# IT Acceptable Use Policy

PeopleIN Ltd ACN 615 173 076

adopted on 27 February 2023

Contents

## 1 Purpose and Context

The IT Acceptable Use Policy is designed to provide a general framework and boundaries of technology resources around the use of technology for all PeopleIN employees, contractors, consultants, temporary employees, vendors, visitors, business partners, and others performing work for PeopleIN and or its entities. The primary focus of the policy is to help users understand what is/isn't acceptable including behaviour, actions, and uses for IT resources, technology, systems, data, and IT facilities.

At its highest level this policy covers the following key points:

- Ensures Information Technology (IT) resources including computers, networks, and internet connections are used for business purposes and extremely limited personal use.
- Provides guidelines to reduce the risks, threats, and impacts from the misuse of internet, IT systems, data, etc. These risks can include items such as virus attacks, compromise of networks and systems, data loss, and licensing/legal issues.
- Always ensures that all PeopleIN personnel use information and data appropriately while respecting the confidentiality of the information and data used in the course of their employment.
- Manages security effectively through a collaborative effort involving the participation and support of every PeopleIN employee and affiliate. It is the responsibility of all employees and anyone using PeopleIN technology resources to know these guidelines and to conduct their activities accordingly.
- Confirms that this policy always applies, while PeopleIN owned computers or personally owned devices accessing PeopleIN systems or data, network connections or internet connections are in use, regardless of the location of the user.
- Validates that this policy also forms part of the Code of Conduct to be observed by technology users.

## 2 Policy Objectives

PeopleIN technology users are provided with access to the internet, software applications, computing, mobile devices, and network resources to assist with the performance of their individual duties for official business purposes.

All software, telecommunications systems, data, and company issues computers are the property of PeopleIN Ltd. and may only be used for authorised business purposes. Regardless of the mode of access, company owned device or personal device, all users of PeopleIN's IT systems and are responsible for using these facilities in a professional, ethical, and lawful manner.

The objective of the policy is to describe and define the boundaries of acceptable use that applies to all users

of PeopleIN's IT systems.

## 3 Scope and Audience

The scope of this policy extends to the use of all PeopleIN IT systems including, but not limited to, hardware, software, data, network, internet access, or mobile device regardless of the nature of how it is hosted – internally or via a hosting provider.

This policy applies to all users of PeopleIN owned or managed IT systems, regardless of the physical location of the user (e.g., Office, mobile, hotel. home), IT systems, or equipment used.

Users of PeopleIN IT facilities includes all types of PeopleIN employees, contractors, consultants, temporary employees, vendors, visitors, business partners, and others performing work for PeopleIN and/or its associated Business Units, or any person engaged to undertake business with or within PeopleIN and use PeopleIN IT systems in their role.

This policy also applies to any users utilising their own equipment over PeopleIN's networks or internet connections.

## 4 Roles and Responsibilities

| Role | Responsibilities |
|---|---|
| **IT Leadership** | Responsible for ensuring that the IT Acceptable Use Policy is understood and applied within their organisations. |
| **Branch and General Managers** | Promote and ensure that these policies are followed within their business areas. |
| **PeopleIN staff** | All users are responsible to make sure that their use of PeopleIN's IT resources adheres to PeopleIN's various IT policies. Users are responsible for any activity carried out using their accounts. Passwords may not be shared and should not be easily accessible to others.<br>Any observable breaches of these policies should be reported to the Head of Information Technology.<br>Any questions about the policies should be directed to the Head of Information Technology. |

## 5 Policy Detail

By accessing PeopleIN's IT infrastructure, networks, services or application solutions, the user accepts the following:

### 5.1 Business Purposes

PeopleIN provides the IT environment for business purposes, however, users may use the IT environment for limited personal use during the employee's normal business hours, non-business use must be:

- Infrequent and brief
- Not a violation of any governmental policy, legislation, or regulation at a state, regional or national level
- Meets the other obligations set out in this document and other PeopleIN policies
- Causes no additional expense to PeopleIN

### 5.2 Proprietary Information

Any files, data pictures, screen shots, or information that is created, stored, or downloaded to any PeopleIN device including portable media (USB Drives, CDs/DVDs, etc.) are owned by PeopleIN. Downloading data to a personal device is prohibited.

### 5.3 Inappropriate Material

- The actions of the user will not cause inappropriate material to be accessed, sent, received, displayed, printed, or otherwise disseminated, or brought into PeopleIN's environment.
- The actions of the user will not violate the PeopleIN IT Acceptable Use Policies imposed by contract and/or any acceptable use policies of a client when performing work at their facility.
- Inappropriate material is anything deemed to be offensive, fraudulent, illegal or which a reasonable person would, in the opinion of PeopleIN HR, consider embarrassing, sexually explicit, obscene, intimidating, defamatory, racist, sexist, or would amount to harassment.
- Any access of material deemed to be illegal is strictly prohibited and will be dealt with promptly, including reporting to the relevant law enforcement agencies, as appropriate. PeopleIN staff may also face internal disciplinary action including:
    - A formal reprimand or other disciplinary action
    - Withdrawal of access to IT resources/services
    - In serious cases, breaches of this policy may be grounds for dismissal

### 5.4 Copyright, Licensing, Software Installation

- All software used in PeopleIN's IT environment must be licensed to PeopleIN or its affiliates. The use of software licensed to other organisations or individuals is not permitted.
- The use of unlicensed software is not permitted.
- Users are not to install any trial software, new software, or modify existing software without prior approval from the PeopleIN IT team. IT support staff may remove any unsupported software from PeopleIN's IT environment.
- Users shall not copy, dispose, or transfer any commercial software provided by PeopleIN

### 5.5 Data Integrity, Security, Availability, Saving, Taking Offsite

- Users shall not use or access any other user's account. Authorised members of PeopleIN IT Support staff undertaking support functions should use administrator ID accounts to deliver necessary support. Sharing user account credentials (ID and passwords) is prohibited.
- Passwords must follow the complexity and other requirements detailed in the PeopleIN Access Control policy and **must not** be:
    - Easily identifiable
    - Recorded in such a way that it may be easily seen, accessed, or used by others
    - Disclosed to any person. The only exception is when an authorised member of PeopleIN IT support staff needs access to provide support and an employee is not available to login themselves. If a password is provided to PeopleIN IT Support the Support Analyst, as part of policy, must change the password once the support service is completed. This will force the account owner to create another secure password.
    - Service Desk staff, if they must do this, should mark the user account as expired and force the user to do a password change.
    - Users are not to hack, tamper, damage, or unnecessarily modify or delete any of PeopleIN's data whether stored on servers, local drives, email systems, or other storage media.
    - Users are to follow the IT security policies, procedures and controls put in place by PeopleIN IT.
    - Any files emailed or opened on a PeopleIN device will be automatically virus scanned. The virus scan always runs on local machines. If a user is accessing a USB device, they can trigger a scan of the whole device otherwise the virus scan will only target files upon access.

- Users shall only access, modify, or remove data stored on PeopleIn IT resources where they have authority to do so.

### 5.6 Cause Harm, Misuse, Install Hardware

- Users must use the IT environment responsibly. That is, not to knowingly cause harm, delays, outages, or disruptions to other users.

- Users are not to install new hardware or modify existing hardware devices without prior approval from the IT Service Desk. This includes any hardware purchased individually or brought in from home.

- Users should attempt to minimise heavy system usage, such as sending large emails or printing excessively large files, etc. as PeopleIN does have limitations on file size. If you are unable to send or receive a file due to file size restrictions, please contact the IT Service Desk for assistance and access to proper large file transfer tools.

- Users shall not use any PeopleIN or IT resources to harass others or to interfere with their work. For example, to send or publish obscene, abusive, fraudulent, threatening, repetitive, chain style, or advertising (SPAM) messages to a user or group of users.

### 5.7 Purchasing

Any technology purchasing must follow PeopleIN IT standards. Any purchases outside of these standards must be pre-approved by the Head of Information Technology. The Level of Authority policy located on the PeopleIn Intranet specifically details delegated spending authority limits in relation to IT spending.

### 5.8 Non-Business-Related Data

Unless previously approved by the Head of Information Technology, non-business-related files including music, picture, or video files will be removed from any shared system drives. PeopleIN IT support staff may remove these files at any time and for any reason or where they impact the normal operation of the device or network. These files must comply with this policy in reference to inappropriate material.

### 5.9 Remote Access/Home Support

- PeopleIN IT will not provide support for any personal owned devices or related hardware, software, connectivity, or applications.

### 5.10 Internet Usage

- The following activities are strictly prohibited:

    - Sending, receiving, displaying, printing, or otherwise disseminating material that would

match the definition of inappropriate material above

- Accessing websites that contain material that would match the definition of inappropriate material listed under Item 5.3
- Using PeopleIN's internet resources for unauthorised commercial or personal advertisements, solicitations, promotions, political material, or any other similar use unless it's expressly authorised by your supervisor or the Head of Information Technology
- Downloading or uploading personal audio or visual material on the internet at any time
- Accessing the internet other than through the PeopleIN's systems, for example, accessing the internet through identity concealed means is strictly prohibited
- Allowing external sources to access the PeopleIN network and IT systems. If external access is required, it must be approved in writing by the Head of Information Technology
- Violating the Intellectual Property Rights of PeopleIN or others, such as breaching copyright by copying graphics or text material or using other license software without authorisation of the Head of Information Technology.

### 5.11 Email Usage

- Staff may send 'personal email', that is, non-work-related emails or internal emails provided that:
  - Only minimal amounts of personal email are accessed (read, sent, or forwarded)
  - They are sent during designated breaks or rest periods
  - All other rules set out in this policy are complied with.
- All email and attachments via PeopleIN mail systems are the property of PeopleIN Ltd. And is not private.
- All staff should be vigilant around email from unidentified sources, with unknown or strange attachments, or with abnormal information requests, as potential phishing, or virus scams. If unsure the IT Service Desk should be contacted.
- All email that uses PeopleIN's name and address and gives the impression that the sender is speaking with the authority of PeopleIN (even though this may not be the case and PeopleIN may not have authorised this):
  - May, in certain circumstances, be inspected by parties outside of PeopleIN, for example, in the event of litigation

- Is automatically copied. All incoming and outgoing email is automatically logged and/or saved to a PeopleIN server for archival purposes
- Is not guaranteed to be delivered. There are many possible reasons within the email infrastructure, networks, and the internet, both inside PeopleIN and external, for email delivery being delayed or prevented. Time critical emails should be confirmed with the intended receiver. In the general course of business, emails are delivered promptly, or the sender will receive a notification of non- delivery
- Containing files with an ".exe" extension should not be opened without consulting the IT Service Desk.

- The following activities are strictly prohibited:
  - Subscribing to non-work-related mailing lists, sending unsolicited email messages (spam)
  - Sending email using another user's email address unless such use is expressly authorised by that user
  - Inappropriate usage of distribution lists. Best judgement should always be used, if unsure about appropriate email distribution list usage a local marketing representative should be consulted

### 5.12 Teams Usage

- PeopleIN utilises Microsoft Teams to facilitate communications between staff via instant messaging (IM), voice and video. Teams' usage is:
  - Limited to work related communications
  - Stored in accordance with PeopleIN retention policies
  - Designed to be used in place of long distance calling and to enhance collaboration
- It is appropriate to use Teams video capabilities from locations with sufficient bandwidt

## 6 Enforcement

**Auditing and Monitoring**

PeopleIN reserves the right to monitor, track, and audits its IT environment. PeopleIN will conduct audits from time to time to ensure compliance with its Information Technology policies. PeopleIN may monitor and track specific components of the IT environment upon request from senior management or where required to do so by law (e.g., Search warrant).

**Breaches**

Breaches of the policies set out in this document may result in:

- Formal reprimand or other disciplinary action
- Termination of internet access
- Disciplinary actions and/or dismissal

## 7 Review

The Head of Information Technology and/or its delegates are responsible for the annual review of this policy.

## 8 References

This policy should be read in conjunction with PeopleIN's other policies including:

- Code of Conduct Policy
- PeopleIN Infrastructure, Data and Cybersecurity Policy
- IT Access Control Policy