



IRON ACTON PARISH COUNCIL IT POLICY

1. Purpose

This policy sets out how Iron Acton Parish Council uses information technology to conduct its business securely, lawfully and efficiently. It applies to all councillors and the Clerk when undertaking council business.

2. Scope

This policy covers:

- email and electronic communications,
- use of council and personal devices,
- storage and sharing of council information,
- access controls and security,
- arrangements when councillors or staff leave office.

3. Council Email Accounts

- All official council business must be conducted using council-provided .gov.uk email accounts.
- Personal email accounts must not be used for council business.
- Emails relating to council business form part of the council's records and may be subject to the Freedom of Information Act 2000.

4. Devices and Access

- Councillors and the Clerk may use personal devices for council business where necessary, provided reasonable security measures are in place (for example, password or biometric protection).
- Devices used for council business must not be shared with others where council information could be accessed.

5. Passwords and Security

- Passwords must be kept confidential and not shared.
- Strong passwords should be used, and changed where there is any concern about compromise.
- Access to council systems and accounts will be restricted to authorised users only.

6. Storage and Handling of Information

- Council documents and personal data must be stored securely.
- Personal data must be handled in accordance with the Council's Data Protection Policy and UK General Data Protection Regulation.
- Information must not be downloaded, copied or shared unnecessarily.



7. Leaving Office

- When a councillor or the Clerk leaves office, access to council systems and email accounts will be removed promptly.
- Any council information held on personal devices must be deleted or returned to the Council.

8. Breaches and Incidents

- Any suspected data breach, loss of equipment, or unauthorised access must be reported immediately to the Clerk.
- Incidents will be handled in accordance with the Council's Data Protection Policy.

9. Review

This policy will be reviewed at least every two years, or earlier if required.

Approved: 16/02/2026

Minute No:	
------------	--