

IT Acceptable Use Policy

20/04/2026

Purpose

The purpose of this policy is to set out the acceptable use of Tudor Griffiths Group's IT systems and resources.

This policy aims to protect the organisation, its employees, customers and suppliers from legal, security and reputational risks arising from the misuse of IT systems.

Scope

This policy applies to all employees, contractors, agency workers and third parties who access or use company IT systems.

It covers all IT resources, including (but not limited to):

- computers, laptops and mobile devices
- telephony and communication systems
- email and internet access
- business applications and cloud services
- social media accounts used for business purposes

This policy also applies where personal devices are used to access company systems, applications or data, including company email, telephony services, CCTV applications or other business platforms.

Acceptable Use of IT Systems

IT systems must be used:

- primarily for legitimate business purposes
- in a lawful, secure and responsible manner
- in accordance with company policies and procedures

Limited personal use may be permitted where it does not:

- interfere with work duties
- compromise security or system performance
- expose the organisation to risk

Users must take reasonable care to ensure company systems and information remain secure, including when accessed remotely or on personal devices.

Unacceptable Use

Users must not:

- access, create, store or distribute illegal, offensive or inappropriate material
- attempt to bypass security controls or monitoring systems
- share login credentials or allow unauthorised access to systems
- misuse company information or confidential data
- install unauthorised software or services

Any activity that exposes the organisation to legal, security or reputational risk is prohibited.

Email, Internet & Communications

Company email and internet access are provided primarily for business use.

Users must:

- communicate in a professional and appropriate manner
- exercise caution when receiving unsolicited emails, links or attachments
- remain alert to phishing and social engineering attempts

Electronic communications sent using company systems are company records and may be monitored in accordance with applicable law and company policy.

Social Media Use

Social media presents specific cyber security and reputational risks.

Where social media accounts are used on behalf of the company:

- access must be limited to authorised individuals
- company information must not be disclosed inappropriately
- care must be taken to avoid social engineering, profiling and impersonation risks
- strong passwords and multi-factor authentication must be used where available
- idle or unused business social media accounts must be reviewed and removed

Users must not share excessive information relating to:

- business practices
- customers, clients, suppliers or third parties
- employees or internal operations

All users with access to company social media accounts must follow training and guidance designed to reduce risks arising from human error, phishing and malicious activity.

Mobile Phones & Devices

Handsets and tablets issued by Tudor Griffiths Group remain company property and must be used primarily for business purposes.

All mobile devices accessing company data — whether company-supplied or personal (BYOD) — must be:

- protected with a strong PIN or biometric lock
- kept up to date with operating system and security patches
- running approved security software where provided by the IT department

Personal mobile phones must not be used during work hours except during designated breaks or with explicit line manager permission, and must not be used while operating machinery or vehicles.

Hands-on use of any mobile phone while driving a company or personal vehicle on company business is prohibited.

Lost or stolen devices must be reported to the IT department immediately so company data and access can be secured.

Tariff allocation, cost management and handset replacement rules for company-supplied devices are maintained separately by the IT department in conjunction with Finance.

Passwords & Account Security

Users are responsible for safeguarding their access credentials.

Passwords must:

- meet company security requirements
- be kept confidential and not shared
- be changed where compromise is suspected

Access to IT systems must be removed promptly where it is no longer required, including when a user leaves the organisation.

Monitoring, Recording & Privacy

Use of IT systems may be monitored where lawful and necessary.

Specific activities such as call recording, CCTV and system monitoring are governed by the Monitoring & Recording Policy and must be carried out in accordance with applicable laws.

Responsibilities

All users are responsible for:

- complying with this policy
- protecting company systems and information
- following security guidance and training

Any suspected misuse of IT systems, security incident, or activity that does not look right must be reported promptly in line with company procedures.

Managers are responsible for ensuring their teams understand and comply with this policy.

Breaches of this Policy

Failure to comply with this policy may result in disciplinary action and, where appropriate, legal action.

Policy Control

This policy is owned by the Group ICT Manager and approved by the Group Finance Manager and Company Secretary. It will be reviewed annually or sooner where business needs, legislation or the threat landscape change materially.