Bring Your Own Device (BYOD) Policy

Version: 1.0

Last Amendment: N/A

Approved by: Executive Committee

Policy owner/sponsor: Director, Digital Library Services and CIO

Policy Contact Officer: Manager, ICT Services

Policy No: PD/40 TRIM File No: 51966

Date approved: 07/10/2014

Next review: 01/10/2016

1. Summary

Technology is part of the everyday life of the modern public sector worker. Consumer technology is evolving quickly and is often more advanced than the technology available in the workplace. Employees increasingly prefer to use their own smart phones, tablets and other devices to access corporate information. Empowering them to do so supports greater workplace morale, mobility and flexibility.

Many government agencies have adopted the use of mobile communication devices including laptops, smart phones, tablets and similar equipment as efficient business communication tools. The Office of Finance and Services have established government contracts covering the procurement and connection of mobile communication devices for government agencies.

The State Library of New South Wales (the Library) has determined that the use of mobile communication technology for Library staff, contributes to the efficiency and effectiveness of staff, especially when they are remote from the Library or mobile within the premises.

To ensure security of the Library's systems accessed by staff own mobile devices, ICT Services is implementing MDM (**M**obile **D**evice **M**anagement) software. MDM will be used to manage all mobile devices used to access our internal systems and ensure security of corporate data stored on the mobile devices. These procedures will define MDM requirements and roles and responsibilities of staff using their mobile devices to access the Library's internal systems.

The purpose of this policy and associated BYOD procedures is to allow staff to use their own mobile devices if they wish to do so, while also ensuring they take steps to minimise the risk of unauthorised access to the Library's systems or unauthorised use or disclosure of the data held by the Library.

This BYOD Policy and associated procedures have been informed by the NSW Government Mobility Solutions Framework. The Framework assists NSW Government agencies to define their agency specific mobility strategy and approach.

2. Policy statement

This policy and associated BYOD procedures set out the terms of use for BYOD within the Library. It affects any device or accompanying media that staff may use to access the systems and data of the library, whether they are used within or outside the standard working hours.

This Policy applies to all Library staff (see definition in Section 4 below) and must be read in conjunction with the BYOD procedures and other Library's policies and the Code of Conduct.

3. Legislative and Policy Framework

This policy supplements the Library's *Information and Technology Services Policy*.

You should also have regard to the following statutory rules, policy documents and standards. They provide direct or related guidance for the use of technology and the collection, storage, access, use and disclosure of data by NSW public sector agencies:

Most relevant legislation

- *Copyright Act 1968 (Cth)*
- *Crimes Act 1900*
- *Crimes Act 1914 (Cth)*
- *Electronic Transactions Act 2000*
- *Email Policy*
- *Evidence Act 1995*
- *Government Information (Public Access) Act 2009*
- *Government Sector Employment Act 2013*
- *Health Records and Information Privacy Act 2002*
- *Library Act 1939*
- *Library Regulation 2010*
- *Privacy and Personal Information Protection Act 1998*
- *Public Finance and Audit Act 1983*
- *Public Interest Disclosures Act 1994*
- *State Records Act 1998*
- *Workplace Surveillance Act 2005*

Related and/or most relevant State Library and government policies

- *AS/NZS ISO 31000 Risk management - Principles and guidelines*
- *AS/NZS ISO/IEC 27000:2013 Information Technology – Security techniques – Code of practice for information security management 2013*
- *Code of Conduct*
- *Electronic Document Management Policy*
- *Information and Communications Technology (ICT) Services Policy*
- *M2012-15 Digital Information Security Policy*
- *Mobile Technology Usage Policy*
- *NSW Government Cloud Services Policy and Guidelines*
- *NSW Government ICT Strategy*
- *NSW Government Mobility Solutions Framework 2013*
- *NSW Government BYOD Devices Policy 2013*
- *NSW Government Open Data Policy*
- *NSW Government Social Media Policy and Guidelines*
- *NSW Procurement: Small and Medium Enterprises Policy Framework*
- *Password Policy*

- *Privacy Management Plan*
- *Records Management Policy*
- *Remote Access Policy*

4. Sector Definitions and acronyms

- ***Account*** - Telecommunication services provider billing account.

- ***Application*** – Computer software designed to assist end users to carry out useful tasks. Examples of applications may include the Microsoft Office suite of products or smartphone applications such as Google Maps.

- ***Bring Your Own Device (BYOD)*** - Any electronic device owned, leased or operated by an employee or contractor of the Library which is capable of storing data and connecting to a network, including but not limited to mobile phones, smartphones, tablets, laptops, personal computers and netbooks.

- ***Data*** - Any and all information stored or processed through a BYOD. Library's data refers to data owned, originating from or processed by the Library's systems.

- ***Device hygiene*** - BYOD must have appropriate and up-to-date 'hygiene' solutions installed. Device hygiene includes anti-virus, anti-spam and anti-spyware solutions.

- ***Minimum requirements*** - The minimum hardware, software and general operating requirements for a BYOD.

- ***Mobile Device Management (MDM)*** – Solution which manages, supports, secures and monitors mobile devices.

- ***Wipe*** – A security feature that renders the data stored on a device inaccessible. Wiping may be performed locally, via an MDM product, or remotely by a network administrator

- ***Staff*** - all staff on the State Library payroll and all contractors, consultants, members of the Library Council of NSW, volunteers, State Library scholars and fellows.

5. Responsibilities

- The Director, Digital Library Services and CIO is responsible for:
    - ownership of the policy
    - assessing and acting on serious breaches of the policy requiring suspension and termination of access
    - tabling serious breaches of this policy to the Executive Committee

- The Executive Committee is accountable for:
    - leading the implementation of this policy including its conformity to legislative and other compliance requirements, especially those relating to the security of corporate information and protection of personal information
    - ensuring this policy is communicated effectively to managers, supervisors and coordinators
    - Reviewing serious breaches of the policy ensuring that the policy is reviewed every two years.

- Manager, ICT Services is responsible for:
    - implementing procedures to ensure auditing of ICT infrastructure and systems security complies with this policy and other Library and ICT policies
    - Ensuring breaches are escalated to the Director, Digital Library Services and CIO promptly for assessment and possible further action.

- Division Directors are responsible for:
    - ensuring there is ongoing and effective communication of this policy to all staff
    - ensuring all reports of breaches of the policy are raised as soon as possible with the ICT Service Desk.

- Managers and supervisors are accountable for:
    - ensuring there is ongoing and effective communication of this policy to all staff
    - ensuring all reports of breaches of the policy are raised as soon as possible with their Executive member
    - ensuring the Privacy Contact Officer is informed of any breach of privacy
    - ensuring feedback on the implementation of the policy is communicated to the ICT Service Desk.

- ICT Services Branch staff are accountable for:
    - ensuring the policy is followed when working with:
        - personal user account creation and deletion
        - restricted group account creation and deletion.
    - ensuring the policy is followed when assisting State Library staff accessing the internal network and ICT services
    - revalidating ICT network and systems access privileges for State Library staff and third-party vendors on a yearly basis.

- The Privacy Contact Officer is responsible for:
    - managing privacy issues and applications for internal review, which may result from a breach of this policy, in accordance with the State Library's Privacy Management Plan.

- State Library staff are responsible for:
    - understanding and complying with this policy
    - ensuring that records created as a result of compliance with this policy are managed in accordance with the Records Management Policy.

6. BYOD Procedures

Staff must review and accept *BYOD Policy* with associated procedures before using their own mobile devices to access the Library's internal systems. The agreement to the requirements of this policy is indicated by staff signature/acceptance of the *BYOD Acceptance Form (BYOD Procedures - Appendix B).*

7. Privacy

The State Library is required to comply with the *Privacy and Personal Information Protection Act 1998* (NSW) and the *Health Records and Information Privacy Act 2002* (NSW) both of which contain Principles that the Library must abide by when it collects, stores, uses and discloses personal or health information.

Reasonable steps must be taken to ensure the security of personal, health or sensitive information against loss, unauthorised access, modification or other misuse.

It is the responsibility of all users to understand and comply with the Privacy Principles within each Act and the State Library's Privacy Management Plan.

8. Recordkeeping

The State Library is required to comply with the *State Records Act 1998* including Standards and Disposal Authorities issued under the Act.

Corporate records, and the information they contain, must be protected appropriately according to their importance and sensitivity. Corporate records created or received on your device must be registered in the recordkeeping system TRIM.

It is the responsibility of all users to understand and comply with the State Library's Records Management Policy, Electronic Document Management Policy, Email Policy and associated procedures.

9. BYOD Policy Breaches

Compliance or policy breaches are to be reported to the Director, Digital Library Services and CIO in the first instance for assessment and appropriate action, which may include suspension or termination of access.

Appeals to any suspension or termination of access decision may be lodged in writing to the NSW State Librarian and Chief Executive for review and consideration.

The Director, Digital Library Services and CIO will report serious breaches requiring suspension or termination of access to the Executive Committees.

10. Approval

This policy was approved by the Executive Committee on **07 October 2014**.

11. Implementation

This policy is implemented on **31 October 2014**.

12. History

N/A

13. Prepared by:

Manager, ICT Services, Digital Library Services
30 September 2014

14. Document History and Version Control

Version	Date approved	Approved by	Brief description
1.0	07 October 2014	Executive	First Release