), proper log-off procedures must be followed before handing over.

5. Remote Use (Home Working)

When working from home:

- Devices must be stored in a secure, private area of your home, away from shared or public spaces.
- Equipment must not be used by anyone other than the authorised user.
- Screen lock must be enabled during short breaks.
- Devices must be fully logged out or shut down when work is complete.
- Work-related conversations or video calls must not be overheard by unauthorised individuals.

6. Transporting IT Equipment

When transporting IT equipment:

- Devices must be placed in the boot of the vehicle, out of view at all times.
- IT equipment must never be left visible, such as on car seats or dashboards.
- Do not leave devices unattended in a vehicle for extended periods or overnight.

7. Security and Access Controls

- Two-Step Verification (2SV) must be set up and verified by the Town Clerk on:
  - o Your Windows account
  - o Your Google Workspace account
- All users are responsible for the security of their login credentials:
  - o Use strong, unique passwords.
  - o Do not write down or store passwords insecurely.
  - o Regularly review and update passwords as needed.

8. VPN (Virtual Private Network) Usage

- A Council-issued VPN must be used at all times when working remotely or accessing Council systems from outside the workplace.
- VPN connection is required before accessing any work files, cloud platforms, or email accounts.
- The Council will provide the VPN software and configuration instructions.

9. Data Breaches and Reporting

- If you suspect a data breach, unauthorised access, or any suspicious activity, you must report it to the Town Clerk immediately.
- Do not attempt to resolve IT security issues independently unless directed to by authorised personnel.

10. Compliance and Enforcement

• Failure to follow this policy may result in:
o Disciplinary action
o Withdrawal of IT access or equipment
o Reporting to relevant authorities in the case of serious breaches
• All users are expected to comply with the Council's wider Data Protection, Information Security, and Acceptable Use policies.

11. Policy Review

This policy will be reviewed annually or sooner if there are significant changes in legislation, technology, or Council procedures.

12. Backups

To ensure the protection and recovery of important Council data, all users must adhere to the following backup procedures:

1. **Local Backup:** Ensure you have a copy of any important files and data securely stored on your laptop or computer.
2. **Cloud-Based Backup:** Use Google Drive or other approved Council cloud storage to back up working documents and ensure accessibility in case of device failure.
3. **External Backup:** Conduct a **monthly backup** of all essential data onto an external hard drive or memory stick. This backup must be stored securely in a **locked office or cabinet** to prevent unauthorised access.
4. **Backup Confirmation:** Users must confirm that backups have been completed by recording the date and details of each backup in the **Data Backup Log** located on the Council's shared drive.

Regular checks will be carried out by the Town Clerk to ensure compliance with these procedures.

User Acknowledgement
I confirm that I have read, understood, and agree to comply with the IT Usage Policy for Downend and Bromley Heath Parish Council.

Name: ___________________________
Signature: _________________________
Date: _____________________________