BRATTON FLEMING PARISH COUNCIL
INFORMATION TECHNOLOGY POLICY

Adopted May 2026

1. Purpose and Scope
This Policy applies to all Councillors, employees, contractors and volunteers who use IT systems to carry out council business, whether on council-owned or personal devices.

2. Council Email Use
All official Parish Council business to come from a Council-owned email address.
Emails to the Council must be via this council-owned email address and not to the Clerk's personal email address.
Password strength must be at least twelve letters / figures and include an icon such as !£$*+
Access to emails should be through a password.

3. Data Protection and GDPR
Personal data must not be stored unencrypted on USB sticks, personal laptops, or cloud services such as Dropbox, unless approved by the Council.

It is not necessary for this Council to have a Data Controller.

The Council has a Data Protection Policy in force, reviewed and adopted on an annual basis.

The Council has a Freedom of Information Act Policy in place and a Subject Access Requests Policy, reviewed on an annual basis.

These Policies are on the Council website and gives guidance on how Freedom of Information requests are dealt with.

4. Website Management and Accessibility.
The Council's website meets WCAG 2.2 AA standards and all required documents are published on it. (Minutes, AGAR (Annual Governance and Accountability Return), Councillors' details.

The Clerk is responsible for updating the website.

The Clerk frequently accesses the website to check for accessibility and broken links.

5. Use of Council Equipment.
The Council does not own any IT equipment. The Clerk uses there own equipment for Council business.

6. Cyber Security and Online Safety.
Suspicious emails received by the Clerk are reported to report@phishing.gov.uk

Councillors are informed, in a separate email, of the details and action taken, so as to make them aware.

The Clerk never clicks on links or downloads material felt to be a risk or considered suspicious.

For emails that could be suspicious, the advice is to hover the mouse over the email address to check for authenticity.

Check for spelling mistakes and form of greeting.

Check the website address separately to verify if the firm is legitimate.

Telephone the firm to enquire if it was them who sent the email.

Reuse of passwords across personal and Council accounts should not be used.

7. Social Media and Communications.
Councillors with knowledge of posting on Facebook will, when necessary, put items on relating to the Council for general information to the public.

Councillors should not comment as individuals on behalf of the Council and professionalism should be used at all times.

8. Training and Review.
This Policy will be reviewed on an annual basis.

The Clerk will be responsible for updates.

Next Review: May 2027 (to be in line with review of other Policies)