IT* Acceptable Use Policy

This Policy applies to all employees and service providers and sets out the minimum requirements and expectations when using Company IT.

TODD CORPORATION

Acceptable Use

Take care of your Company issued devices and promptly report any incidents of damage or loss.

- You are personally responsible for looking after Company devices allocated to you and for ensuring the security of these devices.
- If you have a Company issued phone or laptop, take it home with you to ensure business continuity.
- Only you can use your Company issued devices. No one else can use it at any time.
- If your Company issued device is not fit for purpose, return it to the Technology & Security Team.
- You must report the loss, theft, or damage of Company IT assets to your manager / supervisor or the Technology & Security Team as soon after the event as possible.
- At the end of your employment / contract, you are required to return all Company issued devices.

Use a unique password and a second factor of authentication if available.

- Every employee is provided with an individual account and you must never use another employee's account.
- Use a secure password and an additional factor of authentication for your account when available.
- Don't share passwords or additional factors of authentication with other employees.
- Don't use the same passwords for work and personal accounts.

Personal devices may be used for Company purposes provided they meet certain requirements:

- They only connect to Guest networks in Company offices.
- M365 applications can be installed but Company Confidential or Company Personal Information (PI) must not be stored on personal devices / storage services.

Ask your manager / supervisor or the Technology & Security Team about which applications to use.

- You must use only approved applications and cloud services for work related tasks. If there's any uncertainty consult your manager / supervisor or the Technology & Security Team.
- If you can't find what you need, make a request to the Technology & Security Service Desk.

Please report any security breaches or concerns.

- Immediately report any unauthorised access, suspicious activity, or cybersecurity incidents to ensure the safety and confidentiality of our Company IT and OT.

Stay up to date with all required security training.

- You are required to complete annual acceptable use training.
- You may be asked to complete additional cyber training modules to mitigate risks associated with the dynamic nature of cyber-attacks.

Company issued devices are managed and monitored, and must be used responsibly.

- Company devices and IT systems are managed and monitored by the Company.
- The use of Company devices and IT systems must adhere to all applicable laws, align with Company policies, and safeguard the Company from any risks.
- The Company reserves the right to monitor and delete personal data and information on its devices and IT systems as per its policy and legal regulations.
- Company devices may be utilised for personal purposes, as long as such use does not impede work duties, diminish job performance, or conflict with professional responsibilities.
- Do not sign up for personal services or subscriptions using your Company provided email address.
- A Company mobile phone and mobile phone plan are primarily for business purposes. Reasonable personal use is allowed provided it does not incur additional cost.
- International calling, global roaming, and paid text services must only be for business purposes.
- All purchases of additional data packs and roaming services for business travel must have prior approval from your line manager / supervisor.
- The Company may charge you for any additional costs incurred due to personal use.
- You may keep the mobile number from your Company phone, if approved, to use it as your personal number after you leave the Company.

***Information Technology (IT):** Any services, equipment, or interconnected system(s) or subsystem(s) of equipment, that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. Examples include Company issued devices and Company licenced applications such as Microsoft 365, TechnologyOne, Salesforce etc.

Prohibited Use

Don't let anyone else use your Company issued devices.

- Company devices are assigned for employee or service provider use only.
- Do not allow family members, friends, or other colleagues to use these Company devices.
- Misuse by others can lead to disciplinary action against the Company device's assigned owner.

Don't share your account and/or password with anyone, including other employees.

- Avoid writing down passwords where others can find them.
- Refrain from using the 'Remember Password' feature on shared devices.
- Never disclose your password in response to an email, phone, or chat request.

Don't use unapproved cloud applications and storage, or attempt to install unapproved applications.

- Don't sign up to, or store Company data on, unapproved cloud services.
- Don't attempt to download or install unapproved applications on Company workstations connected to Company networks.
- If you can't find what you need, make a request to the Technology & Security Service Desk.
- Respect any restrictions on application or cloud service use imposed by the Company for security and compliance reasons.

Don't plug in unapproved USB devices.

- Only use Company approved USB devices to store or move data.

Don't try and circumvent our security controls.

- Don't try to circumvent our security controls, they are there to protect the Company.
- Adhere to the Company's Technology & Security policies and be vigilant when it comes to IT and OT security, risks, scams and emails from unverified or unknown senders.

Exceptions

- The Technology & Security Team may allow or deny a particular prohibited use to any employee based on appropriate risk analysis, risk management and business justification, and they may revoke this right at any time.
- Requests to use Company IT or Non-Company IT in exemption from this Policy must be submitted to the Technology & Security Service Desk.

Compliance

- Any use of Company IT which breaches this Policy may be classified as misconduct or serious misconduct under the Code of Conduct, and may be subject to disciplinary action, up to and including dismissal.