GDPR Security Compliance Checklist

General Data Protection Regulation (UK GDPR) and Data Protection Act 2018

Town and Parish Councils are required to comply with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. Individual councillors also have personal responsibility to ensure that any personal data they handle in the course of their council duties is processed lawfully, fairly, and securely.

This applies only to **living individuals** and does not apply to information relating solely to deceased persons, companies, other public authorities, or charities.

This checklist is aligned with guidance issued by the Information Commissioner's Office (ICO) and the National Association of Local Councils (NALC) and reflects good practice for elected members.

What is Personal Data?

Personal data means any information relating to an identified or identifiable individual. This includes, but is not limited to:

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

Purpose of This Checklist

This checklist is intended to support councillors in meeting their individual responsibilities under data protection legislation and to demonstrate compliance with council policies and procedures.

All councillors are expected to complete this checklist. Completed records should be retained by the Council for the duration of a councillor's term of office.

Security Checklist

Action	**Confirmed ✓**
All devices used for Council business (computers, laptops, phones, tablets) are protected by a secure password, PIN, or biometric control	✓
Council issued email account is password protected	✓
Emails or email chains containing personal data are not forwarded without a lawful basis	
Hard copy information is reviewed regularly and, where no longer required, is disposed of securely (e.g. cross-cut shredding or approved destruction service). The Town Clerk is informed prior to destruction	
Where practicable, correspondence containing personal data is directed to the Town Clerk for processing and consent management	
Personal data is not routinely stored at a councillor's home or on personal devices	
Where storage is unavoidable, personal data is kept securely (locked room or cabinet, or encrypted folder/drive)	

Anti-virus software and operating system updates are installed and kept up to date	✓
Device and router firewalls are enabled	✓
USB/flash drives used for Council business are password protected and encrypted where possible	
External hard drives are password protected and encrypted where possible	
Cloud-based services used for Council business are secured with strong passwords (and multi-factor authentication where available)	✓
Access to Council information is restricted to authorised persons only *(server and SharePoint data is locked down by user accounts)*	
Any actual or suspected personal data breach is reported to the Town Clerk without delay and no later than **48 hours**	

Declaration

I confirm that I have read and understood the information above and that I am aware of my responsibilities as a Town Councillor under the UK GDPR and the Data Protection Act 2018.
I understand that failure to comply with data protection requirements may result in a breach of Council policy and/or legislation.
On leaving office, I confirm that I will securely delete or return any personal data held in connection with work undertaken for or on behalf of the Town Council.

Councillor name: _____

Councillor signature: _____

Date: _____