



Ref: P004	TLS Social Media Policy
-----------	-------------------------

Context and Overview

Key Details

- Policy prepared by: Tracey Hobson
- Approved by Management/Directors: 08/01/2016
- Policy became operational on: 08/01/2016

Introduction

Employees of TLS Ltd may be able to access social media services and social networking websites at work, either through company IT systems or via their own personal equipment.

This social media policy describes the rules governing use of social media at TLS Ltd.

It sets out how staff must behave when using the company's social media accounts. It also explains the rules about using personal social media accounts at work and describes what staff may say about the company on their personal accounts.

This policy should read alongside other key policies. The company's internet use policy is particularly relevant to staff using social media.

Why this policy exists

Social media can bring significant benefits to TLS Ltd., particularly for building relationships with current and potential customers.

However, it's important that employees who use social media within the company do so in a way that enhances the company's prospects.

A misguided status update can generate complaints or damage the company's reputation. There are also security and data protection issues to consider.

This policy explains how employees can use social media safely and effectively.

Policy Scope

This policy applies to all staff, contractors and volunteers at TLS Ltd. who use social media while working – no matter whether for business or personal reasons.

It applies no matter whether that social media use takes place on company premises, while travelling for business or while working from home.

Social media sites and services include (but not limited to):

Ref: P004	Revision No: 07	Date Issued: 17/01/2026	Approved By: PC
-----------	-----------------	-------------------------	-----------------

- Popular social networks like **Twitter** and **Facebook**
- Online review websites like **Reevoo** and **Trustpilot**
- Sharing and Discussion sites like **Delicious** and **Reddit**
- Photographic social networks like **Flickr** and **Instagram**
- Question and Answer social networks like **Quora** and **yahoo Answers**
- Professional social networks like **LinkedIn** and **Sunzu**

Responsibilities

Everyone who operates a company social media account or who uses their personal social media accounts at work has some responsibility for implementing this policy.

However, these people have key responsibilities:

- The **Director** is ultimately responsible for ensuring that TLS Ltd. uses social media safely, appropriately and in line with the company's objectives.
- The **IT Administrator** is responsible for providing apps and tools to manage the company's social media presence and track any key performance indicators. They are also responsible for proactively monitoring for social media security threats.
- The **Director and Operations Managers** are responsible for working with the **IT Administrator** to roll out marketing ideas and campaigns through our social media channels.
- The **Operations Managers** are responsible for ensuring requests for assistance and support made via social media are followed up.

General social media guidelines

The power of social media

TLS Ltd. recognises that social media offers a platform for the company to perform marketing, stay connected with customers and build its profile online.

The company also believes its staff should be involved in industry conversations on social networks. Social media is an excellent way for employees to make useful connections, share ideas and shape discussions.

Safe, responsible social media use

The rules in this section apply to:

Ref: P004	TLS Social Media Policy
-----------	-------------------------

- Any employees using company social media accounts
- Employees using personal social media accounts during company time
- Employees using TLS Ltd. or personal TLS social media accounts outside of working hours

Users must not:

- Create or transmit material that might be **defamatory or incur liability** for the company
- Post message, status updates or links to material or content that is inappropriate

Inappropriate content includes: pornography, language, racial or religious slurs, gender-specific comments, information encouraging criminal skills or terrorism, or materials relating to cults, gambling and illegal drugs.

This definition of inappropriate content or material also covers any text, images or other media that could reasonably offend someone on the basis of race, age, sex, religious or political origin, disability, sexual orientation or any other characteristic covered by law.

- Use social media for any **illegal or criminal activity**.
- Send **offensive or harassing** material to others via social media.
- Broadcast **unsolicited views** on social, political, religious or other non-business related matters.
- Send or post messages or material that could damage TLS Ltd.'s image or reputation
- Interact with TLS Ltd.'s competitors in any ways which could be interpreted as being **offensive, disrespectful or rude**. (Communication with direct competitors, should be kept to a minimum).
- Discuss **colleagues, competitors, customers or suppliers** without their approval.
- Post, upload, forward or link to **spam, junk mail or chain emails and messages**.

Copyright

TLS Ltd. respects and operates within copyright laws. Users may not use social media to:

- Publish or share any **copyrighted software, media or materials owned by third parties**, unless permitted by that third party.

If staff wish to **share content published on another website**, they are free

Ref: P004	Revision No: 07	Date Issued: 17/01/2026	Approved By: PC
-----------	-----------------	-------------------------	-----------------

to do so if that website has sharing buttons or functions on it.

- Share links to **illegal copies** of music, films, games or other software.

Security and data protection

Employees should be aware of the security and data protection issues that can arise from using social networks.

Maintain confidentiality

Users must not:

- Share or link to any content or information owned by the company that could be considered **confidential or commercially sensitive**.

For example, if a competitors marketing strategy was leaked online, employees of TLS Ltd. should not mention it on social media.

- Share or link to data in any way that could breach the company's **data protection policy**.

Protect social accounts

- Company social media accounts should be **protected by strong passwords** that are changed regularly and shared only with authorised users,
- Wherever possible, employees should use **two-factor authentication** (often called mobile phone verification) to safeguard company accounts.
- Staff must not use a new piece of **software, app or service** with any of the company's social media accounts without receiving approval from the **IT Administrator**.

Avoid social scams

- Staff should watch for **phishing attempts**, where scammers may attempt to use deception to obtain information relating to either the company or its customers.

Employees should never reveal sensitive details through social media channels. Customer identities must always be verified in the usual way before any account information is shared or discussed.

- Employees should **avoid clicking links** in posts, updates and direct messages that look suspicious. In particular, users should look out for URLs contained in generic or vague-sounding direct messages.

Ref: P004	TLS Social Media Policy
-----------	-------------------------

Policy enforcement

Monitoring social media use

Company IT and internet resources – including computers, smart phones and internet connections – are provided for legitimate business use.

The company therefore reserves the right to monitor how social networks are used and accessed through these resources.

Any such examinations or monitoring will only be carried out by authorised staff.

Additionally, all data relating to social networks written, sent or received through the company's computer systems is part of official TLS Ltd. records.

The company can be legally compelled to show that information to law enforcement agencies or other parties.

Potential sanctions

Knowingly breaching this social media policy is a serious matter. Users who do so will be subject to disciplinary action, up to and including termination of employment.

Employees, contractors and other users may also be held personally liable for violating this policy.

Where appropriate, the company will involve the police or other law enforcement agencies in relation to breaches of this policy.

Paul Chamley



Managing Director

Ref: P004	Revision No: 07	Date Issued: 17/01/2026	Approved By: PC
-----------	-----------------	-------------------------	-----------------



Ref: P004	TLS Social Media Policy
-----------	-------------------------

Revision History

Revision	Date	What has changed?	Who has written it?	Who has approved it?
00	08/01/2016	First Issue	QE&SH Manager	MD
01	26/05/2020	Reviewed, updated to new document control format, removal of superfluous logos, some changes to text to make accurate of current situation, name & signature of MD added.	Systems Manager	MD
02	26/05/2021	Reviewed and added TA logo	Systems Manager	MD
03	26/05/2022	Reviewed	Systems Manager	MD
04	24/01/2023	New TLS Group Logo added	Systems Manager	MD
05	17/01/2024	Annual review	Systems Manager	MD
06	17/01/2025	Annual review	Systems Manager	MD
07	17/01/2026	Review	Systems Manager	MD

Ref: P004	Revision No: 07	Date Issued: 17/01/2026	Approved By: PC
-----------	-----------------	-------------------------	-----------------



Ref: P004	TLS Social Media Policy
-----------	-------------------------

Ref: P004	Revision No: 07	Date Issued: 17/01/2026	Approved By: PC
-----------	-----------------	-------------------------	-----------------

Uncontrolled if Printed or Copied