Acceptable IT and Internet Use Policy

At [Organisation Name], we recognise the importance of maintaining a secure and productive IT and internet environment. This policy outlines the guidelines and responsibilities for the acceptable use of IT resources and internet access.

Scope

This policy applies to all employees, contractors, volunteers, and authorized users who have access to [Organisation Name]'s IT resources and internet facilities. It encompasses all devices, systems, networks, and software provided by the company for business use, including but not limited to computers, laptops, tablets, smartphones, email systems, and internet access.

Responsibilities

Management:

- Management is responsible for establishing and enforcing IT and internet use policies in accordance with Australian legislative requirements.
- They are responsible for providing appropriate training and resources to employees to ensure they understand their responsibilities regarding IT security and acceptable internet use.
- Management must monitor compliance with this policy and take appropriate disciplinary action in cases of non-compliance or misconduct.

IT Department:

- The IT department is responsible for maintaining the security and integrity of [Organisation Name]'s IT infrastructure, including networks, systems, and software.
- They must implement technical measures, such as firewalls, antivirus software, and access controls, to protect against cyber threats and unauthorised access.
- The IT department must conduct regular audits and assessments to identify and address potential security vulnerabilities or breaches.

Employees:

- Employees are responsible for using [Organisation Name]'s IT resources and internet access in a responsible, ethical, and lawful manner.
- They must comply with all applicable laws, regulations, and company policies regarding IT security, data protection, and acceptable internet use.
- Employees should exercise caution when accessing and sharing information online, avoid visiting unauthorized or inappropriate websites, and refrain from engaging in activities that may compromise IT security or the reputation of the company.

Acceptable Use Guidelines

Authorized Use: IT resources and internet access provided by [Organisation Name] are to be used for business purposes only. Personal use is permitted within reasonable limits but should not interfere with work responsibilities or consume excessive bandwidth.

Data Protection: Employees must take measures to protect sensitive and confidential information from unauthorised access, disclosure, or loss. This includes using strong passwords, encrypting sensitive data, and following company policies for data handling and storage.

Cybersecurity: Employees should be vigilant for phishing scams, malware, and other cyber threats, and report any suspicious activities or security incidents to the IT department immediately. They must not engage in activities that may compromise IT security, such as downloading unauthorised software or accessing unsecured networks.

Internet Access: Access to the internet is provided for work-related research, communication, and collaboration purposes. Employees should use the internet responsibly and refrain from accessing websites or content that is offensive, illegal, or in violation of company policies.

Social Media and Online Conduct: Employees representing [Organisation Name] on social media platforms or online forums must adhere to the company's social media policy and conduct themselves professionally and respectfully. They should not disclose confidential information or make derogatory remarks about the company, colleagues, clients, stakeholders etc.

Compliance and Enforcement

Non-compliance with this policy may result in disciplinary action, up to and including termination of employment or legal consequences, depending on the severity of the violation. Employees who have concerns or questions about acceptable IT and internet use should contact their supervisor or the IT department for guidance and support.

Review and Updates

This policy will be reviewed periodically to ensure its effectiveness and compliance with Australian legislative requirements and industry standards. Updates may be made as necessary to reflect changes in technology, business practices, or legal requirements.

Authorised by

[Sign]

[Name]
[Position]
[Company]