BROADBRIDGE HEATH PARISH COUNCIL – INFORMATION TECHNOLOGY (IT) POLICY

Effective Date: 03 November 2025
Review Date: November 2026

1. Purpose

The purpose of this IT Policy is to set out how council staff and authorised users should use IT and communications equipment provided by the Council. It aims to:

- Ensure safe, secure, and appropriate use of IT resources.
- Protect the Council from loss, damage, or misuse of data.
- Clarify acceptable and unacceptable use of IT resources.
- Raise awareness of IT risks and responsibilities.

2. Scope

This policy applies to:

- All employees, council members, volunteers, and contractors using Council IT systems.
- All IT equipment and communications services, including but not limited to: computers, laptops, tablets, mobile phones, email, internet access, remote access connections, servers, file storage, websites, telephones, and any software or cloud services provided by the Council.

3. Roles and Responsibilities

- The Clerk and RFO has overall responsibility for implementing, monitoring, and reviewing this policy.
- Staff are expected to read, understand, and comply with this policy.
- The Council may review IT usage to ensure compliance and safeguard data, provided staff are informed of such monitoring.

4. Related Policies

This IT Policy should be read in conjunction with the following Council policies:

- Data Protection Policy
- Disciplinary Rules
- Equality and Diversity Policy

- Social Media Policy (if applicable)

5. Monitoring

- The Council may monitor IT usage, including email, internet, and telephones, where there is a legitimate reason.
- Monitoring will be proportionate, justified, and communicated to staff.
- Personal use of Council IT may be permitted within agreed limits, but the Council reserves the right to monitor usage.

6. Passwords and Access

- Passwords must be strong, confidential, and not shared unless authorised.
- Access to another employee's account should only occur with permission and documented justification (e.g., sickness cover).
- Password-protected documents must have secure transmission of the password separately.
- Staff must report suspected password compromise immediately.

7. Computer and IT Equipment Usage

- Computers must be shut down at the end of each day.
- Staff should log out or lock computers when away from their desks.
- Documents must be saved in designated locations for regular backups.
- Equipment should never be left unattended in public areas.

8. Personal Devices (BYOD – Bring Your Own Device)

- Staff may use personal devices for work only if authorised.
- Such devices must meet Council security standards.
- The Council is not liable for loss or damage to personal devices used for work purposes.

9. Data Protection

- Staff must comply with the Data Protection Act and Council Data Protection Policy.
- Personal data must be collected, stored, retained, used, disclosed, and disposed of securely.

- Confidential or sensitive information must be protected at all times, including during transmission.

10. Mobile Phone Use

- Work-related text messages must be professional, clear, and avoid abbreviations.
- Messages must not contain illegal, discriminatory, or offensive content.
- Council mobile phones must be used appropriately for Council business.

11. Email Communication

- Emails must be professional and reflect the Council's standards.
- Staff must not enter into binding agreements with external parties via email without proper authorisation.
- Emails containing confidential or sensitive information must be appropriately protected.

12. Internet Usage

- Internet access is provided for Council-related purposes.
- Limited personal use may be allowed, but staff must not access inappropriate, offensive, or illegal content.
- Staff must not use Council IT to engage in chat rooms, messaging services, blogs, or social media unless authorised.

13. Software

- Only authorised software may be installed on Council devices.
- Downloading or running unapproved software is strictly prohibited.

14. Training and Support

- Staff will receive guidance on IT security and acceptable use as part of their induction.
- Ongoing support and training will be provided as needed.

15. Misuse of IT Facilities

Misuse of IT equipment may result in disciplinary action. Misuse includes, but is not limited to:

- Breaching this policy or attempting to bypass IT security.

- Accessing or sharing another user's account without permission.
- Using IT resources for illegal, abusive, or offensive activities.
- Deliberately wasting computer resources or leaving devices unsecured.
- Installing malware or software intended to damage Council systems.

16. Policy Review

This policy will be reviewed annually or when there is a significant change in IT provision, legislation, or best practice.