MAHI MIHINARE
ANGLICAN ACTION

MOBILE DEVICE POLICY

Category:	Information and Communications Technology
Last Review Date:	December 2021
Next Review Date:	December 2023
Endorsed by:	The Anglican Action Missioner
Approved by:	The Anglican Action Mission Trust Board

Purpose

The purpose of this policy is to ensure the appropriate purchase and use of mobile devices connected to the Mission mobile plan.

Statement

Anglican Action recognises the need for authorised staff to have access to a Mission mobile device for agency purposes.

Scope

This policy applies to all mobile devices:

(a) owned by the Mission
(b) connected to the Mission's mobile plan
(c) used for Mission purposes.

Definitions

Agency	Agency means the Employer or Staff member as applicable.
Approved supplier	Approved supplier means a service provider/vendor with whom the Mission has a formal negotiated supply agreement
Client	Client means any individual, family, group of persons, incorporated body, association, or community on whose behalf

	the agency provides or agrees to provide a service or to whom the agency is legally obligated to provide a service.
Employer	Employer means 'The Anglican Action Mission Trust Board', referred to as 'Anglican Action', 'Agency or 'The Mission' in this policy.
Mission mobile device	Mission mobile device means any mobile device owned by the Mission.
Mission mobile plan	Mission mobile plan means the mobile device service and usage options selected by the Mission and provided by the approved supplier.
Mission purposes	Agency purposes means any activity that a staff member is expected to undertake during the course of their work.
Mobile device	Mobile Device means any device that connects to a cellular network (e.g., mobile phone, tablet, SIM card or mobile data stick)
Mobile device account	Mobile device account means the provision and record of services and usage for a specific mobile device
Mobile device holder	Mobile device holder means the staff member to whom the mobile device has been issued
Personal information	Personal information means information about an identifiable individual.
Social Media	Social Media means the collective of online communication channels, portals and websites dedicated to facilitating community-based interactions, sharing and collaborations. Social media allow people to socially interact, converse, network and share with one another online; examples of social media sites and applications include Facebook, YouTube, Twitter, and Instagram.
Staff member	Staff member means all employees (permanent, fixed-term, or casual), trustees, consultants, contractors, service providers, students, and volunteers engaged by the Mission.

Policy

1. Staff may be issued a mobile device if their Mission responsibilities require:
   (a) that they use a mobile device in their day to day work
   (b) they must be reachable immediately
   (c) they are on call outside of normal business hours
   (d) they are often not based at a fixed place of work and need to be easily contactable
   (e) they make frequent and/or prolonged travel outside of their main work place

2. Authority to approve the provision of a mobile device to a staff member rests with the General Manager
3. Mission mobile phones, SIM cards and mobile data sticks must be purchased from an approved supplier
4. The Mobile device to be purchased should be the most cost-effective model that will enable the staff member to efficiently carry out their work
5. Mission mobile devices must use the Mission mobile plan. Exceptions to this must be approved by Management
6. Mobile phone numbers shall be published in Mission directories unless there are specific security/privacy reasons why they should not be. Management will approve exceptions
7. Mobile device holders must always operate mobile devices safely and legally
8. Mobile device holders must take all practical steps to avoid loss or damage to their mobile device(s)
9. The mobile device holder is responsible for the security of the Mission data stored on the mobile device
10. Mobile devices must be locked when not in use by using a PIN, password, biometrics or other such security functionality
11. Usage of all mobile devices on the Mission mobile plan will be monitored
12. All mobile devices on the Mission mobile plan must be configured to connect to the Mission's Wi-Fi networks
13. The Mission may install software and configure its mobile devices for the purposes of security, recovery of devices and compliance with licensing obligations
14. Mission mobile device holders must report, as soon as possible, the loss/theft of a mobile device to Management
15. Any Mission data stored on a mobile device remains the property of the Mission and may be subject to internal investigation or disclosure by the Mission under freedom of information legislation (the Official Information Act and the Privacy Act), or in the course of the discovery process if there is litigation in progress. Those using the mobile device should therefore be aware that there are situations where the Mission may be legally required to disclose information within its power or control, and that it cannot guarantee the complete protection of personal information stored on Mission devices
16. Costs arising from the personal use of chargeable services which are not included in the Mission's mobile plan such as 0900, audioconferencing, PXT, competition TXT etc. shall be reimbursed by the mobile device holder
17. Costs arising from excessive personal data usage as determined by Management (set at 2GB per month as at December 2021) shall be reimbursed by the mobile device holder
18. The Mission may initiate action to recover any personal-use costs from the mobile device holder
19. On cessation of employment with the Mission, a mobile device holder must return all Mission mobile device(s), complete with SIM card and additional accessories to the Infrastructure Team
20. Mission mobile devices and telephone numbers remain the property of the Mission. Exceptions to this must be approved by Management
21. All information on a mobile device must be securely erased before the device is transferred to another staff member

22. Old or unwanted Mission mobile devices must be recycled with a reputable IT recycling firm
23. Breaches of this policy may result in disciplinary action.

Key Accountabilities & Responsibilities

Person / Party	Responsibilities
Governance	Review policy every two years or as required
Management	Ensure that staff members are aware of this policy and processes
Leadership	Ensure that staff members are aware of this policy and processes
Staff	Have access to this policy and understand their obligations

Related Policies, Legislation, Regulations and Documents

- Harmful Digital Communications Act 2015
- Official Information Act 1982
- Privacy Act 2020
- Anglican Action Code of Conduct
- Anglican Action Code of Ethics
- Anglican Action Computer and Internet Use Policy
- Anglican Action Privacy and Personal Information Policy
- Anglican Action Anti-harassment Policy