Risk management for staff taking service devices off-site

The following guidance is general in nature. As every service is unique, you should adapt your practices to suit your service's arrangements and after consulting staff and families where appropriate. You can also check your approach with IT experts and the regulatory authority.

Current requirements:

- The National Model Code states that 'approved providers and their services should have strict controls in place for the appropriate storage and retention of images and videos of children.'
- Under the Australian Privacy Principles 3: 'organisations must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure'.

Governance and approvals

- There should always be a business/operational reason for staff taking devices off-site (including staff taking devices home with them)
- Conduct a risk assessment – keep it on file ready for compliance inspections. Keep risk assessments up to date and do them in consultation with the school/s (if appliable)
- Provide written authorisation for staff, with details of device ID
- Create an agreement for staff to sign that states how devices are to be handled at off-site, including at home, or during excursions and transport – e.g.,:
    - Device must remain secured at all times when not in use (locked bag, safe storage at home)
    - Device must not be shared with family/friends
    - For work purposes only and staff understand privacy and security responsibilities
    - Staff must not use personal cloud accounts or apps to store service data
    - No public Wi-Fi
    - Incident response requirements
- Have clear authorisations and restrictions for who and what data staff can access, modify or disclose off-site – e.g., blocks on accessing apps that include photos/videos of children
- Keep all documents up-to-date and on file, ready for inspection

Device management & configuration

- Have strict security controls – e.g.,
  - Enable biometric lock (face or fingerprint) and a strong passcode, ensure auto-lock out timer is on
  - Multi-Factor Authentication on all on all cloud systems that contain personal information
  - Enrol devices in Mobile Device Management (MDM) (e.g., for apple devices could use https://www.jamf.com/#jamf-small-business)
  - Activate remote lock/wipe through the service IT system/MDM system (e.g., if the device is lost or stolen)
  - Ensure encryptions are enabled
  - Where feasible, don't allow photos/videos of children to be stored on local devices that are taken home - **can configure devices to** capture into a managed app that uploads directly to the service's cloud and auto-clears local caches
  - No screenshots, no personal backups allowed (iCloud, Google Photos)
  - No personal cloud/IDs or app use on the device (social media, messaging apps) – block these from being installed
  - Avoid public Wi-Fi; if used, require VPN; disable AirDrop/Bluetooth sharing by policy; forbid USB exports of images/records

Monitoring and compliance

- Keep a log of devices authorised to leave site, who has them, and when
- Regularly audit devices for compliance
- Train staff on privacy obligations, the National Model Code and what to do if there is a breach or a device is lost or stolen (i.e., contact nominated supervisor immediately so data can be wiped