Alpine Resorts Victoria

# Mobile Devices

## Safe and Acceptable Use of Mobile Devices Policy

## 1. Overview

In the modern workplace, a range of mobile devices are used as effective communication tools. However, in certain situations mobile devices can be distracting to staff or cause a hazard in the workplace. Further, whilst mobile devices are convenient for staff to access information whilst on-the-go, appropriate security measures must be implemented to ensure public sector information is stored and accessed in a secure manner.

## 2. Purpose of the Policy

The purpose of this policy is to provide staff with guidelines regarding the safe and appropriate use of mobile devices in the workplace, when ARV-supplied mobile devices are to be issued, and how information on mobile devices is secured.

## 3. Scope

The scope of this policy applies to employees, board members, contractors, and delegates of ARV.

## 4. Policy

### 4.1 Safe use of mobile devices

A mobile device may be operated when driving a light passenger or utility vehicle only if safe to do so and when permitted by law. It is noted relevant mobile phone use legislation may be changed by other state agencies from time to time, and employees wishing to safely operate a mobile phone whilst driving must make themselves familiar with and adhere to any relevant road safety legislation.

Under **Distracted Driver Road Rules** in Victoria, a fully licensed driver may use a phone to make or receive a phone call, to use its audio/music functions or perform a navigational (GPS) or intelligent highway vehicle system (in vehicle warning system) function but only if the phone:

- is secured in a commercially designed holder fixed to the vehicle, or
- can be operated by the driver without touching any part of the phone, and the phone is not resting on any part of the driver's body.

All other functions (including video calls, texting, emailing, task management, photography, social media, shopping and share economy apps) are prohibited while driving.
No mobile device function of any kind may be used when operating plant equipment or over-snow vehicles at any time, unless if exempted in an approved SWMS or JSA document.
A mobile device may not be operated in certain workplaces, including but not limited to when performing refuelling operations, in some medical centre settings, and other locations indicated that mobile device use is not permitted.

### 4.2 Acceptable use

Mobile devices, both ARV-supplied and personal mobile devices, are to be used during work hours for tasks that clearly relate to their ARV work duties.

Limited and reasonable personal use is permitted for minor activities such as communication, internet browsing and reading. Limited and reasonable personal use must not impact an employee's performance in their role.

Employees must not send, view, download or store illicit, fraudulent, obscene content on ARV-supplied mobile devices. All staff are to adhere to the Victorian Public Sector Code of Conduct when accessing content on a mobile device.

### 4.3 ARV-supplied mobile devices

Employees may be issued with ARV-supplied mobile devices if required for their duties. The following factors are taken into consideration when determining if an ARV mobile device needs to be supplied for the role:

- frequently moves around the resort for operational tasks and needs to remain contactable, for example trade roles;
- requires a high degree of remote work,or works across multiple resorts and corporate office locations.
- needs to be readily contactable by a wide range of staff, stakeholders and entities, to make a high number of work calls, and be available at a wide range of hours, for example Senior Management roles.
- performs an On Call or Emergency Management component as part of their role.

Approval for an ARV-supplied mobile device will either be stated as Equipment on their Employment Contract, or if approved in writing from a General Manager or the CEO.

The Head of ICT or their delegate will select the most appropriate mobile device hardware, accessories, and service plan based on ARV procurement principles and job requirements.

ARV employees must take reasonable care of ARV-supplied mobile devices issued to them, and promptly report any loss, theft or damage to their Manager. If the employee has contributed to the circumstances in which the device is lost, stolen, or damaged (e.g. through lack of care), then the employee may be responsible for the cost of repair or replacement.

An ARV-supplied mobile device may be used for limited and reasonable personal use of domestic calls, text, and data providing the allowance on the service plan is not exceeded. If the service plan allowance is exceeded as a result of excessive personal use, the employee will be responsible for reimbursing ARV for the additional charges incurred.

International calls, texting, and data roaming are not permitted unless authorised in writing by a General Manager or the CEO. When authorised, international usage will be for a set duration and is not ongoing.

ARV employees with an ARV-supplied mobile device are to make themselves reasonably contactable during work shifts and when rostered on-call. Contact details for ARV-supplied mobile devices will be listed on the Corporate Directory.

### 4.4 Personal mobile devices

It is acknowledged that from time-to-time ARV employees may need to use their personal mobile device for ARV work purposes, or employees eligible to be issued with an ARV-supplied mobile device may have a preference to use their own personal device instead.
The actual costs of ARV work related calls, text, and data usage may be reimbursed if they can be reasonably apportioned from personal usage. The maximum cap reimbursed for work use on a personal phone plan will be the equivalent amount to if the staff member was on the ARV Corporate Account (as of June 2023 this is $35/month).

### 4.5 Personal mobile devices for Multifactor Authentication technology

In line with the Protective Data Security Plan a required Information Access measure is for Victorian organisations to implement logical access controls, such as Multifactor Authentication (MFA), as an access control to Victorian Government public sector information.

As a result of this requirement, ARV employees may be reasonably requested to receive occasional authentication codes, push notifications, or similar Multifactor Authentication technology to a personal mobile device. Due to the minimal data requirement required for this technology, MFA is considered a reasonable request and MFA data usage alone is not eligible for reimbursement.

### 4.6 Information Security of ARV data on mobile devices

ARV employees using mobile devices to access public sector information are bound by the **Network Access and Authentication Policy** and related policies as amended from time to time.

The Head of ICT is responsible for overseeing information security controls on mobile devices (both ARV - supplied mobile devices and the work component of personal mobile devices). Due to an evolving cyber security landscape, information security controls will be updated from time to time to reflect Victorian government and industry information security best practices.
Due to the nature of personal mobile devices, work use functionality may be limited compared to the functionality of an ARV-supplied mobile device.

If a mobile device is suspected of containing malware, computer virus, or similar security threat, ICT staff may remove the mobile device from the ARV network or perform other appropriate response measures as detailed in the ARV Cyber Incident Response Plan.

If an ARV-supplied mobile device is suspected to be lost, stolen, or otherwise compromised, ICT staff are authorised to issue a “device erasure”, “device lockout”, or similar remote commands in order to protect both the hardware and public sector information from potential misuse.

If a personal mobile device used for work purposes is suspected to be lost, stolen, or otherwise compromised, ICT staff are authorised to issue remote commands to remove ARV public sector information from the device.

### 4.7 Applicability of other policies

This document is part of the organisation’s cohesive set of information security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

## 5. Relevant External Agencies

**Office of the Victorian Information Commissioner**, notably the Protective Data Security Plan where controls are required for Information Access: An organisation establishes, implements and maintains an access management process for controlling access to public sector information.

**Victorian Public Sector Commission**, notably the Code of Conduct for Victorian Public Sector Employees.

## 6. Enforcement

Employees identified as breaching this policy may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment.

Where persons suspected to be involved in illegal activities or theft of organisation property (physical or intellectual), the organisation will report such activities to law enforcement authorities as appropriate.

## 7. Definitions

**Mobile Device** any piece of electronic equipment such as a mobile phone or small computer that can be used in different places. This includes tablets, smart watches, and wearables.

## 8. Authorisation and Document parameters

| | | | |
|---|---|---|---|
| **Document Reference:** | BP.CS.2 | **Owner:** | Board |
| **Approved By:** | Board | **Approval Date:** | 19/06/2023 |
| **Last Amended:** | N/A | **Next Review Date:** | 30/06/2026 |
| **Comments:** | This policy replaces all Mobile Devices Policies within all Victorian Alpine Resorts from the date of approval. | | |