**Blisworth Parish Council - IT and Communication Policy**

**Introduction**

The Parish Council understands that the use of digital and electronic communication enables it to interact in a manner that improves the communications both within the Parish Council and between the Parish Council and the people, businesses and agencies it works with and serves.

Emails and other communications should be considered by Councillors and the Clerk as being in the public domain and as such, open to scrutiny.

The Parish Council has a website and uses email to communicate. The Parish Council will always try to use the most effective channel for its communications. Should the Parish Council add to the channels of communication that it uses as it seeks to improve and expand the services it delivers, this policy will be updated to reflect the new arrangements. Councillors and the Clerk may also use other forms of digital communication, such as text messages, for convenience. This policy also covers all digital communications.

Under the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA) councillors should be aware of the risks and data protection obligations and responsibilities, particularly with regard to use of personal email addresses. The Parish Council has obligations relating to the confidentiality, integrity and availability of all personal data it holds. This means that the Council is accountable for any Council business conducted involving personal data on any device or through any email account.

**1 Purpose and scope**

**Purpose:** To set standards, responsibilities, and procedures for the secure, lawful, accessible, and transparent use of information technology and electronic communications by Blisworth Parish Council.
**Scope:** This policy applies to all individuals using the Parish Council's IT resources, including:

- Council-provided computers, laptops, mobile devices, and software.
- Personal devices used for council business (BYOD – Bring Your Own Device).
- Networks, internet connections, cloud storage, and email accounts.

It supplements the Council's Data Protection Policy, Communications Policy, Social Media Policy and Records Retention Schedule.

**2 Legal and regulatory compliance**

Blisworth Parish Council complies with: UK GDPR, Data Protection Act 2018, Freedom of Information Act 2000, Transparency Code, and Accessibility Regulations 2018 (WCAG 2.2 AA). The Council publishes an Accessibility Statement and required transparency information on its gov.uk site. The Council recognises its roles as both Data Controller and Data Processor.

**3 Roles and responsibilities**

- **The Council:** approves policy, allocates resources, and ensures publication of required transparency information.
- **Clerk:** operational lead for data protection, DPIAs, SARs, audits, breach response, ICO liaison, and training coordination. Contact details are published on the Council's gov.uk page.
- **Councillors and staff:** must follow this policy, use **gov.uk assigned email addresses** for council business, complete required training, and report incidents promptly.
- **IT providers and contractors:** must sign Data Processing Agreements, act only on documented instructions, and meet contractual security and audit requirements.

**4 Data protection, mapping and audits**

**Lawful processing:** Personal data is processed only where a lawful basis exists and in line with data protection principles: purpose limitation, minimisation, accuracy, storage limitation, integrity, confidentiality, and accountability.
**Data map:** The Council maintains an **updated data map** documenting processing activities, data categories, lawful bases, retention periods, and third-party transfers, which is reviewed at least annually and after significant service changes.
**Subject rights:** Procedures exist to respond to subject access requests, rectification, erasure, restriction, portability, and objections within statutory timescales.

**5 IT services, accounts and official channels**

- **Gov.uk domain and website:** The Council maintains a gov.uk domain for all official email addresses and a website that meets WCAG 2.2 AA accessibility standards and includes a clear Accessibility Statement.

- **Official email use:** All councillors and staff must use their gov.uk assigned email address for council business. Personal email accounts must not be used for council matters.
- **Social media:** Facebook is the Council's only official social media channel. Admin access is restricted, logged, and managed under the Communications Policy. All social posts must meet accessibility and content standards.
- **Official storage: Microsoft 365 (SharePoint/Teams/OneDrive/Outlook)** is the authorised storage for council data.
- **Councillor email lifecycle:** Councillor accounts are created for council business only and will be deactivated and removed when a councillor resigns. The Clerk will ensure statutory records are retained before deletion.

**6 Acceptable use and communications standards**

**Acceptable use:** Council IT resources and email are for official council activities; Users must respect copyright and avoid inappropriate content.
**Public records:** Council communications are public records and may be subject to FOI and public scrutiny. Draft and store communications accordingly.
**Email standards:** Emails must be professional, civil, and clear. Confidential or sensitive information must not be sent by email unless encrypted. Be vigilant for phishing and verify attachments and links before opening.
**Group email etiquette:** Use **reply-all** only when necessary to preserve transparency. Avoid unnecessary group emails. When forwarding email trails, remove irrelevant personal information to protect privacy.

**7 Device, software and BYOD requirements**

- **Authorised devices:** Where possible, authorised devices and software will be provided by the Council. Unauthorised installation of software on council devices is prohibited.
- **BYOD security:** Personal devices used for council business must have up-to-date operating systems, security updates, reputable antivirus/anti-malware, encryption if storing council data, and screen lock protection. Do not store council data permanently on personal devices; transfer to official storage promptly and delete local copies when no longer required.

**8 Authentication, passwords and account security**

- **Multi-Factor Authentication (MFA): MFA is mandatory** for the council email and website accounts.
- **Passwords:** Use strong passphrases; never share passwords or MFA codes. Change passwords immediately if compromised.
- **Access control:** Admin access to systems and social accounts is restricted and logged.

**10 Incident management and breach notification**

- **Reporting:** Report suspected security incidents or data breaches immediately to the Clerk within **48 hours** of discovery.
- **Initial response:** Target initial containment and assessment **within 24 hours**.
- **Regulatory notification:** Notify the Information Commissioner's Office **within 72 hours** when required and notify affected data subjects when there is a high risk to their rights.
- **Incident log:** Maintain an incident log and lessons-learned register. Conduct post-incident reviews and remediate findings.

**11 Retention and archiving**

Emails should be retained and archived in accordance with legal and regulatory requirements. Regularly review and delete unnecessary emails to maintain an organised inbox.

**12 Monitoring, privacy and proportionality**

**Monitoring:** The Council reserves the right to monitor IT and email usage to ensure compliance. Monitoring will be proportionate, documented, and GDPR-compliant. A monitoring notice is published.

**13 Training, awareness and culture**

**Training:** The Council provides regular data protection and IT security updates**.**
**Awareness:** Periodic communications reinforce good practice, policy updates, and lessons learned from audits and incidents.

### 14 Third parties, procurement and contracts

**Processor agreements:** Contracts with third-party processors must include Data Processing Agreement clauses, security requirements, and audit rights. The Council will assess suppliers' security posture during procurement.
**Right to audit:** The Council retains the right to audit processors where necessary to verify compliance.

### 15 Compliance, enforcement and sanctions

Non-compliance may result in suspension of IT privileges, disciplinary action, contractual remedies for third parties, and reporting to regulators where appropriate. Enforcement actions are applied proportionately and documented.

### 16 Review and approval

This policy is reviewed at least annually or sooner when legal, operational, or technological changes require updates. Changes are approved by the Council and communicated to all relevant parties.

---

### Appendices

#### Appendix A — Incident response checklist

**Checklist:** report to Clerk; contain and isolate; preserve evidence; assess risk to data subjects; notify ICO within 72 hours if required; notify affected data subjects if high risk; remediate and record lessons learned.

#### Appendix B — Councillor email checklist

- Use **gov.uk assigned email** for all council business.
- Do not register councillor email on non-council services.
- Do not use councillor email for business or commercial activity.
- Transfer council data to Microsoft 365 storage promptly.
- Delete local copies from personal devices after archiving.
- Report breaches immediately to the Clerk.

| Version | Details of any revision | Approved at | Date | Review Date |
|---|---|---|---|---|
| v1 | Adopted new BPC Electronic Communication Policy | Approved at BPC Meeting: 06/03/2023 Minute Point: 17 | 06/03/2023 | May 2023 |
| Readopted | None | Readopted at BPC Meeting 02/05/2023 Minute Point: 31 | 02/05/2023 | May 2024 |
| Readoption | None | Readopted at BPC Meeting 13/05/2024 Minute Point: BPC/58/24-25 | 13/05/2024 | May 2025 |
| Readopted | None | Readopted at BPC Meeting 12/05/2025 Minute Point: BPC/31/2025 | 12/05/2025 | May 2026 |
| v2 | Adopted new BPC Blisworth Parish Council - IT and Communication Policy | Adopted at BPC Meeting 02/03/2026 Minute Point: BPC/292/2026 | 02/03/2026 | May 2027 |