

IT & Device Use Policy

For Australian Small & Medium Enterprises

Template Version 1.0 | December 2024

Important Notice

This template provides general guidance for IT and device use. Tailor the policy to your organisation's specific equipment, systems and requirements. Consider your monitoring and privacy obligations when implementing.

1. Purpose

This policy establishes guidelines for the use of IT equipment and devices provided by [Company Name]. It aims to ensure responsible use, protect company assets and maintain security and productivity.

2. Scope

This policy applies to:

- All employees, contractors and authorised users
- All company-provided IT equipment and devices
- Desktop computers, laptops and tablets
- Mobile phones and smartphones
- Printers, scanners and other peripherals
- Associated software and applications

3. General Principles

IT equipment and devices are provided to enable employees to perform their work duties. Users must:

- Use equipment responsibly and professionally
- Protect equipment from damage and theft
- Maintain security of devices and data
- Follow all company IT policies

4. Equipment Allocation

4.1 Issuing Equipment

- Equipment is allocated based on job requirements
- An equipment register will be maintained
- Employees must sign for equipment received

- Equipment remains the property of [Company Name]

4.2 Equipment Standards

- Standard configurations are determined by IT
- Requests for non-standard equipment require approval
- Equipment will be replaced on a scheduled cycle

5. Acceptable Use

5.1 Business Use

Company IT equipment should primarily be used for:

- Work-related tasks and communications
- Accessing company systems and applications
- Professional development and training
- Approved business activities

5.2 Personal Use

Limited personal use may be permitted provided it:

- Does not interfere with work duties
- Is kept to a reasonable minimum
- Does not breach any policy requirements
- Does not create security risks
- Is conducted outside of work hours where possible

6. Prohibited Activities

The following activities are prohibited:

- Installing unauthorised software
- Downloading illegal or inappropriate content
- Modifying system configurations without approval
- Removing or disabling security software
- Using equipment for personal business
- Sharing equipment access credentials
- Connecting unauthorised peripherals
- Using equipment for illegal activities

7. Software and Applications

7.1 Approved Software

- Only approved software may be installed

- Software licenses must be valid
- Request additional software through IT
- Do not copy or distribute licensed software

7.2 Updates and Patches

- Allow automatic security updates
- Do not defer critical updates
- Report issues with updates to IT
- Restart devices when required for updates

8. Security Requirements

8.1 Device Security

- Enable screen lock with password/PIN
- Lock device when unattended
- Do not share passwords or access
- Report lost or stolen devices immediately
- Keep antivirus software active and updated

8.2 Physical Security

- Secure portable devices when not in use
- Do not leave devices unattended in public
- Use cable locks where provided
- Store devices securely when travelling
- Keep equipment away from food and liquids

9. Care and Maintenance

9.1 User Responsibilities

- Handle equipment with care
- Keep devices clean and in good condition
- Protect from environmental damage
- Transport laptops in protective cases
- Report damage or faults promptly

9.2 Repairs and Maintenance

- Do not attempt to repair equipment yourself
- Report all issues to IT
- Only authorised personnel may service equipment
- Follow instructions for warranty claims

10. Data Storage

- Save work files to approved locations
- Use company file sharing and backup systems
- Do not store sensitive data on local drives unnecessarily
- Back up important files regularly
- Do not store personal files excessively

11. Printing and Consumables

- Print only when necessary
- Use double-sided printing where possible
- Collect printouts promptly, especially confidential
- Report printer issues to IT
- Do not print excessive personal material

12. Remote and Mobile Use

When using company devices outside the workplace:

- Follow all security requirements
- Use secure networks or VPN
- Do not leave devices visible in vehicles
- Be mindful of screen visibility in public
- Ensure devices are transported safely

13. Return of Equipment

13.1 When Required

Equipment must be returned:

- When employment ends
- When requested by management
- When equipment is being upgraded
- During extended leave if required

13.2 Return Process

- Return all equipment and accessories
- Equipment will be checked against the register
- Data will be wiped according to procedures
- Outstanding items may be recovered or charged

14. Loss and Damage

14.1 Reporting

- Report loss or theft immediately
- Report any damage promptly
- Complete incident reports as required
- Cooperate with investigations

14.2 Liability

- Employees may be liable for damage due to negligence
- Each case assessed individually
- Normal wear and tear is expected

15. Monitoring

[Company Name] may monitor use of IT equipment:

- For security purposes
- To ensure policy compliance
- To protect company assets
- As required by law

Users should have no expectation of privacy when using company equipment.

16. Responsibilities

16.1 Employees

- Use equipment responsibly
- Protect equipment from loss and damage
- Comply with this policy
- Report issues promptly

16.2 IT Department

- Maintain equipment register
- Provide technical support
- Manage equipment lifecycle
- Ensure security compliance

17. Policy Breaches

Breaches of this policy may result in:

- Withdrawal of equipment privileges
- Disciplinary action

- Requirement to pay for damage
- Termination for serious breaches

18. Review

This policy will be reviewed:

- At least annually
- When technology changes
- When business needs change

Employee Acknowledgement

I acknowledge that I have read and understood [Company Name]'s IT & Device Use Policy. I understand my responsibilities for company IT equipment and agree to comply with this policy.

Employee Name: _____

Signature: _____

Date: _____