

AR0150 – Mobile Device Personal Use

Interior Health would like to recognize and acknowledge the traditional, ancestral, and unceded territories of the Dākelh Dené, Ktunaxa, Nlaka’pamux, Secwépemc, St’át’imc, Syilx, and T̓sìlhqot’in Nations, where we live, learn, collaborate and work together.

Interior Health recognizes that diversity in the workplace shapes values, attitudes, expectations, perception of self and others and in turn impacts behaviors in the workplace. The dimensions of a diverse workplace includes the protected characteristics under the human rights code of: race, color, ancestry, place of origin, political belief, religion, marital status, family status, physical disability, mental disability, sex, sexual orientation, gender identity or expression, age, criminal or summary conviction unrelated to employment.

1.0 PURPOSE

To define appropriate Personal Use and processes of Interior Health (IH) provided Mobile Devices.

2.0 DEFINITIONS

TERM	DEFINITION
<i>Mobile Device</i>	<i>Any cellular enabled device – typically a phone or tablet – issued to an IH employee as a requirement to enable them to fulfill their responsibilities.</i>
<i>Personal Use</i>	<i>Use that is not business related and is for an individual's own consumption and/or enjoyment.</i>
<i>Personal Data</i>	<p><i>All data on the device that does not belong to IH and/or that is not the result or product of any work performed for IH. This could include but is not limited to:</i></p> <ul style="list-style-type: none"> <i>• Files</i> <i>• Location or GPS data</i> <i>• Credentials used to access other non-IH services particularly social media sites</i> <i>• Device PINs and passwords</i> <i>• Personal contact information</i> <i>• History logs including web logs</i> <i>• Personal email or personal social media communications</i> <i>• Personally-purchased movies, music, e-books, or apps</i> <i>• Phone conversations, text messages, or logs</i> <i>• Screenshots, input or output of microphones, cameras, or keyboards</i>
<i>Erase</i>	<i>The process of deleting and removing all content permanently from an IH provided Mobile Device.</i>

Policy Sponsor: VP, Digital Health		1 of 3
Policy Steward: Manager, Workplace Technologies		
Date Approved: August 1, 2023	Date(s) Reviewed-r/Revised-R:	
<i>This is an Interior Health CONTROLLED document. A copy of this document in paper form is not controlled and should be checked against the electronic file version to ensure accuracy.</i>		

AR0150 – Mobile Device Personal Use

<i>Mobile Device Management</i>	<i>A tool used to manage all IH assigned Mobile Devices that enables deployment of IH business applications, apply certain settings and controls, and remotely Erase a phone if required.</i>
---------------------------------	---

3.0 POLICY

- 3.1 IH provides Mobile Devices, such as cellular phones, to employees whose role requires them to carry a phone and have more convenient access to work-related information and collaboration tools i.e., email / instant messaging and Microsoft Teams.
- 3.2 Personal Use is limited to within Canada. Mobile Devices are configured for cellular use in Canada only.
 - 3.2.1 For business related travel outside of Canada, travel packages can be purchased with approval from the employee’s manager as outlined in [Section 2.8 of the Travel User Guide](#).
- 3.3 Personal Use must align to the limitations of the monthly paid rate plan provided by IH for business use.
 - 3.3.1 Business use takes precedent over Personal Use as it applies to the rate plan allowances for voice and data.
 - 3.3.2 Personal Use may fill the gap between consumed allowances for business use, and the remainder of services up to the limitations of the rate plan. For example, if a 5GB data plan is assigned to an employee for their role and business requirements use 3GB each month within the billing period, the employee could consume the remaining 2GB of data for Personal Use.
- 3.4 The provided Mobile Device is the property of IH and remains a business device.
 - 3.4.1 Devices are managed using a Mobile Device Management tool.
 - 3.4.2 Personal Data placed on the device by the assigned employee is not the responsibility of IH to support, maintain, backup, or manage.
 - 3.4.3 Employees are responsible for backing up their personal data to a Personal Data storage location (i.e., personal cloud storage) including all photos, videos, documents, etc.
 - 3.4.4 Information within IH phones is subject to FOI requests.
- 3.5 Lost or stolen devices must be reported immediately to the [Digital Health Service Desk](#) and to Information Privacy, and will be remotely locked or Erased.
- 3.6 If a Mobile Device has been compromised, IH Digital Health holds the decision on whether to Erase a device, including all content, to minimize any cybersecurity risk that may exist to IH.
- 3.7 Devices are selected based on a provincial cellular agreement between IH and a given carrier. A standard device and cellular plan are provided and configured to meet the business needs of the employee and/or business group.

Policy Sponsor: VP, Digital Health	2 of 3
Policy Steward: Manager, Workplace Technologies	
Date Approved: August 1, 2023	Date(s) Reviewed-r/Revised-R:
<i>This is an Interior Health CONTROLLED document. A copy of this document in paper form is not controlled and should be checked against the electronic file version to ensure accuracy.</i>	



AR0150 – Mobile Device Personal Use

- 3.7.1 Accommodation to support accessibility or business requirements may be provided to those who have a reasonable need, i.e., larger screen, higher data capacity plan.
- 3.8 It is the responsibility of the employee to reimburse IH for charges incurred from Personal Use which exceed the monthly rate plan.
- 3.9 The employee’s manager is responsible for ensuring that charges to IH based on Personal Use are reimbursed to the organization. In exceptional circumstances, an employee’s director may waive the requirement to reimburse for Personal Use.
- 3.10 All Mobile Device users must read and accept these terms as part of the mobile phone request process.
- 3.11 IH provided mobile devices must not be used by anyone other than the employee.
- 3.12 Personal Use of a Mobile Device must adhere to Section 3.2 of [AR0100 – Acceptable Use of Digital Information Systems](#).

4.0 PROCEDURES

- 4.1 Request for a new phone
 - 4.1.1 All requests are processed through the [Service Now Service Request portal](#). This web application includes all items that can be ordered and configured for an employee, including processes for manager approval, and tracking of requests as they flow through the various fulfillment steps.
- 4.2 Request for Travel Plan for business: Contact [IH Mobility Services](#)
- 4.3 Process to review billing and identify personal charges/data overages:
 - 4.3.1 [IH Mobility Reporting Process](#)
- 4.4 Process to repay personal charges/data overages: Contact [IH Mobility Services](#)

5.0 REFERENCES

1. [AU0100 – Standards of Conduct for IH Employees](#)
2. [AR0400 – Privacy and Management of Confidential Information](#)
3. [AP0300 – Travel and Meeting Expense](#)
4. [AR0500 – Email & Text Messaging](#)
5. [AR0100 – Acceptable Use of Digital Information Systems](#)
6. [AF0100 – Freedom of Information](#)
7. [AL0700 – Records Retention](#)

Policy Sponsor: VP, Digital Health	3 of 3
Policy Steward: Manager, Workplace Technologies	
Date Approved: August 1, 2023	Date(s) Reviewed-r/Revised-R:
<i>This is an Interior Health CONTROLLED document. A copy of this document in paper form is not controlled and should be checked against the electronic file version to ensure accuracy.</i>	