# Watton Town Council

# Information Technology, Communications & Social Media Policy

Adopted 08.11.2022

**Information Technology (IT), Communications & Social Media Policy**

## ABOUT THIS POLICY

The Watton Town Council IT and Communications Systems are intended to promote effective communication and working practices within our organisation and should be read in conjunction with our Privacy and Data Protection Policies.

This policy outlines the standards you must observe when using these systems, the circumstances in which we will monitor your use, and the action we will take concerning breaches of these standards.

In the context of this policy, IT equipment includes desktop computers, laptops, tablets, telephones, smart mobile phones, network routers, modems or any other device which provides an electronic method for internet access, messaging or document storage.

Electric Communications includes emails, texts and any other direct messaging tool used by Councillors and staff on Social media platforms.

This policy covers all users: - employees, Councillors, contractors, interns, School/University placements, casual workers, agency workers and anyone with access to our communication systems.

Misuse of IT and Communications systems can cause reputational damage to the Council and place us vulnerable to prosecution. Any Breach of this policy may be dealt with under our Standards Procedure (Councillor s) or Disciplinary Procedure (staff) and, in serious cases, may be treated as gross misconduct leading to summary dismissal. A breach by a user will be reported to the appropriate Line Manager in the first instance.

This policy does not form part of any employee's employment contract, and we may amend it at any time.

## 1. PERSONNEL RESPONSIBLE FOR THE POLICY

1.1 The Clerk and the Deputy Clerk to The Council (The Clerk) are responsible for effectively implementing this policy.
1.2 The Clerk is responsible for ensuring compliance with this policy, and all Councillors and employees must comply.

**1.3** All requests for permission or assistance under any policy provisions will be dealt with by The Clerk, who may specify certain equipment standards or procedures to ensure security and compatibility.

**1.4** Council to review annually or if circumstances or law changes.

## 2. CORRESPONDENCE

**2.1** Receiving Correspondence - Under normal circumstances, the Clerk, as the Proper Officer of the Council, is authorised to receive all correspondence. Where correspondence needs to be

shared with Councillors, this should routinely be done electronically. Exceptionally, hard copies can be either requested or viewed at the Office.

**2.2** Responding to Correspondence - As Proper Officer, the Clerk will respond to correspondence received or may write correspondence related to the stated business and day-to-day management of the activities or adopted policies of the Council.

**2.3** It is noted that electronic communications are the preferred means of correspondence. However, the current policy is that correspondence should generally be responded to in the format received.

## 3. WORKING WITH THE MEDIA

**3.1** The Clerk, if contacted by the media for information, must only give the facts and the view of the Council as a body.

**3.2** If the press contacts a Councillor directly, the Town Council expects any comments given not to deviate from Council policy or decision and expects Councillors to act with integrity in giving a suitable response.

**3.3** Councillors should not use their association with the Town Council for political purposes in the press or promote business or personal interests.

**3.4** Photographs relating to Town Council matters should not be supplied to the press without permission from the Clerk or Town Council.

**3.5** Official Press releases. The Clerk is responsible for overseeing press releases on behalf of the Town Council.

**3.6** Press releases can be compiled by other members of staff or Councillors but should be approved by the Clerk or full Council dependent on content. Press statements must be clear, consistent, based on fact and in keeping with the Council's policies, aims and priorities.

**3.7** Councillors can issue *personal* press releases. These must be signed personally without the word Councillor attached to the name. Each press release should also contain the following statement: *"This is a personal statement and is not necessarily the view of the Town Council"*.

## 4. EQUIPMENT SECURITY AND PASSWORDS

**4.1** Councillors and employees (you) are responsible for the security of all IT equipment allocated to or used by you. You must not allow it to be used by anyone other than under this policy.

**4.2** You are responsible for the security of any computer terminal/VPN you use. You must lock your terminal or log off when leaving it unattended or on leaving your Office to prevent unauthorised users from accessing the system in your absence. Anyone not authorised to access our network should only be allowed to use terminals under supervision.

**4.3** Watton Town Council Office Desktop PCs and telephones or computer equipment cabling should not be moved or tampered with without consulting the IT Service provider.

**4.4** You should use passwords on all IT equipment, particularly items you take out of your Office. You must keep your passwords confidential and change them regularly. In addition, you must not use another person's username and password, make it available, or allow anyone else to log on using your username and password.

**4.5** If you have been issued with a laptop, tablet computer, smartphone, or other mobile device, you must ensure that it is always kept secure, especially when travelling to external meetings and events. For example, passwords must be used to secure access to data on such equipment to ensure that confidential data is protected in the event of loss or theft. You should also be aware that when using equipment away from the workplace, third parties could see documents and subject data on the device.

**4.6** When working from home or remotely or using your personally owned desktop, laptop, tablet, smartphone, or other mobile devices, all parts of paragraphs 3.1 to 3.5 still apply.

**4.7** On the termination of employment (for any reason), you must provide details of your passwords to the IT Service Provider and return all Council-owned equipment.

## 5. SYSTEMS AND DATA SECURITY

**5.1** You must not delete, destroy or modify existing systems, programs, information, or data (except as authorised in the proper performance of your duties).

**5.2** You must not download or install software from external sources without the proper authorisation of The Clerk. This includes instant messaging programs, screensavers, photos, video clips and music file media. Incoming files and data should always be virus-checked before they are downloaded. If in doubt, staff should seek advice from the IT Service Provider.

**5.3** You must not attach any device or equipment to our systems without authorisation from The Clerk. This includes any USB flash drive, tablet, smartphone, or other similar devices, whether connected via the USB port, infra-red connection wi-fi or in any other way. Any equipment attached to our systems must have virus protection and firewalls.

**5.4** We monitor all emails passing through our system for viruses. Therefore, you should exercise extreme caution when opening unsolicited emails from unknown sources or an email that appears suspicious (for example, if it contains a file whose name ends in .exe). If you suspect your computer may have a virus stop using it immediately and inform the IT Service Provider.

**5.5** We reserve the right to delete or block access to emails or attachments in the interests of security. We also reserve the right not to transmit any email message.

**5.6** You should not attempt to gain access to restricted areas of our network or any password-protected information except as authorised in the proper performance of your duties.

**5.7** You must be particularly vigilant if you use our or your own IT equipment to access Council software outside the workplace and take such precautions as we may require against importing viruses or compromising system security. The system contains information that is confidential and subject to data protection legislation. Such information must be treated with extreme care under our Data Protection Policy.][This would apply if you use your personal computers when working from home.

## 6. EMAIL

**6.1** Although email is a vital business tool, you should always consider if it is the appropriate method for each particular communication. Correspondence with third parties by email should be written as professionally as a letter. Messages should be concise and directed only to relevant individuals. Our standard disclaimer should always be included. Hard copies of emails should be kept in the appropriate file.

**6.2** You should not routinely use 'reply' or 'reply to all' when responding to emails as this will increase the size of the chain as well as risk a Data Breach by sharing the subject Data of others, as well as potentially sensitive information to those who are not intended to see it. This also clogs the server with repeated data and can cause unnecessary work in the event of either a Freedom of Information Request (FOI 2000) or a Subject Access request under the UK GDPR 2018.

**6.3** You must not send abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory, pornographic, or inappropriate emails. Anyone who feels that they are (or have been) harassed or bullied, or offended by material received from a colleague via email should inform The Clerk in the first instance.

**6.4** You should take care with the content of all email messages, as incorrect or improper statements can give rise to; claims for discrimination, harassment, defamation, breach of confidentiality, breach of contract, *et al*. Remember that you have no control over where the recipient may forward your email. Avoid saying anything that would cause offence or embarrassment if your email was forwarded to colleagues or third parties or found its way into the public domain.

**6.5** Email messages are required to be disclosed in legal proceedings in the same way as paper documents. Deletion from a user's inbox or archives does not mean that an email cannot be recovered for disclosure. All email messages should be treated as potentially retrievable, either from the main server or by specialist software.

**6.6** In general, you should not:
**(a)** Send, forward or read private emails at work that you would not want a third party to read.
**(b)** Send or forward chain mail, junk mail, cartoons, jokes or gossip. Aside from the irrelevance of such action, you could also forward Subject Data to unauthorised recipients.
**(c)** Contribute to system congestion by sending trivial messages, copying or forwarding emails to those who do not need to receive them, or unnecessarily using "reply all" on an email with a large distribution list.
**(d)** Sell or advertise using our communication systems or broadcast messages about lost property, sponsorship, or charitable appeals, without the specific authority of the Clerk of the Deputy Clerk.

**(e)** Agree to terms, enter contractual commitments, or make representations by email unless the appropriate authority has been obtained. A name typed at the end of an email is legally considered a signature, like a name written at the end of a letter.
**(f)** Download or share text, music, or any other content without the permission of The Clerk.
**(g)** Send emails from another person's email address (unless authorised) or under an assumed name.
**(h)** Send confidential messages via any messaging platform that is not known to be secure and has not been authorised by The Clerk.

**6.7** If you receive an email in error, you should inform the sender.

**6.8** All emails sent from (name)@wattontownCouncil.gov.uk should display, as part of the prepopulated signature block, a caveat to inform the recipients of emails sent in error of what they should do. Currently, Watton Town Council use: -

*"General Data Protection Regulation: The Council's Privacy Statement can be viewed here Disclaimer: This email may contain privileged and/or confidential information. If you receive this in error, please notify the sender immediately and do not use, rely upon, copy, forward or disclose its content to any other party. Any views or opinions expressed are those of the author and do not necessarily represent those of the Town Council. Viruses: Although we have taken steps to ensure that this email and attachments are free from virus, we advise that in keeping with good computing practice the recipient should ensure they are actually virus free"*

**6.9** All marketing, 'round-robin' newsletters or any other 'cold-call' emails should include a link allowing the recipient to 'unsubscribe'. Any request to unsubscribe should be sent an acknowledgement email and the Subject Data removed from the mailing list.

**6.10** Employees should not use their private email account to send or receive emails for Council business and should only use the email account provided by the Council.

**6.11** Whilst there is no restriction on Councillors using their private email addresses, they should be encouraged to use email addresses provided by The Council where possible. This is particularly significant when the Council needs to manage responses to either a Subject Access Request or Freedom of Information Request.

## 7. USING THE INTERNET

**7.1** Internet access is provided primarily for business purposes. Occasional personal use may be permitted as stated in Paragraph 7.

**7.2** When a website is visited, devices such as cookies, tags or web beacons may enable the site owner to identify and monitor visitors. If the website is of the kind described in Paragraph 9, such a marker could be a source of embarrassment to the visitor and us, especially if inappropriate material has been accessed, downloaded, stored, or forwarded. Such actions may also, in certain circumstances, amount to a criminal offence if, for example, the material is offensive.

**7.3** You should not access any web page or download any image, document or other files from the internet which could be regarded as illegal, offensive, discriminatory, in bad taste, or immoral. Even legal web content in the UK may still be inappropriate and fall within this

prohibition. Generally, if any person (whether intending to view the page or not) might be offended by the contents of a page, or if the fact that our software has accessed the page or file might be a source of embarrassment if made public, then viewing it will be a breach of this policy.

## 8. PERSONAL USE OF OUR SYSTEMS

**8.1** We permit the occasional use of our internet, email, and telephone systems to send personal emails, browse the internet and make personal telephone calls subject to certain conditions below. Personal use is a privilege and not an entitlement. It must not be overused or abused. We may withdraw permission at any time or restrict access at our discretion.

**8.2** Personal use must meet the following conditions:
**(a)** Use must be minimal and take place substantially out of normal working hours
**(b)** Use must not interfere with business or office commitments.
**(c)** Use must not commit us to any marginal costs.
**(d)** Use must comply with this and our other policies, including our Data Protection Policy, Privacy Policy and code of conduct.

**8.3** You should be aware that personal use of our systems may be monitored (see Paragraph 8). Where breaches of this policy are found, action may be taken under the disciplinary procedure (see Paragraph 9).

## 9. MONITORING

**9.1** Monitoring is only done to the extent permitted or required by law and as necessary and justifiable for business purposes.

**9.2** Our systems enable us to monitor the Office telephone, email, voicemail, internet, and other communications. -

**9.3** For business reasons and to carry out legal obligations in our role as an employer, use of our telephone and computer systems, and any personal use of them, may be continually monitored by automated software or otherwise.

**9.4** We reserve the right to retrieve the contents of email messages relating to Watton Town Council's business interests.

**9.5** We reserve the right to check internet usage (including pages visited and searches made) as reasonably necessary in the interests of Watton Town Council

**9.6** Watton Town Council's business interests include the following purposes (this list is not exhaustive):
**(a)** To monitor whether the use of the email system or the internet is legitimate and covered under this policy.
**(b)** To find or retrieve messages lost due to computer failure.
**(c)** To assist in the investigation of alleged wrongdoing.
**(d)** To comply with any legal obligation.

## 10. PROHIBITED USE OF OUR SYSTEMS

**10.1** Misuse or excessive personal use of Watton Town Council telephone or email system or inappropriate internet use will be dealt with under our Disciplinary Procedure or the Standards Arrangements.

*How to complain about a District, Town or Parish Councillor in Breckland.*
***https://www.breckland.gov.uk/article/15341/Standards-Arrangements***

Misuse of the internet can, in some circumstances, be a criminal offence. However, it will usually amount to gross misconduct to misuse our systems by participating in online gambling, forwarding chain letters, or by creating, viewing, accessing, transmitting, or downloading any of the following material (this list is not conclusive):

**(a)** Pornographic material (any form of writing, images, audio or video clips of a sexually explicit).
**(b)** Offensive, obscene, or illegal material or other material which is liable to cause embarrassment to us as a Town Council or in any way offend others who may receive it.
**(c)** A false and defamatory statement about any person or organisation.
**(d)** Material that is discriminatory in any way to others, especially on the grounds of ethnicity, age, religious belief or gender identity.
**(e)** Confidential information about us, our business, any of our Councillors, staff, service providers or those with whom we have a legitimate contact. (except as authorised in the proper performance of your duties).
**(f)** Any other statement likely to amount to a criminal or civil offence (for you or The Council).
**(g)** Material in breach of copyright.

**10.2** Where evidence of misuse is found, we may conduct a more detailed investigation under the Standards/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 Standards/Disciplinary Procedure. In addition, such information may be handed to the appropriate law enforcement agencies concerning a criminal investigation if necessary.

## SOCIAL MEDIA

### 11. COMPLIANCE WITH RELATED POLICIES AND AGREEMENTS.

**11.1** Social Media should never be used in a way that breaches any of our other policies. If an internet post breaches our policies in another forum, it will also breach them online. For example, you are prohibited from using Social Media to:
**(a)** breach our IT and Communications Systems Policy.
**(b)** breach our obligations concerning the rules of relevant regulatory bodies.
**(c)** breach any obligations contained in those policies relating to confidentiality.
**(d)** breach our Disciplinary Policy or procedures.
**(e)** harass or bully others.
**(f)** unlawfully discriminate against other staff or any third party or breach our Equal Opportunities Policy.
**(g)** breach our Data Protection Policy (for example, never disclose personal information about a colleague, a member of the public or any other data subject online); or
**(h)** breach any other laws or regulatory requirements.

**11.2** You should never provide references for other individuals on social or professional networking sites. Positive or negative references can be attributed to the Council and create legal liability for both the author of the reference and the Council.

**11.3** Anyone who breaches any of the above policies will be subject to disciplinary action up to and including termination of employment.

## 12. PERSONAL USE OF SOCIAL MEDIA

Personal use of Social Media is NOT permitted during working hours or at any time.

## 13. PROHIBITED USE OF SOCIAL MEDIA

**13.1** You must avoid making any Social Media communications that could directly or indirectly damage the interests or reputation of Watton Town Council.

**13.2** You must not use Social Media to defame or disparage Watton Town Council, any Councillor or member of the Council staff or any third party, to harass, bully or unlawfully discriminate against staff or third parties, make a false or misleading statement, or to impersonate colleagues or third parties.

**13.3** You must not express opinions on our behalf via Social Media unless expressly authorised by The Clerk.

**13.4** You must not post comments about sensitive Council-related topics, such as our performance, or do anything to jeopardise confidential information, intellectual property, and brand or otherwise damage the excellent reputation of **Watton Town Council.**

**13.5** Details of business contacts made during your employment shall be considered personal data controlled by **Watton Town Council.** Therefore, once The Council no longer employs you, you must provide us with all such information and confirm that you have deleted these details from your records.

**13.6** Any misuse of Social Media that directly or indirectly alludes to **Watton Town Council** should be reported to The Clerk.

## 14. COUNCIL BUSINESS USE OF SOCIAL MEDIA

**14.1** If your duties require you to post or speak on behalf of The Council on a Social Media platform, you must seek approval for such communication from The Clerk, who may require you to undergo training before you do so and impose specific requirements restrictions on your activities.

**14.2** Likewise, if you are contacted for comments about the Council for publication anywhere, including in the press or any other Social Media outlet, you must direct the enquiry to your Line Manager and not respond without written approval.

**14.3** The use of Social Media for Council purposes is subject to the remainder of this policy.

## 15. GUIDELINES FOR RESPONSIBLE PERSONAL USE OF SOCIAL MEDIA

**15.1** You should make it clear in Social Media postings or personal profiles(s) that you speak on your behalf and not that of The Council. Write in the first person and use your personal email address.

**15.2** Be respectful to others when making any statement on Social Media and be aware that you are personally responsible for these communications published on the internet for anyone to see.

**15.3** If you disclose your affiliation to Watton Town Council on your profile or in any Social Media postings (Linkedin as an example), you must state that your views do not represent those of The Council (unless you are authorised to speak on our behalf as set out in Paragraph 5.3). You should also ensure that your profile and any content you post are consistent with the professional image you present to the public and colleagues.

**15.4** If you are uncertain, concerned, or doubt the appropriateness of any statement or posting, trust your instinct and refrain from posting it.

**15.5** If you see any Social Media content written by anyone else that disparages or reflects poorly on us, you should immediately inform The Clerk.

## 16. MONITORING

**16.1** We reserve the right to monitor, intercept, and review staff activities without further notice using our IT resources and communications systems. This includes but is not limited to Social Media postings and activities to ensure that our rules are complied with and for legitimate business purposes. You consent to such monitoring by using such resources and systems.

## 17. RECRUITMENT

We may use internet searches to perform due diligence on candidates during recruitment. Where we do this, we will act under our Data Protection and Equal Opportunities obligations.

## 18. BREACH OF THIS POLICY

**18.1** Breach of this policy may result in disciplinary action up to and including dismissal. Any Councillor or staff member suspected of breaching this policy will be required to cooperate with our investigation, which may involve handing over relevant passwords and login details.

**18.2** You may be required to remove any Social Media content that we consider to violate this policy. Failure to comply with such a request may result in disciplinary action.

-END-

AMENDMENT RECORD

Any amendment to this policy should be recorded here, with the version and date in the footer updated accordingly.

| Amendment no | Creating version No. | Date | Amended by | Signed off by |
|---|---|---|---|---|
| 0 | 1 | Date of roll-out | | |
| Details of amendment<br>Version 1 of this document was approved and published. | | | | |
| Amendment no | Creating version No. | Date of amendment | Amended by | Signed off by |
| | | | | |
| Details of amendment | | | | |
| | | | | |
| Amendment no | Creating version No. | Date of amendment | Amended by | Signed off by |
| | | | | |
| Details of amendment | | | | |
| Amendment no | Creating version No. | Date of amendment | Amended by | Signed off by |
| | | | | |
| Details of amendment | | | | |
| Amendment no | Creating version No. | Date of amendment | Amended by | Signed off by |
| | | | | |
| Details of amendment | | | | |