Safe Places for Children

IT ACCEPTABLE USE POLICY

Safe Places Australia Limited and all related bodies corporate (Safe Places) is committed to providing and maintaining secure, effective, and reliable IT infrastructure and services. This objective supports the Safe Places vision and the ongoing commitment to our mission that at Safe Places it's all about the young people. The enforcement of these acceptable use and security requirements has been established to protect all internal and external stakeholders from problems such as error, fraud, defamation, breach of copyright, unlawful discrimination, illegal activity, privacy violations and service interruptions.

The purpose of this policy is to set clear parameters and expectations for the appropriate use of the Safe Places information technology resources. All employees, contractors, vendors, and any other individual granted access to Safe Places IT resources (including computer systems, mobile phones, networks, software, and data) shall comply with the following:

- **Authorised Use**: IT resources are to be used solely for business-related activities and within the scope of employment or contractual obligations. Personal web browsing use is permitted only during designated break times and should not interfere with work responsibilities.
- **Access Control**: Employees must safeguard their credentials and ensure that unauthorised individuals do not gain access to their accounts. Sharing passwords, attempting to bypass security measures, or accessing others' accounts without permission is strictly prohibited.
- **Data Protection**: Employees are responsible for protecting sensitive and confidential information. Data must be stored, transmitted, and disposed of according to the Safe Places data security policies and relevant regulations. Data should never be downloaded to portable drives or forwarded to personal email accounts.
- **Malicious Activities**: Engaging in any form of hacking, malware distribution, unauthorised network probing, or any activity that compromises the integrity of IT resources is strictly prohibited.
- **Software Usage**: Software installation must comply with the Safe Places software licensing agreements. Only authorised software should be installed, and users should refrain from using unauthorised, pirated, or unlicensed software.
- **Network Usage**: Network resources are to be used responsibly and efficiently. Activities such as excessive bandwidth consumption (downloading), streaming unrelated to work, or engaging in online gaming are prohibited. Any attempt to bypass network controls is strictly prohibited.
- **Email Etiquette**: Employees are expected to use Safe Places email for business-related communication only. Respectful and professional language should be maintained in all emails. Employees should not cc their own private email address when sending business related emails.
- **Phishing Awareness**: Employees should exercise caution when handling email attachments or links from unknown or suspicious sources. All suspicious emails must be reported to the IT department.
- **Professional Conduct**: While using social media on Safe Places premises or using Safe Places resources, users should maintain a professional tone and avoid posting content that could harm Safe Places reputation.
- **Internet Browsing**: Internet usage should be work-related. Visiting inappropriate content (offensive, obscene, pornographic, sexually suggestive, abusive, discriminatory, defamatory, threating, bulling, hateful, racist, sexist, that infringes copyright, or is otherwise unlawful) gambling, or malicious websites are prohibited.

All Safe Places employees have a responsibility to safeguard the security, reliability, and ethical use of all information technology resources, while promoting a productive and safe computing environment for all users. Employees who receive internal or external electronic communication that is offensive or inappropriate, should inform their supervisor immediately. All suspected violation of this policy must be reported to your supervisor and/or the IT department. Violation of this policy may result in disciplinary action, up to and including termination of employment or contractual agreement. Legal action may be taken for serious breaches.

This policy was approved by the Managing Director on the 16th August 2023.