Hatfield Peverel Parish Council – Social Media, IT & Electronic Communications Policy (2026)

1. Introduction

Hatfield Peverel Parish Council is committed to ensuring responsible, secure, and respectful use of social media, information technology, and electronic communications. This policy sets out the standards and expectations for councillors, staff, contractors and volunteers in line with legal obligations and best practice.

2. Purpose of the Policy

This policy provides a clear framework for the use of social media, IT systems, and electronic communications. It ensures transparency, protects personal data, promotes respectful engagement and supports the effective operation of the Council.

3. Scope

This policy applies to all councillors, staff, contractors and volunteers using Council IT systems, social media platforms, email or personal devices for Council-related work. It also applies to any digital communication that relates to Council business.

4. Official Council Social Media Channels

The Council operates official social media accounts including a website, Facebook page, and X (formerly Twitter). Only the Communications Officer, Clerk or Deputy Clerk may post on these platforms. No other individuals, including councillors, may post on behalf of the Council.

5. Conduct & Content Standards

All Council communications must be civil, respectful and lawful. Content must not be defamatory, offensive, discriminatory, or infringe copyright. Personal data should not be shared unless necessary and lawful. Political advertising is prohibited.

6. Moderation & Removal of Content

The Council reserves the right to remove any content from its platforms that is obscene, racist, defamatory, threatening, libellous or otherwise inappropriate. Repeat offenders may be blocked. Posts alleging policy or legal breaches will be referred to formal channels.

7. Councillor Use of Social Media (personal vs official capacity)

Councillors must not post on official Council channels. When using personal social media, councillors must make clear they are expressing personal views and not speaking on behalf of the Council. They must avoid predetermination and maintain confidentiality.

8. WhatsApp & Messaging Apps (rules, FOI, predetermination)

WhatsApp must not be used for Council decision-making or discussions that risk predetermination. Staff must not be included in councillor WhatsApp groups. WhatsApp content may be subject to Freedom of Information (FOI) requests. It is not an official communication channel and must not be used to instruct staff or conduct Council business.

9. Community Hub / Third-Party Pages

Councillors must not respond to Council-related posts on third-party platforms such as the Hatfield Peverel Community Hub. Abusive or defamatory content should be reported to group administrators or relevant authorities. Officers may post factual updates with comments disabled.

10. Website Content & Responsibilities

Officers manage the Council website.

11. Email & Electronic Communication

Council email accounts are for Council business. Limited personal use is permitted during breaks. Staff must use Council email accounts; councillors may use personal devices but must use Council email addresses for official correspondence. All emails are subject to FOI and data protection laws.

12. IT & Equipment Use (staff vs councillors, limited personal use)

Staff must use Council-issued devices. Reasonable personal use is permitted during breaks. Devices must be used responsibly, kept secure and maintained in good condition. Councillors may use their own devices for all Council work, subject to security requirements.

13. Use of Personal Devices (BYOD – councillors permitted for all work)

Councillors may use personal devices for all Council work. Devices must be protected with passwords or PINs, kept updated and used in accordance with data protection principles. Confidential data must not be stored locally unless encrypted and access-controlled.

14. Remote & Home Working

Staff and councillors working remotely must ensure secure access to Council systems, avoid public Wi-Fi and protect confidential information. Devices must be locked when unattended and data must be stored securely.

15. Cybersecurity & Passwords (NCSC-aligned)

All users must use strong passwords based on the NCSC's 'three random words' guidance. Devices must be kept updated, protected with PINs or passwords, and configured to lock after inactivity. Council data must not be stored on unsecured devices or services.

16. Monitoring (proportionate, lawful)

The Council may monitor IT and communication systems to ensure compliance with this policy. Monitoring will be proportionate, lawful and limited to what is necessary to protect Council systems and data.

17. Data Protection & Confidentiality

All users must comply with the UK GDPR and Data Protection Act 2018. Personal data must be processed lawfully, fairly and securely. Confidential information must not be disclosed without authorisation.

18. Review of Policy

This policy will be reviewed annually or in response to legislative or operational changes. Last reviewed: May 2026.