Shadingfield, Sotterley, Willingham & Ellough Joint Parish Council

Social Media & Electronic Communications Policy (Updated 2026)

1. Purpose

The purpose of this policy is to provide clear, lawful and practical guidance on the acceptable use of email, messaging services, websites and social media by Councillors and the Clerk. As your original policy states, its aim is to ensure behaviour is *"consistent with the Council's Employee Code of Conduct, Acceptable Use policies, Risk Management Strategy and professional best practices"* .

This policy reflects current legislation, including the UK GDPR, Data Protection Act 2018, Online Safety Act 2023, and relevant local government transparency requirements.

Nothing in this policy restricts the proper use of digital communication for legitimate Council business.

2. Scope

This policy applies to:

- All Councillors
- The Clerk
- Any person acting on behalf of the Council in an official capacity

It covers:

- Email
- SMS and messaging apps (including WhatsApp)

- Social media platforms
- Websites and online forums
- Any digital communication used for Council business

3. Legislative Framework (Updated 2026)

3.1 Data Protection

All digital communication must comply with:

- **UK GDPR (2021–2026)**
- **Data Protection Act 2018**
- **ICO 2025 guidance on messaging apps and email security**

Key requirements:

- Personal data must only be shared when necessary and lawful.
- Councillors must use **separate Council email addresses** to ensure data segregation.
- WhatsApp or similar apps must **not** be used to share personal data unless end-to-end encryption is active and the data is strictly necessary.

3.2 Freedom of Information (FOI)

All Council-related digital communication may be subject to FOI disclosure.

Councillors must:

- Copy the Clerk into all Council-related emails and messages.
- Retain records of decisions and discussions relevant to Council business.
- Avoid conducting substantive Council business on private devices without proper record-keeping.

3.3 Online Safety Act 2023

The Online Safety Act introduces duties relating to:

- Harmful content
- Illegal content
- Protection of individuals from harassment and abuse online

Councillors must not:

- Post or share harmful, abusive or misleading content
- Engage in online arguments or political campaigning on Council channels
- Amplify misinformation or unverified claims

3.4 Defamation Act 2013

Councillors must avoid statements that could be defamatory.

3.5 Equality Act 2010

Digital communication must not discriminate on the basis of protected characteristics.

3.6 Local Government Act 1972

Council business must be transparent and accessible.
Digital communication must not:

- Replace lawful decision-making in meetings
- Exclude the public from processes
- Conduct planning discussions privately

4. Acceptable Use Requirements

4.1 General Conduct

Councillors and the Clerk must:

- Be respectful, factual and professional
- Use correct spelling, grammar and punctuation
- Avoid profanity, bullying or harassment
- Avoid political debate or campaigning on Council channels

4.2 Prohibited Actions

You must not:

- Use language that could offend, discriminate or embarrass
- Share confidential or exempt information
- Enter into contracts or commitments without authority
- Post material that could cause reputational harm
- Use Council channels for jokes, memes or irrelevant content

5. Use of Social Media

Council social media accounts must:

- Provide factual, timely information
- Avoid political content
- Not engage in debate or arguments
- Comply with accessibility standards (Public Sector Bodies Accessibility Regulations 2018)

Personal accounts:

- Must not give the impression of speaking on behalf of the Council

- Must not disclose confidential information
- Should include a disclaimer if discussing local issues in a personal capacity

6. Use of Messaging Apps (WhatsApp, SMS, etc.)

Updated requirements:

- WhatsApp must **not** be used for decision-making
- Personal data must not be shared unless strictly necessary
- Group membership must be controlled by the Clerk
- Messages relating to Council business that constitute records must be forwarded to the Clerk for retention

7. Security Requirements

Councillors must:

- Use Council-specific email addresses
- Enable two-factor authentication where available
- Use strong passwords
- Report any data breach immediately to the Clerk
- Avoid using public Wi-Fi for Council business unless using a VPN

8. Transparency & Record Keeping

- All Council-related communication must be copied to the Clerk
- Decisions must not be made via WhatsApp, email or social media
- Any communication relevant to Council business must be retained for FOI and audit purposes

9. Enforcement

Breaches of this policy may result in:

- Referral to the Monitoring Officer
- Formal investigation under the Code of Conduct
- Reporting to the ICO (for data breaches)
- Legal action (defamation, harassment, etc.)

10. Review

This policy will be reviewed every two years or sooner if legislation changes.

Date of adoption: May 2026
Date of next review: May 2028
Chair: C. Ellis
Clerk: V. Ellis