

Baldons Parish Council

IT Policy

1. Introduction

This policy sets out how Baldons Parish Council expects councillors, the Clerk, and anyone else acting on behalf of the council to use information technology in the course of their duties. The council is committed to using IT in a secure, lawful, and responsible manner that protects personal data, safeguards the council's reputation, and complies with its obligations as a public authority and employer.

This policy applies whether the equipment being used is owned by the council or is personal equipment used for council purposes.

2. Scope

This policy applies to:

- the Clerk to the Council, in relation to all council business;
- all councillors, in relation to their official duties as members of Baldons Parish Council;
- any contractors or volunteers acting on behalf of the council.

It covers all use of IT equipment and software for council purposes, including computers, laptops, tablets, mobile phones, email, cloud storage, and online services.

3. Authority-Owned Equipment

Where the council provides equipment (such as a laptop or mobile phone) for use by the Clerk:

- The equipment must be used exclusively for council business.
- Only software authorised by the council should be installed. The Clerk should seek the Chair's approval before installing any new software.
- The equipment must be kept secure at all times - locked when unattended, and not left in an unattended vehicle.
- The equipment must not be used by family members or others who are not acting on behalf of the council.
- If the equipment is lost, stolen, or damaged, the Clerk must notify the Chair immediately.
- When a Clerk leaves the post, all council-owned equipment must be returned promptly, and council data on any personal devices must be deleted.

4. Use of Personal Equipment

The council recognises that councillors and the Clerk may carry out some council business using personal devices. Where personal equipment is used for council purposes:

- The device should have an up-to-date operating system, antivirus software (where applicable), and a secure password or PIN.
- Council documents and personal data must not be stored in personal cloud storage accounts (such as a personal Google Drive or iCloud) unless the service is appropriately configured and access is controlled.

Adopted:	September 2026	Minute:	051/26	Review date:	May 2027
----------	----------------	---------	--------	--------------	----------

Baldons Parish Council

- Personal data held on personal devices in connection with council duties is subject to UK GDPR. The council is the data controller; the individual is responsible for the security of the data on their device.
- When council duties cease, any council-related data held on a personal device must be securely deleted.

The council will keep the use of personal devices for council business under review and aims to provide the Clerk with a council-owned laptop and phone as resources allow.

5. Email

The council uses www.baldonspc.org and councillors have named email accounts under this domain. The following rules apply:

- The Clerk should use a clearly identifiable email account for council business. Where a personal email account is used, council correspondence should be kept clearly separate from personal communications.
- Councillors should be aware that emails sent in their capacity as councillors may be subject to Freedom of Information requests.
- Emails containing personal data about individuals should be treated with care. Sensitive personal data should not be sent by email unless encrypted or sent via a secure method.
- Once a council email system is in place, it must be used for all council business.

6. Data Storage and Security

All council records, including minutes, financial documents, correspondence, and any personal data, must be stored securely.

- Electronic documents should be saved in a location that is backed up regularly. The Clerk is responsible for ensuring council records are not held solely on a single unprotected device.
- Personal data must only be held for as long as necessary, in accordance with the council's Data Retention Policy.
- Documents containing personal data must not be stored in shared folders or systems accessible to individuals who do not need access.
- If cloud storage is used for council records, the service must be based in the UK or European Economic Area, or have appropriate safeguards in place. Consumer-grade services not subject to UK data protection law should not be used.

7. Passwords and Access

- All devices and accounts used for council purposes must be protected by a strong, unique password or passphrase.
- Passwords must not be shared with others.
- Where accounts allow two-factor authentication, it should be enabled.
- Access to shared council accounts (such as a council email inbox) should be reviewed whenever someone leaves their role.

8. Social Media

Councillors and the Clerk should exercise care when using personal social media accounts in ways that could be associated with the council. In particular:

- Councillors must not represent personal views as the official position of the council.

Adopted:	September 2026	Minute:	051/26	Review date:	May 2027
----------	----------------	---------	--------	--------------	----------

Baldons Parish Council

- Complaints or disputes involving residents, contractors, or other parties must not be discussed on social media.
- Councillors remain subject to the Code of Conduct in their online conduct as well as in person.

Where the council operates an official social media account, only those authorised by the council may post on its behalf.

9. Reporting a Problem or Incident

Any suspected loss, theft, or unauthorised access involving a device or account used for council purposes must be reported to the Clerk and/or to the Chair as soon as possible. If the incident involves personal data and may constitute a data breach, the council's Data Breach Policy must be followed.

10. Responsibilities

The Clerk is responsible for day-to-day implementation of this policy and for raising any IT security concerns with the Chair.

The council as a whole is responsible for ensuring the policy is reviewed annually and that adequate resources are made available for council-owned equipment and secure systems. Individual councillors are responsible for complying with this policy in their own use of IT for council purposes.

11. Review

This policy will be reviewed annually or sooner if there is a significant change in the council's technology use, staffing, or relevant legislation.

12. Legal and Regulatory Framework

This policy has regard to the following:

- UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018
- Network and Information Systems (NIS) Regulations 2018
- Computer Misuse Act 1990
- Freedom of Information Act 2000
- Public Sector Bodies (Websites and Mobile Applications) (No. 2) Accessibility Regulations 2018
- Transparency and Accountability: A Guide for Smaller Authorities (DLUHC)
- ICO guidance on data protection for elected representatives and local councils
- NALC guidance on IT policies for local councils

This policy is maintained to meet the requirement in paragraph 1.54 of the Practitioners' Guide, tested under Assertion 10 of the Annual Governance Statement.

Adopted:	September 2026	Minute:	051/26	Review date:	May 2027
----------	----------------	---------	--------	--------------	----------