

Social media policy and guidance

This policy applies to staff and elected members.

1. Background

Social media is a key communications platform for the council and widely accepted as making a significant positive contribution to delivering the council's strategic aims and communications programme.

Social media plays an important role in engaging with our residents, businesses, not-for-profits and partners and can significantly help us facilitate two-way communication with a broad group of key stakeholders. Its power should not be underestimated.

Tower Hamlets Council's key corporate accounts (managed by the communications team) and other official accounts (managed by approved council service areas) are [listed on our website](#).

It is also common practice for elected members and some council officers to hold 'personal' social media accounts that are broadly and visibly used to engage with our stakeholders and through which they list their roles. They are therefore considered to be representing the council.

All of these accounts together help the council to have a strong, open, accountable and approachable presence on social media, and allow the council as a whole and our staff as individuals to have an active voice in our community.

This activity is bound by a policy, in order to minimise the risks associated with using social media.

2. Benefits and risks

Social media gives us an excellent opportunity to reach and engage with a large audience. It is an important way that the council communicates news, events, decisions and policy. It also supports our plan to save the council money and improve customer services by enabling residents to complete transactions and get support online.

However, there are also risks associated with social media use, including:

- Damage to the council's reputation as a result of negative comments or criticism on social media, which can be compounded by press coverage of the issue.
- Disclosure of confidential information or breaches of safeguarding responsibilities.
- Civil or criminal liability resulting from contraventions of statutory provisions or other unlawful conduct.

- Trolling (when someone posts deliberately inflammatory messages to invoke a response) or offensive language, unsuitable or inappropriate posts and comments targeting the council.
- Malicious software attacks (virus, malware or phishing) or social engineering attacks.

3. Purpose and application

The policy applies to all council employees (including contractors, temporary staff), members and anyone who has access to the council's network, systems and information.

This protocol covers the use of social media networks, online blogs, discussion forums and other digital activity to ensure consistent and appropriate use across the organisation. This includes (but is not limited to) Facebook pages and Facebook groups, Twitter, Instagram, LinkedIn, WhatsApp and Snapchat.

It aims to support successful two-way engagement with our residents and communities, and ensure appropriate, effective and consistent use of social media, while reducing associated risks.

Please note, additional social media usage policies are in place for:

1. Periods before an election or referendum (purdah), which applies to all council employees (including contractors, temporary staff) and members.
2. Council officers who manage corporate or official accounts.

These are available on the intranet.

4. Your responsibilities

4.1 Staff conduct on social media

This policy sets out the responsibilities of council employees (including contractors and temporary staff) when using social media. This includes any social media account that links you to the council or the work of the council (ie listed as your employer on your profile).

Employees must not use any social media tool for council business unless they have first received training from the council's communications team. They also need to be aware that the information they post on social media websites and associated documents can be subject to requests under the Freedom of Information Act 2000.

Employees must:

- Ensure they are aware of their responsibility to comply with good practice and the law so that the council is not brought into disrepute.
- Ensure the reputation of the council and its staff is not damaged and that children, young people and vulnerable adults are safeguarded by reducing the risk of positions of trust being abused or misused.
- Minimise the risk of misplaced or malicious allegations being made against those who work with vulnerable groups.

- Ensure they are able to clearly identify where information provided is legitimately representative of the council.
- Ensure the use of social media is aligned to this policy.
- Keep their personal and professional lives separate and always maintain appropriate professional boundaries.
- Be responsible for their own actions and conduct and avoid behaviour which could be misinterpreted by others or which could put themselves in a position where there is a conflict between their work for the council and their personal interests.
- Use social media in a professional, responsible and respectful way and must comply with the law in their online communications.
- Be aware that everything they post online is public, even with the strictest privacy settings. Once something is online, it can be copied and redistributed and it is easy to lose control of it. They should therefore assume that everything they post online will be permanent and will be shared.
- Be aware that when using social media for business purposes, they are acting as ambassadors for the council. What they say and post online will directly impact the reputation and image of the council.
- Ask and secure permission from the information owner before publishing any documents, photos, emails and/or reporting on social media any conversations that are intended to be private, confidential or internal.

Employees must not:

- Represent their personal views as those of the council on any social medium or discuss personal information about service users, their family members, council staff or any other professionals or organisations they interact with as part of their council job.
- Name or otherwise identify council staff, service users, former service users or their family members, or colleagues in social media conversations.
- Use social media or the internet in any way to attack, insult, abuse, harass, defame or otherwise make negative, offensive or discriminatory comments about council staff or service users, family members, colleagues, other professionals, other organisations, or the council or any other person.
- Browse, download, upload or distribute any material that could be considered inappropriate, offensive, defamatory, illegal or discriminatory.
- Undermine the integrity or impartiality of the council in anything they write.
- Express personal views and/or advocate a particular position on a subject, especially on issues associated with party-political controversy.
- Become 'friends' with those they come into contact with as part of their work for the council in ways that could lead to a conflict of interest or give rise to potential security and privacy issues.
- Cite or make reference to colleagues, clients, other third parties etc or post photographs of other people without their express consent.
- Use any information that they obtain in the course of their work for the council for personal gain or advantage or pass it on to others who may use it in such a way.
- Publish photographs, videos or any other types of image of service users and their families or images depicting employees (including contractors and temporary staff) wearing council uniforms or clothing with council logos or images identifying sensitive council premises (e.g. care homes) on personal accounts.
- Use council email addresses and other official contact details for setting up personal social media accounts or for communicating through such media.

If you have any questions about the use of social media you should consult the communications team.

4.2 Use of social media by members

The council welcomes members' use of social media in a public way (although it is not a requirement for members to use social media professionally or personally). If members are already using or planning to use social media in connection with their work as a member, they should ensure that they are familiar with the guidance that is set out within this policy and that their use of social media does not: use council resources for party political purposes; put the organisation's information and security systems at risk; or be damaging to the reputation of the council.

Social media can be used:

- to support members in the performance of their community leadership role
- to keep in touch with local views and opinions
- for political campaigning (not using the council's equipment or property)
- for campaigning on local issues.

Members should have due regard to data and internet security and ensure that communications remain proper and appropriate.

Do:

- Consider keeping your personal and member profile on social networking sites separate, have separate accounts and maintain appropriate professional boundaries.
- Be aware that as an elected member, you will most likely be seen as acting in your official capacity when you use social media, including in public pages as well as in WhatsApp and Facebook groups.
- Be aware that you will be seen as acting in your official capacity if you publish information that you could only have accessed by being a member.
- Ensure you use council facilities appropriately; if you use a council provided blog site or social networking area, any posts you make will be viewed as made in your official capacity and should not be used for political campaigning purposes.
- Feel able to make political points but be careful about being too specific or personal if referring to individuals. An attack on individuals may be seen as disrespectful, whereas general comments about another party or genuine comments on policy are less likely to be viewed as disrespectful.
- Set appropriate privacy settings for your blog or networking site especially if you have a private, non-political blog.
- Keep an eye out for defamatory or obscene posts from others on your social media accounts, blog or page and remove them as soon as possible to avoid the perception that you condone such views.
- Comply with equality and diversity laws and don't publish anything that might be seen as racist, sexist, ageist, homophobic, Islamophobic, anti-Semitic or anti-faith etc.
- Set up your Facebook account for your council work as a public 'page' that people can follow rather than a 'person' that people must 'friend'.

Don't:

- Make statements or post comments that could lead to potential liability or that you would not be prepared to make on paper or face to face.
- Request or accept a council employee or contractor providing services to the council as a 'friend' on a social networking site where this suggests close personal association.
- Use social media in any way to attack, insult, abuse, defame or otherwise make negative, offensive or discriminatory comments about council staff, service users, their family or friends, colleagues, other professionals, other organisations, the council or any other person.
- Publish confidential information that you may have obtained, or had access to as part of your role as a member. This includes all correspondence received from council employees (including contractors and temporary staff).
- Browse, download, upload or distribute any material that could be considered inappropriate, offensive, defamatory, illegal or discriminatory.
- Make conspicuous, excessive and continuous use of social media technology during the course of a council or committee meeting so as to give the impression to the public of not being respectful of the proceedings and, more seriously, taking decisions that are not based on full engagement with the facts and arguments.

When using social media, members are bound by the **members' code of conduct** in the same way as for any other written or verbal communication members may engage in. For further advice, speak to the communications team or the monitoring officer.

4.3 Safeguarding

Be aware of child safeguarding issues, as social media sites are often misused by offenders. The council encourages children and young people to stay safe online. Please remember that social media sites should only be used by those who meet the minimum age requirements for each site.

If you have any concerns about the safety of a child, you must report these to the **children's services hotline** on **020 7364 5006** (option three).

Adult safeguarding concerns should be reported to the **safeguarding adults hotline** on **020 7364 6085**.

4.4 Social media and the law

Everyone is responsible for using social media appropriately and must be mindful of the legal implications of inappropriate use of social media.

All employees and members need to be aware that they will be held personally responsible if they break the law when using social media (for example by posting something defamatory). The council may also be held liable for the acts of its employees and members.

All social media users need to be aware of the following legal issues and bear them in mind in when posting content. Liability can arise under the laws regulating:

- defamation (ie libel)
- copyright
- discrimination and victimisation
- contract
- human rights
- protection from harassment
- criminal law and the administration of justice
- data protection
- breaches of confidence.

Liability may also arise from a breach of professional standards.

4.5 Malware and online crime prevention

Social media can be used by the online criminal community to deliver malware, malicious software such as a virus, and facilitate schemes designed to damage property or steal confidential information. To minimise risks posed by such threats, you must adhere to the following guidelines:

- Do not use the same passwords for social media that you use to access council computers or devices.
- Do not follow links or download software on social media pages posted by individuals or organisations that you do not know.
- If any content you find on any social media webpage looks suspicious in any way, close your browser and do not return to that page.
- Connect to social media accounts only through trusted wifi networks or devices.

4.6 Pre-election period (purdah)

The pre-election period (purdah) is a specific period of time, usually around six weeks, in the run up to an election or referendum. It is a time of heightened sensitivity during which the council needs to take particular care over publicity and ensure that it maintains political neutrality. This means the council cannot promote any candidates for election, political parties, campaigns or political messages.

- **Remember that additional important policies apply during this period. This policy document is available on the intranet.**

4.7 Offensive and inappropriate content

We encourage the sharing of personal experiences and opinions and welcome robust, two-way discussion. However, it is important that we maintain a safe and respectful online environment for our community where all social media users, including residents and key stakeholders, feel welcome.

This section refers to content that includes:

- abusive or inappropriate behaviour or language
- obscene, profane, divisive, discriminatory, hateful, or racist content, links or images
- indecent, explicit or blasphemous material
- bullying, spam, trolling or deliberate disruptions to conversations
- repeated off-topic posts and comments by a single user
- posts that are false, misleading, threatening or defamatory to a person or organisation
- solicitations or advertisements for commercial gain
- infringements on an individual's privacy rights.

How to manage these issues appropriately:

- In line with the council's code of conduct, council staff must not post content that is offensive or inappropriate.
- If you manage an official council account or represent the council in a professional capacity, generally we would advise that you do not respond to content of this nature.
 - This is very different from negative comments, questions or criticism – these posts should be responded to in a polite, measured and reasonable fashion.
- Where possible, abusive and obscene comments/posts should be hidden or deleted (please note this is not currently possible on Twitter).
- These posts or accounts can and should also be reported to social media networks for official review (through the automated reporting tools on each social media platform).
- Abusive users can be 'blocked' but if you manage an official account, this should be used very rarely and after careful consideration as it can lead to further negative content being generated, and is unlikely to reduce the volume of offensive content being posted (you just won't be able to see it anymore).
- In extreme cases, social media content may be reported to the police for investigation.

If in doubt, or you would like to seek further advice or support, please contact the Head of External Communications.

5. Guidelines

5.1 Appropriate content

The following general guidelines should be followed when it comes to the managing content and discussions on social media accounts:

- The council itself must be politically neutral and should not be seen to promote any political party or messages. If you are a council officer, be careful not to comment on or share issues that are deemed to be politically controversial or sensitive, or which may be inaccurate.
- Questions relating specifically to council policy should be referred to the communications team / corporate social media account. Council officers must take care not to comment on issues of council policy. This is the role of the communications team, corporate accounts and elected members.
- Do not engage in any conduct that would not be acceptable in the workplace. Show consideration for others' privacy and for topics that may be considered objectionable or inflammatory – such as politics or religion.

- As a general rule, do not post any content or information that you would not be prepared to say to the general public, a newspaper, your manager or in other council communications.

If in doubt about any issue mentioned here, please refer to your line manager or a member of the communications team before responding. If the doubt cannot be resolved, leave it out.

5.2 Tone of voice

Social media by its nature is social, so you can use a more human, relaxed tone to your post. Don't be afraid of having genuine and open conversations with people.

However, please remember that you are representing the council and your social media posts should always be polite, professional and written using correct spelling and grammar. As much as possible, avoid using acronyms, abbreviations or 'text speak'.

5.3 Responding to negative comments

Negative comments or responses on social media should generally be responded to in a polite, helpful and prompt way. They are often an opportunity to answer or address a simple issue, set the record straight or signpost someone to get further support.

Where possible and appropriate, you should:

- Provide assistance by answering the question or signposting them to the correct source/process.
- Politely provide facts or key messages on the council's policy to set the record straight (this is useful for other people who may also be reading the posts).

Scenario specific advice:

- **Bad 'customer' experience**

If you receive a negative post that is a result of a bad personal experience, the respondent is very likely to be identifiable and have, in their opinion, a genuine grievance whether actual or perceived. Individuals, who have had a bad personal experience, can sometimes be helped by identifying that they have an issue and sharing the appropriate channels to have their issue successfully dealt with. Whether you choose to respond or not will depend on how you have been personally implicated, how damaging you consider their personal grievance to be, and the volume of attention the post is receiving.

If you are a member, this is likely to be a constituent who is unhappy about a local issue, a council policy or a part of a government policy for which you may be responsible. An individual may have had a lack of response to their issue through another channel or had a grievance not previously dealt with of a similar nature. This can usually be settled by resolving the issue in a satisfactory manner for the individual without being defensive.

- **Repeat poster**

Sometimes, even after replying to a comment or complaint with relevant information, someone on social media will continue to mention you and/or demand action be taken, even after you have given them all the information and/or taken all the action you can.

In these instances, politely reply to them saying you think you have done everything you can for them and that you are ending the conversation with them on this particular issue. Inevitably they will reply and may well continue to mention you in posts but you can safely ignore their posts once you have told them you can no longer help them.

- **Satirist or joker**

Satirists are individuals who are often recognisable by personal profile and are drawing attention to issues and their particular stance on that issue by making fun of a scenario, person or situation.

Monitor their post and the attention it draws and if they are proactively encouraging other people to share their point. Consider if this is likely to tip into another inappropriate category. Most satirists delight in the attention caused and direct responses can often inflame their point.

- **Trolls or abusive accounts (refer section 4.7 above)**

5.4 Personal use

Employees (including contractors and temporary staff) and members are of course permitted to use social and other digital media in their own time, but always need to be mindful of the employees' and members' codes of conduct.

It is important therefore that employees and members are aware that their actions could have an adverse impact on their professional role and/or on the council's image and reputation, and to avoid a potential conflict between their personal use of social media and their role.

Employees may wish to occasionally share 'proud' work moments or post about key work issues, for example sharing a public health message on their personal accounts. This is a personal choice but care should be taken. Staff may add a disclaimer to such posts, such as "these are my own views and opinions and not those of my employer".

For employees, personal use of social media sites is permitted at work but must be within the individual's own time ie during lunch breaks and on their own personal devices.

Do:

- Be aware of the dangers of sharing personal information online (including addresses, phone numbers, current locations and email addresses).
- Ensure you are aware of the privacy levels of your personal accounts and preferably, select the maximum privacy options to protect personal privacy.
- Keep passwords confidential, change them often and be careful about what is posted online. It is a good idea to use a separate email address just for social networking sites.
- Be cautious about inviting work colleagues to be 'friends' in personal social networking sites (with the exception of LinkedIn). Social networking sites blur the line between work and personal lives and so you should consider any potential impacts on your ability to maintain professional relationships in the workplace.

- Carefully consider 'friend requests' from service users, their families or friends or others (eg contractors, elected members), and accept them only if they are sure it will not put them in the position of having a real or apparent conflict of interest.
- Take personal responsibility for anything that you say online or anything posted from your account.
- Remember, what you post online will stay online forever, even with the 'right to be forgotten' legislation. There's no real such thing as deleting a social media post.

Do not:

- Edit open access online encyclopaedias such as Wikipedia in a personal capacity at work on a work device. This is because the source of the correction will be recorded as the council's IP address and the intervention will, therefore, appear as if it comes from the council itself.
- Identify communications as an employee (including contractors and temporary staff) of the council. This is to prevent information on these sites being linked with the council.
- Seek to establish social contact through any personal social media with any service users or ex-service users, their families or friends or other third parties connected to the council (eg contractors, elected members).

All employees (including contractors and temporary staff) should take care when commenting on council policies and practices and should not do so without the proper authorisation. Employees should avoid commenting on politically controversial issues or those that may interfere with democratic processes. This is particularly so for those who are in roles that are 'politically restricted' and are legally prohibited from speaking publicly with the apparent intention of affecting support for a political party (except where necessary as part of their official duties).

In the event that an employee's online activities impact on the council, this would no longer be a personal matter but would become a matter of concern for the council. Any reports of inappropriate activity by employees (including contractors and temporary staff), linking them to the council will be investigated in accordance with the council's disciplinary procedure and could result in disciplinary action, including dismissal.

6. How to raise concerns

Employees (including contractors and temporary staff) and members are reminded that it is our collective job to protect and enhance the reputation of the organisation and the borough that we represent. Therefore, concerns about council matters, policy or corporate social media accounts should be raised through the appropriate internal channels:

- Your line manager
- The relevant divisional director or corporate director
- Head of external communications
- Corporate Director, Governance and Monitoring Officer
- Democratic services team

Do not raise concerns or complaints about the council publicly through your social media accounts.

7. Breaches of this policy

If you suspect an individual covered by this policy has used social media in an inappropriate manner, please follow the procedure below:

- Take screenshots to capture any inappropriate posts you see before they are deleted.
- Report them to the head of external communications.
- Where appropriate, report the inappropriate post to the relevant social media site following its own reporting procedures.

Any breach of this policy will be viewed as a serious matter and could be considered a disciplinary offence.

In the event of a serious breach of the policy amounting to a breach of the law, the council will be obliged to report this to the police or other external agency as appropriate.

Members who are found to be in breach of the protocol may be subject to action under the provisions of the members' code of conduct.

8. For further information or support

The communications team can provide additional advice and guidance as appropriate.

Training is also available to individual members or groups on the use of social media.

Key internal stakeholders

Name	Role	Email	Phone
Kerry Middleton	Head of External Communications	kerry.middleton@towerhamlets.gov.uk	Ext 4390
External communications team and on-call press officer		communications@towerhamlets.gov.uk	Ext 4389 or 07852 273 984
Asmat Hussain	Corporate Director, Governance and Monitoring Officer	amat.hussain@towerhamlets.gov.uk	Ext 4800