Cockshutt cum Petton Parish Council

Information Technology, Homeworking & Personal Equipment Policy

Cockshutt cum Petton Parish Council recognises the importance of effective and secure information technology (IT) and email usage in supporting its business, operations and communications. This policy outlines the guidelines and responsibilities for the appropriate us of IT resources and emails by council members, clerk, authorised volunteers and contractors.

1. **Purpose**

   This policy sets out how Cockshutt cum Petton Parish Council ("the Council") manages information technology, homeworking arrangements, and the use of personal equipment when conducting Council business.

   The Council is a small authority without a dedicated IT system. Councillors and officers may therefore use personal devices to conduct Council business. This policy ensures:

   - Protection of personal data
   - Compliance with the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018
   - Secure handling of Council information
   - Clear accountability

2. **Scope**

   This policy applies to:

   - All councillors
   - The Clerk and any other employees
   - Contractors & authorised volunteers handling Council information

   It applies to:

   - Email communications
   - Electronic documents
   - Cloud storage
   - All IT equipment such as personal laptops, tablets and mobile phones used for Council business
   - Systems, networks, software and data owned or used by the Council
   - Paper records stored at home

3. **Legal & Regulatory Framework**

   The Council will comply with:

   - UK General Data Protection Regulation (UK GDPR)
   - Data Protection Act 2018
   - Freedom of Information Act 2000
   - Health and Safety at Work etc. Act 1974 (HSWA)
   - ICO guidance for parish councils

4. **Homeworking Arrangements**

   As the Council has no central office IT infrastructure, the Clerk and councillors may work from home.

   4.1 Responsibilities

   Individuals working from home must:

   - Ensure confidential papers are not visible to household members or visitors
   - Store paper records securely

- Avoid conducting Council business on shared devices
- Use secure internet connections (avoid public Wi-Fi where possible)

5. Use of Personal Equipment

The Council permits limited use of personal devices for Council business subject to the following controls:

5.1 Minimum Security Standards

All devices used for Council business must have:

- Password or biometric protection
- Automatic screen lock
- Up-to-date operating system and security updates
- Anti-virus software (where applicable)
- Encrypted storage (enabled by default on most modern devices)

5.2 Email

- The Clerk should use a dedicated Council email account where possible.
- Councillors should use either a council-provided email address (if available) or a separate email folder dedicated to Council matters.

5.3 Storage

- Council documents should be stored in a secure, shared cloud location where feasible.
- Documents must not be permanently stored on personal devices.
- When a councillor leaves office, Council data must be deleted.

6. Information Classification

Council information may include but not limited to:

- Public documents (agendas, minutes)
- Confidential reports
- Personal data (complaints, staffing matters, residents' contact details)

Personal data must always be handled securely and shared only where lawful and in accordance with the Council's Privacy policy

7. Data Retention

Records will be retained in accordance with the Council's adopted retention schedule.
Personal devices must not be used as permanent archives.

8. Freedom of Information (FOI) & Subject Access Requests

Council business conducted via personal devices may still be disclosable under FOI or Subject Access Requests.
Councillors must:

- Co-operate with searches of relevant Council business
- Provide requested records promptly

9. Incident Reporting

Any suspected data breach must be reported immediately to the Clerk (or Chairman if the Clerk is involved). Appendix A

10. Monitoring & Review

The Clerk will review the policy annually and monitor compliance with it. Appendix B

Appendix A

DATA BREACH PROCEDURE

1. **Purpose**
   To provide a clear procedure for managing personal data breaches in accordance with UK GDPR

2. **What Is a Data Breach?**
   A personal data breach includes:
   - Loss or theft of a device
   - Email sent to the wrong person
   - Unauthorised access to council information
   - Paper records lost or disclosed
   - Cyber attack

3. **Immediate Action**
   Any councillor or officer discovering a breach must:
   - Inform the Clerk immediately and provide details:
   - What happened
   - When it occurred
   - What data is involved
   - How many individuals affected
   - Take steps to contain the breach (e.g., recall email, change passwords)

   If the Clerk is involved, notify the Chairman.

4. **Assessment**
   The Clerk will assess:
   - Nature of data involved
   - Sensitivity
   - Number of individuals affected
   - Risk to individuals' rights and freedoms

5. **Reporting to the ICO**
   If there is likely to be a risk to individuals, the breach must be reported to the Information Commissioner's Office within 72 hours.

   If not reported, reasons must be recorded.

6. **Informing Individuals**
   If there is a high risk to individuals (e.g., financial or identity risk), affected individuals must be informed without undue delay

7. **Record Keeping**
   All breaches, including near misses, must be logged in the Council's Breach Register

8. **After any breach, the Council will review:**
   - The cause
   - Whether policy changes are required
   - Whether further training is needed

Appendix B

General Data Protection Awareness Checklist for Councillors

Whilst the Council and its staff is expected to comply with GDPR, individual councillors will also need to ensure that they protect an individual's personal data whether it is stored electronically or as a hard copy. This applies only to living individuals (not the deceased, companies, other authorities and charities)

Personal data includes:

- Names and addresses
- Telephone numbers
- Email addresses
- IP addresses

The following measures are recommended to help councillors comply with GDPR:

Action	Noted ✓
Set up a separate email account for parish council correspondence and try to separate from personal email.	
Ensure that all devices (computers, laptops, phones) are password protected	
Do not forward on emails or email threads that may contain personal data	
Review any hardcopy information and if no longer relevant destroy using a suitable method (Cross cut shredder or destruction service). Ensure Clerk is aware of actions before destruction.	
Where possible direct all correspondence to the Clerk who can obtain the necessary consent	
Where possible avoid holding an individual's information in a councillor's home or on a councillor's own PC. If a councillor has to hold any information containing personal data on behalf of the Parish Council, it needs to be stored securely in a locked room or cabinet or if on a PC, in an encrypted folder or drive.	
Make sure your antivirus software and operating system is up-to-date	
Make sure your computers and router's firewall is turned on	
Inform Clerk and request Data Protection Officer advised of any breaches within 48 hours	
Ensure the Data Protection Officer of any breaches within 48 hours	

I confirm that I have read the information above and understand my responsibility as a parish councillor for protecting personal data.

NAME

Signed: Date: