RTPI Social Media Policy

1. Policy Statement

The RTPI's social media policy demonstrates the importance of social media in communicating, promoting and marketing the Institute. Social media allows the RTPI to directly communicate and engage with members, stakeholders and the public.

Social media allows the RTPI to control the content and timing of the message it shares. It is important that the Institute focuses attention on growing its followers and increasing their engagement with its content in order to grow the RTPI's influence and reach online. Social media is a crucial part of modern marketing and communications.

This policy covers the use of social media (both corporate and personal accounts) for staff and volunteers engaged by the RTPI. It is designed to help make the best use of available technology while managing and mitigating the risks to the Institute.

Social media use contributes to these Corporate Goals:

Pillar 1 - Promoting the value of membership
Pillar 2 – Supporting planning services
Pillar 3 – Raising the profile of planning: Comms & engagement
Pillar 4 – Promoting equality, diversity & inclusivity

The RTPI uses social media at a corporate UK and international level, in the nations, regions and networks. At each level the social media channels used are at the discretion of the Directors and Regional Coordinators in consultation with the communications team. The Social Media Policy will be administered and monitored by the communications team. Across the organisation, the RTPI uses these social media channels:

- Twitter
- Facebook
- LinkedIn
- Instagram
- YouTube

Directors and Regional Coordinators, in consultation with the communications team, can 'opt out' of using any channel that would be ineffective in their nation or region or can delegate to an appropriate member of staff or volunteer as set out in the governance.

The purpose of this policy:

- It sets the core principles for RTPI staff and volunteers on the use of language, tone and style on social media
- It provides platform-specific guidelines and best practice
- It clarifies the management and governance of social media at the RTPI

While social media is constantly changing, the RTPI's values do not. Social media activity should always reflect the values of the Institute. Expert advice is available from the social media manager if needed.

2. Core Principles

These are the RTPI's core social media principles which apply across all channels:

- **Promote the values and views of the RTPI:** social media is a way of promoting the values and views of the Institute. Anything published on social media should be consistent with RTPI values and views
- **Social media activity must be broadly consistent with the RTPI Style Guide:** social media is not as formal as traditional communication so there is an expectation that the tone and style is more casual and personal than the Style Guide indicates
- **Think before you post:**
  If in doubt, don't publish. Even if quickly deleted, publishing something live can be seen by many users or indexed by search engines instantly.
- **Do not plagiarise:** outright copying, quoting or the use of an image without attribution are easily uncovered and potentially criminal offences. Check copyright of images and credit if necessary.
- **Do not discuss personal or confidential information:** while social media blurs the concept of internal and external communications, always make sure any material published on social media is suitable for the public
- **Be honest and use common sense:** take responsibility for use of social media in a corporate capacity, so if in doubt about posting anything, first consult with the communications team for advice
- **Be responsive:** encourage comments and respond to those who have questions. Like, share or retweet relevant content from others. Social media works best when you engage in two-way communication
- **Ensure it is well-resourced:** to be effective, social media channels must remain active with high quality content, and accounts should not be set up unless they can be resourced adequately
- **Racist, sexist, or otherwise offensive or objectionable language will not be tolerated.** any posts which breach our EDI policy and are not in line with RTPI inclusive language guidance or that may bring the RTPI into disrepute could result in disciplinary action, as set out in the Disciplinary and Capability Policy on the intranet.
- **The terms of use of each social media platform must be respected:** their guidelines clearly spell out the legal limits of their service, and should be followed
- **Follow the RTPI guidelines and best practice for use of social media:** this includes the strategy and direction set by the communications team.

Online Trolling

The term "online troll" usually refers to someone who maliciously harasses, attacks, or cyberbullies others. They might take your words out of context, spam you with offensive content or even engage in racist, homophobic, misogynistic, or otherwise hateful rhetoric.

Unfortunately trolling has become more prevalent across the different social media platforms and needs to be taken seriously. There will always be people who do not agree with what you say. If you come across negative or disparaging posts about RTPI or see third parties trying to spark negative conversations:

- Simply **ignore the comments** ie don't feed the trolls
- Do not be tempted to react yourself, especially in the immediate aftermath of a story or event
- **Pass the post(s)** to the social media officer and Director of Communications to advise

- If it gets too much, **think about having a hiatus** from social media for a short period of time.

Staff and volunteers using corporate RTPI or RTPI affiliated social media accounts must agree and follow the RTPI's social media policy.

There may be instances when individuals pass themselves off as being affiliated with the RTPI when in fact they are not or they might be misrepresenting their qualification level eg saying they are Chartered when they are not.

This is especially apparent on LinkedIn when individuals can put RTPI down as an employer on their profile and add any qualifications. Unfortunately, we cannot control what people put on their LinkedIn profiles but if you see something wrong, please flag this with the social media officer in the first instance and report it here. You can also report fake profiles here.

3. Governance Arrangements

3.1 How does the RTPI distinguish between personal and official social media accounts?

The RTPI identifies 3 types of social media accounts.

A **corporate RTPI social media account** is one which is owned by the Institute and operated by an RTPI staff member or volunteer on the Institute's behalf. The @RTPIPlanners Twitter account, Royal Town Planning Institute Facebook page and @RTPIPlanners Instagram account are examples of corporate accounts. The account and login information is the property of the Institute and if the individual leaves, the account remains with the Institute.

An **affiliated RTPI social media account** is one which is owned and operated by a member of RTPI staff or a volunteer. For example, many Policy/Research Officers have personal accounts which stated they are an 'RTPI Policy Officer' or similar.

A **personal social media account** is one which is owned and operated by a member of RTPI staff or volunteer which is NOT used for RTPI purposes and does not identify them as having any connection with the RTPI. If a social media account identifies a connection with the RTPI then it is treated as an affiliated account. Disparaging remarks about your 'employer' or their activity has the potential to bring the RTPI into disrepute. This is a breach of RTPI policy and will be treated seriously.

3.2 Can I have a personal social media account?

Staff and volunteers can continue to use or start up a personal social media account while at the RTPI. The RTPI recognises the value to both the Institute and the individual staff member/volunteer in their use of affiliated social media accounts, particularly on Twitter. It can help build the reputation and influence of both staff/volunteer and the Institute.

If the social media account is affiliated with the RTPI then staff and volunteers must follow the RTPI's core social media principles.

If you use your personal channels to promote RTPI content, be mindful that there will be a clear link between your other content and RTPI. If you have any difficulties with your account, please get advice from the social media manager or Director of Communications.

3.3 Why does the RTPI social media policy include personal accounts?

Many staff and volunteers make use of social media in a personal capacity. While not acting in an official capacity, staff and volunteers need to be aware that what they post on social media could affect the reputation of the RTPI.

However, the RTPI comms team cannot monitor or control what people post, so **if you are concerned about any reputational impact, contact the Director of Communications or the social media officer immediately to inform them.**

Risks arise from the blurring of the lines between personal activity and corporate or professional activity on social media. Even when not at work or representing the RTPI, all employees have a duty not to bring the Institute into disrepute.

In recent history, some built environment membership bodies have had to close down their entire social media presence for weeks if not months while the storm over a single member of staff's behaviour on Twitter was handled. Actions on personal accounts are more likely than not to impact corporate channels. While there may be no direct link between a personal account and an employer, people will find the connection if they want to.

3.4 Who can post from an RTPI social media account?

Before posting from a corporate social media account, users must have permission from the communications team or the manager of the social media account.

Corporate RTPI social media accounts for the entire organisation are managed by the social media manager and they can provide authorisation for other officers to use them.

Social media accounts in the nations and regions are managed and 'owned' by the Nation and Region. **The Director or Regional Coordinator in the Nations and Regions, respectively, authorises, up to two, other staff or volunteers to use social media on their behalf.**

Owners of National and Regional accounts are **responsible for knowing who has access and must always have the correct login information**. Where a social media account is managed by volunteers, a staff member must have access to the account at all times.

All staff and volunteers using corporate or affiliated RTPI social media accounts must read and agree to the Social Media Policy before using it.

3.5 How many people can have access to RTPI social media accounts?

All social media accounts can be accessed by the owner and two others (either staff or volunteers) designated by the owner to manage the account. For example, a Regional Coordinator is the owner of their RTPI Region account and can grant access to two other people to help them manage it.

3.6 What do I do if I've just started managing an existing corporate social media account?

1. Change the password on the account
2. Ensure the email used for logging in is a generic email address so that the account is accessible by others in the event the manager of the account is unable to.
3. Submit the new password and email account to the communications team

3.7 Why does the communications team store social media account passwords and email logins?

The communications team holds a list of all of the passwords and email logins for corporate RTPI social media accounts.

There are many scenarios in which having access to various social media platforms would be a requirement. For example, if the employee in charge of the account leaves the RTPI or is on holiday, general maintenance is required or in the event of a social media disaster.

There are different social media platforms used at a corporate, national, regional and network level, for example, some regions have both Twitter and Facebook accounts, others don't. It's at the discretion of each level to decide which platforms work best for them. For this reason, it's important that all accounts are recorded and held centrally so that there is an overarching view of the social media activity for the whole organisation.

It is also important that any social media accounts that require an external email contact address be linked with a corporate RTPI address and not any personal email address. This will help to keep all password reset requests accessible to the RTPI in the future.

For the above reasons, and to ensure that social media is used in the best possible way to enhance the reputation of the RTPI, all social media activity will be monitored on a regular basis.

This requirement does not apply to personal social media accounts.

3.8 What do I do if I want to set up a new social media account?

The following should be considered before establishing a new RTPI social media account:

- The first step is to understand the **motivation** for establishing a new social media account. Is the material you would like to communicate already covered by another account? Could the activity be championed by another, established social media channel? If so liaise with the manager of the social media channel to communicate the message.
- Do you have enough **time** to maintain a new social media account? For example, Twitter requires at least 2 posts per day, LinkedIn 2-3 times per week.

- Who is the **audience** of the new account? How many people are there currently unserved by an existing account? How will the new account solve the current problem?
- If, after considering these questions, a new account is considered to be the most effective option, you will need to make the **business case** for it to the communications team, outlining why the material can't be included in an existing account, how the new account would be resourced and the views of the relevant Director or Regional Coordinator.

If a new social media account is set up the email and password to log in should be submitted to the communications team. Passwords should, otherwise, not be shared.

In most cases the corporate social media accounts are sufficient for all of the institute's needs and what is most likely required is a communications strategy to ensure your content is being included on those channels.

3.9 What about branding, logos and style?

The consistent use of RTPI branding and logos is an essential part of keeping the Institute's identity coherent, and this applies to the use of social media. The official logo should be used as much as possible, unless agreed with the communications team. The relevant RTPI logo should be the profile picture for all corporate RTPI social media accounts. Any use of the logo should be discussed with the communications team.

The writing style for social media is more informal and succinct than the traditional corporate writing, however, the RTPI style guide should be adhered to as much as possible.

4. Plagiarism and Copyright

Plagiarism is very prevalent online because the means to do so are easy. All quotes, images and material that are not owned by the RTPI should be appropriately referenced.

If in doubt contact the communications team for further guidance.

4.1 What do I do if something goes wrong on social media?

- Contact the communications team with the following information: detail about the offending content, what steps have already been taken, who is aware of the situation (how did it arise), if you cannot speak with a member of the team proceed with the next 2 steps
- Take a screenshot of the offending content and save it in a word document.
- Remove the offending content from social media (bearing in mind other users may have already taken a screenshot of it)
- Contact the communications team a second time with the screen shot of the questionable content and discuss next steps.

4.2 Breach of social media policy

The RTPI entrusts staff and volunteers to use social media accounts in accordance with the policy. Any abuse will be investigated and treated seriously in accordance with RTPI disciplinary and capability policy.

5. Cybersecurity

Social media platforms are a common target for cyber attacks due to the large amount of personal information shared on these sites. Here are some guidelines and best practices for protecting both personal and company information on social media platforms. For example :

- **Strong password management**: Use strong, unique passwords and change them regularly. It should be hard to guess, so don't include your name or common words. Learn more about creating a strong password on Twitter.
- **Enable two-factor authentication:** Two-factor authentication is an extra layer of security that requires a second form of authentication in addition to your password. This can help prevent unauthorised access to your account.
- **Avoid phishing scams:** Don't respond to suspicious emails that ask for sensitive information or click on links or attachments that could be impersonating a company.
- **Limiting access:** Ensure that only authorised colleagues can access company social media accounts. Alerts are sent via email or text message to monitor new and suspicious logins.
- **Security:** Use secure devices and networks, especially if you're out in public. If you're using a public computer or device make sure you sign out of your social media account when you have finished.
- **Keeping software up to date:** Keep your browser and operating system updated with the most current versions and patches—patches are often released to address particular security threats. Be sure to also scan your computer regularly for viruses, spyware, and adware.

5.1 What do I do if my corporate social media account has been compromised?

If you suspect your social media account has been compromised, it's important to act quickly. Here are the steps you should take:

- **Notify the team**. Alert the RTPI social media officer or Director of Comms as soon as possible
- **Change your password:** Create a new, strong password unique to your social media account and set up two-factor authentication. Make sure to avoid using the same password for multiple accounts.
- **Check for unauthorised activity:** Review your activity logs and look for any posts, messages, or other activity you don't recognise. If you find any, delete them and report them to the platform.
- **Check your account settings**: Look for any changes that may have been made to your account settings, such as changes to your profile information, privacy settings, or email address. Change any incorrect information and reset your privacy settings to your preferences.
- **Report the compromise to the platform:** Follow the instructions provided by the platform to report the issue and get help recovering your account.

- **Revoke access to third-party apps**: If you have allowed third-party apps to access your social media account, check which ones have permission and revoke access to any that you don't recognise or no longer use.
- **Monitor your account:** After taking these steps, monitor your account for any signs of suspicious activity. Be vigilant and report any issues immediately to the platform.

Contacts

Shakila Barabhuiya, Communications Officer (social media): shakila.barabhuiya@rtpi.org.uk
Simon Creer, Director of Communications: simon.creer@rtpi.org.uk