SOCIAL MEDIA & EMAIL POLICY

Contents

This Social Media & Email Policy was adopted by the council at its meeting held on 26th May 2026.

SOCIAL MEDIA & EMAIL POLICY

1. POLICY STATEMENT

This policy is intended to help all employees, volunteers and Councillors make appropriate decisions about the use of social media such as blogs, social networking websites, forums, message boards, or comments on web-articles, such as Facebook, Instagram, LinkedIn, X (formerly Twitter), and other platforms, along with email communications. This policy applies to all social media sites, including new and emerging platforms; the principles remain the same regardless of platform.

This policy outlines the standards we require employees, volunteers, and Councillors to observe when using social media, the circumstances in which we will monitor your use of social media and emails, and the action we will take in respect of breaches of this policy.

You are advised to contact the Executive Officer if you are unsure how this policy might apply to a particular situation.

2. THE SCOPE OF THE POLICY

All employees, volunteers and Councillors are expected to always comply with this policy to protect the privacy, confidentiality, and interests of our council.

Breach of this policy by employees may be dealt with under our Disciplinary Procedure and, in serious cases, may be treated as gross misconduct leading to summary dismissal. The use of social media and email is also included in the Employee Code of Conduct, making clear behavioural expectations in and out of work.

Breach of this policy by Councillors may be dealt with under the adopted Code of Conduct. This includes upholding the seven principles of public life and the reputation of the Council. Violations of this policy by Councillors will be referred to the Monitoring Officer at Northumberland County Council.

3. LEGAL AND STATUTORY CONSIDERATIONS

3.1 Legal Framework

The council will abide by all relevant and applicable laws, terms, and conditions to ensure the organisation is not exposed to risks. This includes, but is not exclusively limited to:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Freedom of Information Act 2000
- Online Safety Act 2023
- Public Sector Bodies (Websites and Mobile Applications) Accessibility Regulations 2018 — the current required standard under these Regulations is WCAG 2.2 AA (which superseded WCAG 2.1 AA in October 2024). Compliance with WCAG 2.2 AA is also required to satisfy Assertion 10 of the AGAR (Practitioners' Guide 2025), which all town and parish councils must declare compliance with from the 2025/26 financial year onwards
- Equality Act 2010
- Defamation Act 2013

- Computer Misuse Act 1990

3.2 Council Policies
Council use of social media must be undertaken in accordance with the council's policies and procedures, including but not limited to:

- IT Policy
- Press and Media Policy
- Data Protection and Privacy Policy
- FIO Policy
- Equality, Diversity and Inclusion Policy

3.3 Safeguarding
Use of social media sites will always be consistent with the council's duty to safeguard children, young people, and vulnerable adults, in accordance with relevant statutory requirements. Prior authorisation is required before posting images of minors, in line with safeguarding procedures, and must include appropriate consent from parents/guardians.

3.4 Political Neutrality
Employees using social media sites for business purposes must maintain political neutrality and not indicate individual political opinions.

3.5 Pre-election Period
In the six-week run up to a local, general, or European election – also known as the pre-election period – the council must not do or say anything that could be seen in any way to support any political party or candidate. During this period:

- The council will continue to publish important service announcements using social media but may have to remove responses if they are deemed overtly party political
- Existing content should be reviewed for potential political sensitivity
- Staff should defer publishing content that could be interpreted as influencing voters
- Responses to political comments or questions should be factual only and avoid opinion
- If in doubt, consult with the Executive Officer before posting any content

4. RESPONSIBILITY FOR IMPLEMENTATION OF THE POLICY
The council has overall responsibility for the effective operation of this policy.

The Executive Officer is responsible for monitoring and reviewing the operation of this policy and making recommendations for changes to minimise risks to our work.

All employees, volunteers and Councillors should ensure that they take the time to read and understand the policy. Any breach of this policy should be reported to the Executive Officer/Chair.

Questions regarding the content or application of this policy should be directed to the Executive Officer.

5. USING SOCIAL MEDIA SITES IN OUR NAME

5.1 Authorisation

Only the Executive Officer, or delegated officers, under the direction of the council, are permitted to post material on the council website and social media, in the council's name or on behalf of the council.

The Executive Officer is the Council's nominated Press Officer with the authority to issue official press releases. No other member of staff or members has the authority to issue public statements on behalf of the Council.

5.2 Sharing Official Content

Employees, volunteers, and Councillors are encouraged to share official press releases and postings made by the Executive Officer, on behalf of the council. The Council encourages positive use of social media to engage residents, promote council-supported events, share good news stories etc.

5.3 Account Security

Staff responsible for managing council social media accounts must:

- Use strong, unique passwords for each platform
- Enable two-factor authentication where available
- Never share login credentials via email or messaging
- Update passwords quarterly or when a staff member with access leaves
- Maintain a secure record of access details in line with information security policies

6. USING SOCIAL MEDIA

We recognise the importance of the internet in shaping public thinking about our council and community. We also recognise the importance of our employees, volunteers and Councillors joining in and helping shape local government conversation and direction through interaction in social media.

Before using social media on any matter which might affect the interests of the council ensure that you have read and understood this policy.

When posting personally on social media please ensure you are clear that any views expressed are personal and do not represent the council. Employees/councillors should not identify themselves as such, i.e. as a Cllr or an employee of the Council, if posting in a personal capacity.

7. RULES FOR USE OF SOCIAL MEDIA

Whenever you use social media, you must adhere to the following general rules:

7.1 Content Standards

- Do not upload, post, or forward a link to any abusive, obscene, discriminatory, harassing, derogatory or defamatory content.
- Offensive, obscene, or defamatory content also should not be forwarded, even if not originally authored by the forwarder.

- Any employee, volunteer or member who feels that they have been harassed or bullied or are offended by material posted or uploaded by a colleague onto a social media website should inform the Chair/Executive Officer.
- Never disclose commercially sensitive, personal private or confidential information. If you are unsure whether the information you wish to share falls within one of these categories, you should discuss this with Chair/Executive Officer.
- No information should be published that is not already known to be in the public domain, i.e. available on the Council's website, contained in minutes of meetings, stated in Council publicised policies and procedures, or approved by the Executive Officer (or officer under delegation).
- Do not upload, post, or forward any content belonging to a third party unless you have that third party's consent.

7.2 Legal Compliance

- Before you include a link to a third-party website, check that any terms and conditions of that website permit you to link to it.
- When making use of any social media platform, you must read and comply with its terms of use.
- Be honest and open but be mindful of the impact your contribution might make to people's perceptions of the council.
- You are personally responsible for content you publish into social media tools.

7.3 Conduct Standards

- Do not escalate heated discussions, try to be conciliatory, respectful and quote facts to lower the temperature and correct misrepresentations.
- Do not discuss employees.
- Always consider others' privacy and avoid discussing topics that may be inflammatory.
- Avoid publishing your contact details where they can be accessed and used widely by people you did not intend to see them and never publish anyone else's contact details.
- Be mindful that information published in this way may stay in the public domain indefinitely, without the opportunity for retrieval/deletion.
- Think about whether you are acting in a private capacity, or whether any impression might be conveyed that you are acting for and on behalf of Ashington Town Council.

7.4 Accessibility Requirements

- Ensure social media content is accessible to all users in accordance with the Public Sector Bodies (Websites and Mobile Applications) Accessibility Regulations 2018, meeting the current required standard of WCAG 2.2 AA. WCAG 2.2 superseded WCAG 2.1 as the applicable standard in October 2024 and is required for Assertion 10 compliance
- Include appropriate alternative text for all images

- Provide captions or transcripts for video content
- Use clear language and avoid unnecessary abbreviations or jargon
- Ensure colour contrast meets accessibility standards
- Ensure touch targets (buttons and interactive elements) on social media graphics and linked web content are of sufficient size for users with limited motor control — WCAG 2.2 (SC 2.5.8) requires a minimum target size of 24×24 CSS pixels
- Where the Council uses any online form, login, or authentication process linked from social media, ensure it does not require users to complete a cognitive function test (such as a complex CAPTCHA) as the only means of authentication — WCAG 2.2 (SC 3.3.8) requires an accessible authentication alternative
- Ensure any help mechanism or contact link provided on the Council website (such as a contact form, email link, or phone number) appears in a consistent location across pages — WCAG 2.2 (SC 3.2.6) requires consistent help placement to support users with cognitive disabilities
- Format hashtags using camel case (e.g., #TownCouncilMeeting rather than #towncouncilmeeting)

7.5 Use of AI and Automation Tools

- AI tools may be used to assist with content creation but must have human review before publication
- Automatically scheduled posts should be checked for appropriateness before their publication time
- Be transparent when using AI-generated content and ensure it meets our standards
- AI tools should not be used to respond to residents' queries without human oversight
- Ensure any AI tools used comply with our data protection obligations

8. MONITORING USE OF SOCIAL MEDIA WEBSITES

Employees, volunteers, and Councillors should be aware that any use of social media websites (whether accessed for council purposes) may be monitored and, where breaches of this policy are found, action may be taken against employees under the Disciplinary Procedure and in respect of Councillors, via the adopted Code of Conduct.

Social media monitoring may include any historical material still available online, not just content posted while employed.

Misuse of social media websites can, in certain circumstances, constitute a criminal offence or otherwise give rise to legal liability against the Council and its employees.

A serious case of uploading, posting, forwarding, or sharing a link to any of the following types of material on a social media website, whether in a professional or personal capacity, is likely to amount to gross misconduct (this list is not exhaustive):

- pornographic material (that is, writing, pictures, films, and video clips of a sexually explicit or arousing nature);
- a false and defamatory statement about any person or organisation;
- material which is offensive or obscene;
- material, which is criminal, discriminatory, derogatory or may cause embarrassment to the Council, Councillors, or our employees;
- confidential information about the council or anyone else;
- any other statement which is likely to create any liability (whether criminal or civil, and whether for you or the council); or
- material in breach of copyright or other intellectual property rights, or which invades the privacy of any person.

Any such action by Councillors will be addressed under the adopted Code of Conduct and be referred to the Monitoring Officer. Any such action by employees will be addressed under the Disciplinary Procedure and may result in summary dismissal.

Where evidence of misuse is found we may undertake a more detailed investigation in accordance with our Disciplinary Procedure, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or managers involved in the investigation. If necessary, such information may be handed to the police in connection with a criminal investigation.

Any breach of this policy should be reported to the Executive Officer and Chair of the Council.

9. HANDLING OF HARASSMENT AND ABUSE

9.1 Reporting Procedures

- Staff and councillors experiencing online harassment related to council business should report it immediately to the Executive Officer. Reports should include details of the platform, the nature of the behaviour, and the account or identity of the person responsible where known. The Executive Officer will assess all reports promptly and in accordance with the Council's Vexatious, Persistent, Aggressive and Abusive Complaints Policy, which sets out the staged response framework for managing and escalating unacceptable behaviour
- Capture screenshots or records of concerning communications before blocking or deleting
- In cases of serious threats, contact the police directly and inform the Executive Officer. Where a communication conveys a threat of death or serious harm, or knowingly sends false information with intent to cause psychological or physical harm, this may constitute a criminal offence under the Online Safety Act 2023 (sections 179 and 181, in force 31 January 2024). The Executive Officer will advise on whether a formal police report is appropriate and will ensure that evidence is preserved in a form suitable to support any investigation

9.2 Response Actions

- Do not engage with abusive content or harassment

- The Executive Officer will determine appropriate responses to serious incidents
- Legal advice may be sought in cases of persistent harassment or threats
- Where online harassment constitutes or escalates to unacceptable behaviour under the Council's Vexatious, Persistent, Aggressive and Abusive Complaints Policy, the Executive Officer will invoke the staged response set out in that policy — beginning with a written warning, progressing to formal communication restrictions, and where necessary to immediate action including ceasing all contact and reporting to the police. Decisions to restrict or block individuals will be documented and the individual informed in accordance with that policy
- The Council may block or restrict individuals from its social media accounts where their conduct is abusive, threatening, or persistently unreasonable. Blocking is a protective measure and does not prevent the individual from contacting the Council through other channels. The decision to block will be taken by the Executive Officer, documented, and reviewed at six-monthly intervals in line with the Vexatious Complaints Policy
- Support will be provided to affected staff or councillors

9.3 Preventative Measures

- Regular review of privacy settings on social media accounts
- Training on identifying and handling potential harassment situations
- Clear documentation of incidents and responses
- The Council has a proactive duty under the Worker Protection (Amendment of Equality Act 2010) Act 2023 (in force 26 October 2024) to take reasonable steps to prevent sexual harassment of employees, including harassment that occurs through online or digital channels in the course of employment. This extends to harassment by members of the public, contractors, or others via social media.
- The Crime and Policing Act 2026 (Royal Assent 29 April 2026) strengthens protections for public officeholders including local councillors against stalking and harassment. Where online behaviour directed at a councillor in their official capacity amounts to a course of conduct causing fear or distress, the Executive Officer will advise the affected councillor on available legal remedies including Stalking Protection Orders and police referral under this Act

10. RULES FOR THE USE OF EMAILS

10.1 General Principles

Emails are the primary method to promote effective communication on matters relating to Council business and therefore should be used for that purpose only.

Employees must use official Council email addresses for all Council business. Members must use a hosted email address on a council-owned domain for all Council business. Free consumer email services such as Gmail, Hotmail, Yahoo, or Outlook.com must not be used for Council correspondence — this is a requirement under AGAR Assertion 10 (Practitioners' Guide 2025). The domain suffix does not need to be .gov.uk, but the email service must be a paid, hosted service on a domain owned and controlled by the Council (for example

@ashingtontowncouncil.gov.uk or an equivalent council-owned domain). Free services are prohibited because the Council does not own or control those platforms, which creates risks for data governance, records management, and compliance with Freedom of Information and Subject Access requests. Any member not yet using a compliant hosted email address should contact the Executive Officer to arrange this as a matter of priority.

10.2 Email Standards

Messages sent by email should be written in accordance with the standards of any form of written communication, and the content and language used in the message must be consistent with Council best practice. Messages should be clear and concise and directed to those individuals with 'a need to know.'

Councillors and employees should avoid revealing personal information about others online, this includes by email.

If a sensitive or contentious matter needs to be addressed, consider speaking to the recipient first, by telephone or in person, then follow-up with an email.

10.3 Prohibited Use

Emails should not be used for:

- Spreading gossip
- Personal gain
- Breaching any other Council policy
- Actions inconsistent with Member's Code of Conduct or an Employee's Contract of Employment

10.4 Group Communications

When responding to a large group of recipients, the 'reply all' facility should be used, but caution should be taken that others have not copied in recipients who should not be disclosed to or who have not agreed to share their contact details.

10.5 Confidentiality

Confidential information should not be sent externally without the approval of the Executive Officer.

10.6 Legal Implications

Erroneous email messages can give rise to legal action against the Council or individual Councillors. Claims for defamation, harassment, breach of confidentiality or contract could result. It is vital that email messages be treated like any other form of correspondence and, where necessary, copies should be saved and retained. Messages are disclosable in any legal action commenced against the Council or individual Councillors.

10.7 External Communications

External emails received by individual Councillors should be forwarded to the Executive Officer, and the Chair if appropriate, who will in turn forward to all Councillors.

10.8 Email Security

- Use strong, unique passwords for email accounts
- Enable two-factor authentication where available

- Be vigilant regarding phishing attempts
- Do not open suspicious attachments or links
- Report potential security breaches immediately

10.9 Disciplinary Action

Misuse of emails in the following categories can lead to action being taken in accordance with the Disciplinary Procedure or the Code of Conduct:

- Defamation of character
- Inappropriate, obscene, or offensive content
- Untrue or malicious content
- Any discrimination in line with the Council's Equality Policy
- Breach of confidentiality

11. SOCIAL MEDIA ARCHIVING AND RECORDS MANAGEMENT

11.1 Retention Requirements

- Social media content constitutes an official council record and must be managed accordingly
- Content should be retained in line with the council's Records Management Policy
- Significant social media interactions should be documented and preserved

11.2 Archiving Procedures

- Regular backups of social media content should be maintained
- Screenshots or exports of important conversations should be saved securely
- Third-party archiving tools may be used if they comply with data protection requirements

11.3 Records Management

- Social media records should be incorporated into the council's information asset register
- Deletion of social media content must follow approved retention schedules
- FOI and subject access requests may require retrieval of archived social media content

12. TRAINING REQUIREMENTS

12.1 Mandatory Training

- All staff with social media responsibilities must complete basic social media training
- All councillors should receive social media awareness training upon election/appointment
- Staff managing council accounts must complete advanced social media management training

12.2 Refresher Training

- Annual refresher training on this policy for all relevant staff and councillors

- Additional training when significant policy changes occur
- Specialized training for new platforms or tools before implementation

12.3 Documentation

- Training completion must be documented and records maintained
- Regular skills assessment to identify additional training needs
- Feedback mechanisms to improve training effectiveness

13. RISK ASSESSMENT PROCESS

13.1 Regular Assessment

- Annual formal risk assessment of council social media use
- Quarterly review of emerging platforms and technologies
- Ad hoc assessments when implementing new communication tools

13.2 Risk Mitigation

- Documented strategies to address identified risks
- Clear approval processes for new platforms or uses
- Regular security reviews of social media accounts

13.3 Incident Response

- Documented procedures for handling social media incidents
- Clear escalation paths for different types of incidents
- Post-incident review process to prevent recurrence

14. MONITORING AND REVIEW OF THIS POLICY

The Executive Officer shall be responsible for reviewing this policy annually to ensure that it meets legal requirements and reflects best practice. Changes will be considered by Council. The review should include:

- Assessment of compliance with current legislation
- Evaluation of effectiveness in guiding staff and councillors
- Incorporation of lessons learned from any incidents
- Consideration of new technologies and platforms
- Consultation with stakeholders on potential improvements

APPENDIX A: GLOSSARY OF TERMS

AI (Artificial Intelligence): Computer systems able to perform tasks that normally require human intelligence.

Data Breach: A security incident resulting in accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

GDPR (General Data Protection Regulation): The legal framework that sets guidelines for the collection and processing of personal information.

Social Media: Websites and applications that enable users to create and share content or participate in social networking.

Two-Factor Authentication: A security process requiring two distinct forms of identification before accessing an account.

APPENDIX B: QUICK REFERENCE GUIDE

DO:

- Use official council channels for council business
- Enable security features on all accounts
- Be respectful and professional at all times
- Make content accessible to all users
- Think before you post – content may be permanent
- Report policy breaches promptly

DON'T:

- Share confidential information
- Express political opinions when representing the council
- Engage with abusive users
- Use personal accounts for official business
- Post without considering legal implications
- Share login details with unauthorized individuals

IF IN DOUBT:

Contact the Executive Officer for guidance before posting