Cyber, Information Technology & Artificial Intelligence (AI) Security Policy

1. Purpose

General & Technical Flooring Services Ltd ("the Company") is committed to protecting its information, data, systems and technology from loss, misuse, unauthorised access, cyber threats and operational disruption.

This policy sets out the requirements for the secure, responsible and lawful use of all Company information technology, data and Artificial Intelligence (AI) tools.

The objectives of this policy are to:

- Protect Company, employee, client and third-party information
- Maintain system availability, integrity and confidentiality
- Reduce cyber security and data protection risks
- Ensure compliance with legal, contractual and regulatory obligations

2. Scope

This policy applies to all employees, subcontractors, agency workers and authorised third parties who access Company IT systems, data or technology.

IT facilities include, but are not limited to:

- Computers, laptops, servers and mobile devices
- Software, applications and cloud services
- Email, messaging and collaboration platforms
- Internet access and telephony systems
- Data storage, backup and transmission systems

Data includes all electronic information owned, processed or stored by the Company, including personal data, commercial information and client data.

By using Company IT systems, users consent to reasonable monitoring, auditing and security controls for legitimate business purposes.

3. Monitoring, Privacy & Compliance

The Company reserves the right to monitor, audit, inspect or record IT activity where necessary and lawful, including:

- Email, messaging and internet usage
- Software installations and system configurations
- System access logs and file activity
- Telephone records
- CCTV footage where applicable

Monitoring will only be carried out by authorised personnel and in accordance with UK employment, data protection and privacy legislation.

Monitoring may be undertaken to:

- Ensure compliance with Company policies
- Detect or investigate suspected misconduct, data breaches or cyber incidents
- Maintain system performance, integrity and security
- Support training, safety, quality and legal obligations

Misuse of IT systems may result in disciplinary action up to and including dismissal.

4. Acceptable Use Rules

4.1 General Requirements

Users must:

- Use IT facilities primarily for legitimate business purposes
- Take reasonable care to protect devices and data from loss, theft or damage
- Follow all security measures implemented by the Company
- Immediately report suspected security incidents or policy breaches

Users must not:

- Install unauthorised software or applications
- Connect unapproved hardware or peripherals
- Modify system settings without authorisation
- Attempt to bypass security controls
- Access, store or transmit illegal, offensive or discriminatory material

5. Software & Application Use

- All software must be approved, licensed and installed by the IT Department
- Unlicensed, pirated or unauthorised software is strictly prohibited
- Users must not copy, distribute or install software without permission
- Software audits may be conducted at any time
- All software and updates must be virus-checked before installation

6. System & Access Security

Users must:

- Keep passwords secure and confidential
- Use strong, unique passwords and change them when required
- Lock screens when devices are unattended
- Access Company systems remotely only via approved secure methods (e.g. VPN)
- Use Company-approved devices and networks

Users must not:

- Share login credentials
- Attempt to defeat passwords, encryption or firewalls
- Use unauthorised remote access tools (e.g. TeamViewer, VNC)
- Use IT systems for unauthorised or non-work activities

7. Portable & Mobile Devices

This section applies to laptops, tablets, smartphones and removable media.

Users must:

- Keep devices physically secure at all times
- Avoid viewing sensitive information in public places
- Store devices securely and out of sight when in vehicles
- Use passwords, PINs or biometric security
- Report loss, theft or compromise immediately
- Store data only on Company-approved cloud services
- Encrypt confidential data where local storage is unavoidable

Users must not:

- Lend devices to unauthorised persons
- Store Company data on personal devices or personal cloud services
- Use paid mobile services or subscriptions without approval

8. Data Security & Classification

All electronic data must be classified as:

- Confidential – restricted access, business or client-sensitive
- Internal – general Company use
- Personal – limited personal files (stored at user's risk)
- Public – approved for external release

Rules:

- Confidential data must be encrypted where possible
- Confidential data must not be stored on local drives
- Personal devices and non-Company cloud services must not be used
- Access is limited to authorised personnel only
- Data disposal must be approved by IT
- Removable media must be encrypted
- Copyright and intellectual property rules must be followed
- Data retention must comply with Company retention schedules
- Illegal, offensive or discriminatory data is strictly prohibited.

9. Email & Messaging

The Company may access and monitor email and messaging systems for legitimate business purposes.

Users must:

- Use Company email professionally and appropriately
- Apply Company email disclaimers where required
- Encrypt confidential information
- Be alert to phishing, malware and suspicious messages
- Regularly delete obsolete emails

Users must not:

- Send offensive, inappropriate or discriminatory content
- Send confidential data externally without encryption
- Open unknown or suspicious attachments or links
- Forward chain emails or bulk non-work messages

Personal use must be minimal and may be monitored.

10. Internet & Social Media Use

Internet use is categorised as:

- Business use – permitted
- Limited personal use – permitted where reasonable
- Inappropriate use – excessive or disruptive personal use
- Misuse – illegal, offensive or high-risk activity

Disciplinary action may result from inappropriate use or misuse.

Rules:

- Internet activity may be monitored
- Copyright and security rules must be followed
- Personal online purchases are at the user's own risk
- Social media use during work must be professional and business-related

11. Responsible Use of Artificial Intelligence (AI)

The Company recognises that AI tools can improve efficiency and productivity but must be used responsibly, securely and lawfully.

AI includes, but is not limited to, generative AI tools, chatbots, automated analysis tools and content-generation systems.

Users must:

- Use AI tools only where appropriate to their role
- Ensure all AI-generated outputs are reviewed, checked and validated before use
- Apply professional judgement at all times
- Comply with data protection, confidentiality and client obligations

Users must not:

- Input confidential, personal, commercially sensitive or client-identifiable information into public or unapproved AI systems
- Use AI to make decisions affecting safety, employment, financial commitments or contracts without appropriate human approval
- Present AI-generated content as Company-approved or professional advice without verification
- Use AI tools in a way that breaches intellectual property rights or client agreements

The Company reserves the right to restrict, approve or prohibit specific AI tools.

Misuse of AI may result in disciplinary action.

12. Telephone & Communications Systems

- Telephony systems are primarily for business use
- Personal use must be limited
- Call logs may be monitored
- Excessive personal use may be recharged
- Mobile use is subject to the Company Mobile Policy

13. Incident Reporting & Response

Users must immediately report:

- Lost or stolen devices
- Suspected data breaches
- Suspicious emails, downloads or links
- System anomalies or security weaknesses
- Unauthorised access attempts

The IT Department will investigate and respond in line with Company procedures.

14. Disciplinary & Legal Action

Breaches of this policy may result in:

- Withdrawal of IT access
- Formal disciplinary action
- Termination of employment or contract
- Civil or criminal proceedings where appropriate

15. Review

This policy will be reviewed annually or sooner where:

- Technology or cyber threats change
- Legal or regulatory requirements change
- New vulnerabilities are identified

J.MORRISON (MD) 09/02/2026

DATE	REVISION	DETAIL	PREPARED BY	APROVED BY
November 2025	A	Complete overhaul of policy and added in AI	John Morrison	John Dunn