A picture containing background pattern

Description automatically generatedA black and white text with a yellow line

Description automatically generated

Social Media Policy

All Trident Group Colleagues

|  |  |
| --- | --- |
| **Version:** | 2 |
| **Author:** | Lucy Owen |
| **Issue Date:** | 09 August 2024 |
| **Review Date:** | 09 August 2025 |
| **Staff Affected:** | All Staff |
| **Approved By:** | Nigel Wilson |
| **Lead Officer** | Communications Manager |

**Uncontrolled version if printed or emailed.**   
If you are viewing this document from your personal drive or as a hard copy it may not be the latest version.

**Contents**

|  |  |  |
| --- | --- | --- |
| **Section Number** | **Section Name** | **Page Number** |
| 1. | Introduction | 3 |
| 2. | Personal Use | 3 |
| 3. | Corporate Social Media Policy | 6 |
| 4. | Applying this Policy | 7 |
| Appendices | | |
|  | | |

1. **Introduction**

This policy sets out both the responsibilities of Trident Group (Trident) and that of all staff and volunteers with regard to social networking. This policy on the use of social networking websites is in addition to Trident’s existing policy on email and internet use. This policy covers all staff and volunteers employed by Trident and external stakeholders (including contracted staff and Board).

Social media gives Trident the opportunity to engage and communicate with our audiences in a different way. As part of the Trident’s strategy to engage with our customers and the public, we have embraced this as part of our communication channels to ensure we connect with residents in the way that is most effective for them and promote Trident’s activities positively.

* 1. Purpose

It is also important to ensure that we balance the use of such sites with our duties to our customers, partners and staff, our legal responsibilities and our reputation. The purpose of this policy is to outline the responsibilities of staff using the internet to access social networking websites both while at work, and also in personal time where reference may be made to Trident. As social networking relates to public rather than private communications, Trident has a valid interest in any of these public communications that comment on the organisation, its activities, partners or customers.

* 1. Definitions

Social networking applications include, but are not limited to:

* Social networking such as X (formerly known as Twitter); TikTok; Instagram; Facebook, BlueSky, Threads etc.
* Professional social networking such as LinkedIn
* Chat sites such as SnapChat or WhatsApp
* Blogs
* Online live streaming sites, such as Twitch
* Media sharing services, for example YouTube

There is a clear distinction between 'social networking', which is for personal use and ‟corporate social networking', which is useful to the business. There is more detail on “corporate social networking” in section 3.

1. **Personal Use**

Trident respects our colleague’s right to a private life. However, we must also ensure that our data security, confidentiality and reputation are protected. Whilst staff are not forbidden from identifying themselves as being associated with Trident, if they are identified, they are responsible for representing the company in a professional positive manner.

Where staff become aware that someone is conducting themselves in a way on a social networking site that is detrimental to Trident, they should inform their own line manager in the first instance, who may take appropriate action, including performance management/disciplinary action against the employee. Where the line manager is not available, then any other manager or senior member of staff should be notified. The Communications Team should also be contacted in such instances.

Staff should not make reference to Trident on personal social media accounts, particularly if comments are critical, or ridicule the organisation or any of its colleagues or associated parties. Users should also be aware that the media use social media to gather information about staff, including personal details, telephone numbers, e-mail addresses and links, images and interests, and are entitled to report on anything posted.

When using private social networking, blogs and video sharing websites, no use may be made of the Trident (or any of its affiliates) name or logo without the express permission of the Communications Team. Consideration must also be given to any other matters of copyright.

When using private networking no use may be made of Trident photographs or images without the permission of the Communications Team. Staff should not send messages about Trident work, projects and activity from personal social media accounts.

To protect the reputation of Trident, its affiliates, employees, customers and partners, staff should not set up unofficial or spoof groups, pages or accounts. Staff should be aware that internet and email traffic is monitored to ensure that usage does not endanger the integrity of Trident’s IT systems. Websites visited and the duration of use will be recorded. Line managers may request reports from ICT at any time.

* 1. Behaviour on personal social media

They should:

* Ensure that they do not conduct themselves in a way that is detrimental to Trident or bring the organisation into disrepute.
* Take care not to allow their interaction on these websites to damage working relationships between members of staff, customers, partners and suppliers of Trident. Staff should be careful about crossing professional boundaries.
* If colleagues have identified themselves as working for Trident, ensure any personal posts contain disclaimers that make it clear that the opinions expressed are solely those of the author and do not represent the views of Trident. A disclaimer should be used to say: “The views expressed are the author’s alone and do not necessarily reflect the views of Trident Group or its affiliates”.
* Be mindful that anything published will remain in the public for an indefinite period of time.
* Not criticise work or colleagues, customers, or partners even if you don’t name them – people will be able to work out who is being talked about.
* Be respectful – don’t publish anything abusive, bullying, derogatory, discriminatory or inflammatory.
* Not let social networking activities interfere with work commitments.
* Accessing social network sites should not be conducted when staff are supposed to be working.

Failure to follow the above guidance may result in disciplinary action if it brings Trident Group into disrepute in accordance with our disciplinary policy and procedure.

* 1. Professional Social Media

Professional social media sites such as LinkedIn are important tools to build connections and relationships with different organisations. It can also be used as a successful recruiting tool and having employee recommendations is important to build Trident as a brand to work for. The Communications team want to encourage professional use of these platforms to raise awareness of services, engage with stakeholders, and promote Trident.

At the same time, we wish to ensure that colleagues represent Trident as a professional and reputable organisation. Therefore staff members should not engage in any conduct that would not be acceptable at work or bring the organisation into disrepute.

Staff should therefore:

* Ensure compliance at all times with the law in regard to copyright and using other people’s work. Posting of someone else’s work without permission is not allowed.
* Comply with relevant laws including those related to libel and defamation of character.
* Staff should not comment on Trident or our partners’ performance as an organisation or the individual performance of colleagues, customers, or partners.
* Trident logos should not be used without permission from the Communications Team.
* Pictures of Trident residents or buildings should never be used.
* Whilst it is accepted that situations will arise where some social networking may take place between staff and residents, this should be kept as limited as possible to keep the professional relationship distinct. All communication should be recorded on their records on customer management systems (e.g. CRM, Inform, Sun etc) just like any other form of communication. Staff should not access residents’ social networking sites, unless given express permission to do so.
* Colleagues must not share internal communications such as newsletters, briefing notes, or messages sent through other means like team WhatsApp channels.
* All Trident corporate social networking and video sharing sites will be administered by the Communications Team. The Communications Team reserves the right to refuse any new social media accounts request or close down any social media accounts failing to comply with the policy.

2.2i Additional guidance for colleagues

Identity Theft

Staff should be aware that social networking websites are a public forum. Staff should not assume that their entries on any website will remain private. Staff should be security conscious and should take all the necessary steps to protect themselves from identity theft, for example by restricting the amount of personal information that they give out.

2.3 Monitoring IT Usage at Work

Trident reserves the right to monitor staff’s internet and social networking usage at work. The IT systems required for monitoring purposes are always “on” but are not always actively monitored by ICT.

Trident considers that valid reasons for checking staff internet usage include suspicions that the staff in question has:

* Been spending an excessive amount of time viewing websites in work time that are not work-related
* Acted in a way that damages the reputation of Trident
* Breached the guidance set out in this policy.

1. **Corporate Social Media**

Social networking sites are an expected form of engaging with customers, partners, suppliers and staff. The use of social networking sites and other online business forums gives another way for people to find out about Trident and communicate with us, and we can benefit from understanding different perspectives.

Trident use social media sites to communicate with customers, in an open forum. Social media channels are managed between 9am and 4pm Monday to Friday. During these times the audience can expect a response to their query, where appropriate, within 24 hours. If they have any queries, they are able to contact us on X (@tridentgrp), BlueSky (@tridentgrp.bsky.social) or Facebook (@tridentgrp).

Reports will always be documented on customer management systems as any other form of communication. The Communications Manager and Communications Officer will use their own first names or agreed pseudonym to ensure that accountability can be taken.

Corporate social networking should only be used where it adds value, i.e. to help solve problems, improve skills and services or build a sense of community. The audience should be respected.

When communicating publicly, Trident will have well-established processes in place and only the Communications Manager and Officer authorised to do this. No additional social media accounts, which includes Facebook, X, LinkedIn, BlueSky, and YouTube which relates to Trident’s activities (for example, new projects and initiatives) should be introduced within services or for your areas of work without consent from the Communications Team.

Any employee wishing to open an account must produce a business case clearly evidencing the purpose and demonstrating the business benefits linked to the organisation’s Strategic Plan. They must also invite the Communications Manager to sit as an admin on these accounts. The Communications Team reserves the right to refuse any new social media accounts request or close down any social media accounts failing to comply with the policy.

* 1. Policy on banning or blocking residents from social media channels

Since these are public arenas, there are some instances in which we will remove posts or block individuals. Please see our guidance below for correspondences made via both public posts and private messages:

* Naming individuals – includes Trident staff, residents/customers and other members of the public.
* Giving out personal information – this can be either personal information for themselves or anyone else. Information given out includes: postal addresses, email addresses, and phone/mobile numbers. If we need their private details we will request them to send this information via a private message.
* Using abusive or threatening language.

This is a three strike policy where residents will be encouraged to delete posts and message privately before the resident will be blocked on all accounts. A note will also be added to their customer record of this taking place.

1. **Applying this policy**
   1. Disciplinary Action

Staff are required to follow the guidance set out in this policy. Failure to do so may result in the disciplinary action. Access to the internet may be withdrawn at management discretion, and in particular following any case of misuse of this facility.

* 1. Equality and Diversity

The policy will be applied fairly and consistently to all our residents and staff. We will not directly or indirectly discriminate against any person or group of people because of their race, religion / faith, gender, disability, age, sexual orientation or any other grounds set out in our Equality and Diversity policy.

When applying this policy we will:

* Act in line with Trident’s values, with respect and in consideration of the diverse needs of individual and communities.
* Take positive action to reduce the discrimination and harassment in local communities. This policy and any other Trident publication is available in other formats (e.g. other languages, Braille, large print, audio).

Communications on corporate social media will be designed and published following best accessibility practice.

* 1. Confidentiality and Information Sharing

We will only share information that meets the requirements of the Data Protection Act 1998.

* 1. Monitoring and Accountability

Trident Group Executive Board will be responsible for ensuring that the policy is implemented in full.

Trident’s Executive Lead – Chief Executive will monitor the effectiveness of this policy and recommend policy changes to improve service delivery.

Trident’s Head of ICT will be responsible for ensuring that appropriate IT monitoring tools are in place.

Review Trident will carry out a fundamental review of this policy every year from the date of this policy.

* 1. References
* Trident Communications Strategy
* Disciplinary Policy
* ICT Policy
* Equality and Diversity Policy