Information and Communications Technology (ICT) Acceptable Use Policy

Item	*Description*
Policy description	*Set of rules outlining how Legal Aid NSW information assets and systems connected to Legal Aid NSW networks must be utilised.*
Division	*Information and Communications Technology*
Director	*Wayne Gale*
Contact	*Service Desk*
Date approved	*1 April 2014, 1 May 2017*
Next review	*12 April 2018*
Key words	*AUP, Security, Acceptable Use, Password, Network, Mobile Devices, Information and Communications Technology*

Revision History

Date	*Version*	*Reviewed by*	*Changes made*
1 April 2014	1.0	Wayne Gale	First version approved
26 June 2015	1.0a	Danilo Bernardo	Media, equipment and new division
12 April, 2017	1.0b	Ashish Dahiya	Added user signature page
Date closed	*[to be filled in when document is closed or superseded]*		

Printed copies of this document may not be up to date. Ensure you have the latest version before using this document.

Table of Contents

Policy overview

Scope and purpose of this policy

This Information and Communications Technology (ICT) Acceptable Use Policy is intended to establish a culture of openness, trust and integrity by protecting Legal Aid NSW information systems, assets and resources from intentional or unintentional damage.

This policy applies to the use of all Legal Aid NSW information systems, assets and resources where such use is undertaken through the Legal Aid NSW network services and/or devices as well as personal devices used in conjunction with Legal Aid NSW network services, regardless of the location from where they are accessed.

Although this policy provides a single point of reference for acceptable use of Legal Aid NSW information systems, staff need to be aware of and understand all Legal Aid NSW policies including those listed in the associated documents section below and any future polices that may be introduced.

Applicability and target groups

This policy applies to all ongoing, temporary and casual employees, contractor staff and vendors engaged by Legal Aid NSW (collectively referred to as 'staff'). Managers should ensure that all relevant staff members know about this policy and how to apply it. If anything in this policy is unclear, or you are unsure about how to apply the policy, contact the Service Desk.

Compliance

It is the responsibility of all staff members who access Legal Aid NSW information systems and assets to comply with this policy.

Deliberate breach or circumvention of Legal Aid NSW policies may result in the organisation undertaking a disciplinary investigation and appropriate remedial or disciplinary action in line with the *Government Sector Employment Act 2013 (NSW)*.

Legislative environment

This policy complies with the requirements of;

- Sections 12 and 17(1) of the *Workplace Surveillance Act 2005 (NSW)* requiring employers to notify employees of surveillance
- *Government Sector Employment Act 2013 (NSW)*.
- *OFS-2015-05-NSW Government (DISP) Digital Information Security Policy*

Definitions and abbreviations

Term	Definition
Email	Electronic mail service provided by Legal Aid NSW for the use of staff in the form of an email account and Legal Aid NSW email address (*@legalaid.nsw.gov.au). Includes all messages sent, received and stored using this email account including attachments.
Encryption	The modification of data in such a way that only authorised parties can access.
ICT	Information Communications Technology.
Information, Information Assets	Documents and papers; electronic data; software or systems and networks on which information is stored, processed or communicated, intellectual information acquired by individuals and physical items from which information regarding design, components or use could be derived.
Internet	All references to the internet in this policy should be taken to include all online services including but not limited to the World Wide Web (WWW), email, newsgroups, chat groups, message boards, social media services and file transfer protocol (FTP).
Mobile Devices	Tablet Computers (e.g. iPads), Laptop Computers, Smartphones (e.g. iPhones) and similar devices.
Remote Access	The ability to connect to a system from a remote location. E.g. through a virtual private network (VPN).
Social Media	Forms of electronic communication that are used by large groups of people to share information and to develop social and professional contacts or networks. E.g. LinkedIn, Facebook, Twitter.
Streaming	A technique for the electronic transfer of data, typically to listen to audio or watch video files.
Sensitive Information	Sensitive information may cause limited damage to national security, Australian/NSW Government agencies, commercial entities and members of the public. Sensitive information may contain personal details including, but not limited to first name, last name, address, individuals racial origin, health & Medicare information, political opinion, biometric data, criminal records, and information that may be subject to legal professional privilege.

Security Classified Information	Security classified information has the potential to cause damage to national security, Australian/NSW Government agencies, commercial entities and members of the public. Security classification applies to information subject to the National Security Information (Criminal & Civil Proceedings) Act 2004 and Sensitive Commonwealth Government Cabinet Documents. **Legal Aid NSW will very rarely handle security classified information.**

Monitoring, evaluation and review

This document is to be reviewed every 12 months. The last review was 12 April 2017. See cover page of this policy for more information about changes to the policy since its release.

Further information, additional resources & associated documents

These Legal Aid NSW additional documents should be read, understood and complied with by all staff.

- Legal Aid NSW – Information Security Policies Manual
- Legal Aid NSW – Policy on Use of Internet and Email
- Legal Aid NSW – Policy on Allocation of IT Equipment
- Legal Aid NSW – Social Media Policy
- Legal Aid NSW – Mobile Devices Policy
- Legal Aid NSW – Remote Access Policy
- Legal Aid NSW – Security Token Policy
- Legal Aid NSW – Password Policy
- Legal Aid NSW – Records Management Procedures
- Legal Aid NSW – Media Policy and Protocols

1. Information management and handling

Staff must be mindful of the security requirements of information systems and assets they use at all times. Reasonable precautions must be taken by staff to safeguard information systems and assets against inappropriate or unauthorised access. In particular:

- Legal Aid NSW information systems and assets must be used primarily for business purposes, in line with this policy, the Information Security Policies Manual and any other related agreements/contracts.
- Staff must comply with the non-disclosure provisions under sections 25 and 26 of the *Legal Aid Commission Act 1979*.
- Staff must also adhere to the requirements of the Legal Aid NSW – Privacy Management Plan in relation to the collection, storage, access, accuracy, use and disclosure of personal information and health information.
- Staff must only access Sensitive or Security Classified information when there is a valid business requirement to do so.

Without limiting the generality of the above, staff must also observe the following specific requirements:

JusticeLink Data

- Staff must adhere to their Legal Aid NSW obligations when accessing and using JusticeLink data
- Staff can only access and use information on JusticeLink when there is a business requirement to do so
- This means the information must:
    - relate to proceedings of a Legal Aid NSW applicant or client and
    - be required to perform your work duties
- There is a specific exemption in relation to Family Dispute Resolution matters, where third parties may be considered to be clients.

Centrelink Data

- Staff accessing Centrelink data must ensure that the client has consented to Legal Aid NSW accessing their Centrelink data
- The information must be accessed only for work duties and must not be disclosed to third parties without the client's consent
- The Centrelink CRN or customer identifier must not be disclosed.

ATLAS and CASES

- Information barriers exist in ATLAS and CASES to safeguard information and to ensure that conflict of interest is minimised
- Staff must comply with Legal Aid NSW policies including the *Legal Aid Commission Act 1979* (*NSW*) and conflict of interest guidelines.

Unless stated otherwise by separate agreement, ownership of all information systems, client data and assets is held by Legal Aid NSW.

All Sensitive and Security Classified material must be disposed of securely.

Destruction of Legal Aid NSW records, other than Ephemeral, Facilitative or Duplicate Records with no value to Legal Aid NSW, is to occur only with prior formal approval within appropriate

delegation, and using approved disposal authorities and in accordance with Chapter 8 Managing Records Destruction of the Records Management Procedure.

2. Intellectual property

Intellectual property ("IP") rights protect intellectual or creative effort and may relate to copyright, licenses, trademarks, domain names, social media accounts, designs, patents, software configurations, trade secrets or sensitive or security classified information.

All IP rights held by Legal Aid NSW are assets of Legal Aid NSW and the NSW government.

Some principles for dealing with our IP are as follows:

- Legal Aid NSW allows non-commercial use of its IP by other parties, subject to attribution of the source (examples are Legal Aid NSW publications, training resources and website content) and these may be disclosed by staff;
- Staff should not disclose all other information without approval where such disclosure may be in breach of Legal Aid NSW IP rights (examples are business processes and systems);
- Staff must also take care not to breach the IP rights of third parties or cause Legal Aid NSW to be in breach (examples are advices or systems provided by consultants or vendors).

If staff have any queries regarding Intellectual Property, they should seek guidance from the Legal Policy Branch.

3. Media and equipment

All staff are personally accountable in their use of Legal Aid NSW resources and are responsible for the equipment assigned to them individually or to their position as outlined in the Policy on Allocation of IT Equipment. In particular:

- Staff must report all lost or stolen equipment (including approved 'bring your own' or personally owned devices used to access Legal Aid NSW information services) to their immediate manager and the Service Desk.
- Staff must not modify the security controls and settings on Legal Aid NSW computer equipment or devices e.g. remove or disable anti-virus software.
- Staff must not download, install or use software on Legal Aid NSW computer equipment or devices that has not been licensed by Legal Aid NSW.
- Staff must not connect unauthorised devices or equipment to Legal Aid NSW internal networks, for example, non-departmental laptops, routers, wireless access points etc.
- Staff are also responsible for protecting information originating from external sources such as documents, police briefs, CCTV footage and other case related material which is in their custody.

Staff must adhere to the following requirements when using removable media such as USB sticks, portable disc drives, DVD ROMs etc.:

- Security Classified Legal Aid NSW information must not be stored on removable media without prior authorisation from the CEO
- Any disks, removable media, CD-ROMs or other electronic media must be appropriately handled whilst stored or transferred to premises outside Legal Aid NSW

- All Sensitive information must be encrypted prior to storage on removable media (Refer to 7-Zip Encryption Guide).
- Removable media containing Legal Aid NSW information which has been lost or stolen must be reported to the Service Desk.
- Removable media containing Legal Aid NSW information must be securely destroyed when such information is no longer required and not subject to retention in accordance with the Legal Aid NSW Records Management Procedure.

Legal Aid NSW IT systems must not be used to store personal movies, music, photos or other non-incidental data. Legal Aid NSW may, without notice or employee approval, investigate, replicate and/or remove any illegal or unacceptable material from its computing resources where clearly not related to work purposes.

4. Clear screen and desk

Staff must ensure that Sensitive or Security Classified information including hardcopy material is adequately secured when not in use.

Staff must lock their screens when away from their devices (desktop computers, laptops, tablets, phones etc.).

Staff using devices from remote locations (e.g. public transport, court rooms and interview rooms) should be aware of other unauthorised people viewing their device. Sensitive information must not be accessed on the device when viewable by unauthorised persons.

Unattended remote access sessions using Citrix remote access must be locked to prevent unauthorised access. Locking the desktop/laptop only is not sufficient, remote access session must be locked – select in the remote access session from the Start button --> Log off --> Lock.

5. User access

Access to Legal Aid NSW information systems and assets is restricted through user identification and authentication controls. Each user will be uniquely identifiable to ensure accountability for activities.

Access privileges to information systems and assets are granted to staff on a 'need-to-know' basis, so that the nature and scope of access is based on job functions and responsibilities. Staff must not:

- attempt to access systems for which they are not authorised
- share or let others use their unique usernames
- disclose passwords to anyone (even in periods of absence).

6. Passwords

All staff are responsible for ensuring that passwords used to access Legal Aid NSW information assets, systems and networks align to the requirements of the Legal Aid NSW Password Policy.

Staff must:

- maintain the confidentiality of their password at all times
- change their password if they know or suspect that their password has been compromised
- use different passwords to access Legal Aid NSW systems to those used to access personal services such as email, internet banking or social media sites.

Staff must not:

- include passwords in any automated log-on process, e.g. stored in a macro or function key
- base passwords on anything another individual could easily guess or obtain using personal related information, e.g. names, telephone numbers, dates of birth, etc.
- Share passwords with anyone
- Write down passwords or store them in a file on local computer
- Write passwords on the white board or Post It

User passwords must meet the following complexity requirements:

- Minimum 6 characters in length
- Contain characters from at least three of the four following categories:
    - English uppercase characters (A through Z)
    - English lowercase characters (a through z)
    - Numerals (0 through 9)
    - Non-alphanumeric characters (e.g. *, $, %, @, &).

7. Internet and electronic communication

Email and electronic communication must adhere to the Legal Aid NSW Policy on Use of Internet and Email.

Reasonable personal use of information systems such as internet and email is permitted when a staff member is off duty (i.e. during their lunch break, and at the beginning and end of the day provided they are not claiming this time on their flex sheet). Only incidental and necessary personal use is permitted when a staff member is on duty (i.e. during core hours and at any other time that is claimed on their flex sheet).

Email and Electronic Communication

Staff must not attempt to bypass, circumvent or otherwise negate any controls that Legal Aid NSW may implement in support of the secure and effective operation of its email and electronic communication services.

Staff are prohibited from:

- Installing unauthorised email software on Legal Aid NSW computers
- Automatic forwarding of email to external email accounts
- Transmitting Legal Aid NSW information to their personal email accounts
- Using their Legal Aid NSW email address for the purpose of subscribing to mailing lists except in relation to work or professional development purposes

- Using a private email account as an alternative to their Legal Aid NSW email account for sending or receiving any Legal Aid NSW official communication relating to Legal Aid NSW business activities.

Staff must not use another staff member's email account to send email messages unless given explicit permission to do so through to use of Outlook permissions.

When engaging in online communication, including the use of social networking sites in business and personal capacity, staff:

- Are expected to uphold the values, obligations and expectations of staff outlined in the Code of Conduct
- Should ensure that comments relating to personal views do not imply endorsement by Legal Aid NSW.
- Should be careful not to divulge Sensitive or Security Classified Legal Aid NSW information
- Should ensure personal information, including photographs, are not published without permission.

Internet Usage

The use of the internet or email to make or send fraudulent, unlawful, offensive or abusive information or messages is prohibited. Staff are to report receipt of any such messages to their immediate manager.

Material which is considered to be inappropriate or unsuitable must only be accessed by Legal Aid NSW staff when there is a business requirement to do so, such as part of case management activities, through the formal request process (Procedure – Requesting Access to Blocked Internet Sites).

In addition to the above, the following activities are not permitted using internet and email services provided by Legal Aid NSW. Staff must not:

- Intentionally access, create, transmit, distribute, or store any offensive information, data or material that violates Australian or State regulations or laws. Legal Aid NSW reserves the right to audit and remove any illegal material from its computers without notice.
- Undertake any form of computer hacking (illegally accessing other computers).
- Use the internet or email for activities that might be questionable, controversial or offensive, such as gambling, gaming, accessing chat lines, transmitting inappropriate jokes or sending junk programs.
- Intentionally transmit copyright-protected material which subsisting intellectual property rights exist without the written permission of the owner.
- Use any online third-party storage service (e.g. cloud storage facilities such as iCloud, Google Docs, OneDrive/SkyDrive and Dropbox) for the permanent or temporary storage or transfer of any Legal Aid NSW information unless prior written approval is provided by the Director ICT.
- Illegally download, stream or upload copyright protected content such as videos, music and other data.
- Staff must not download and install program files (i.e. executable software). Employees requiring access to additional software must complete the appropriate form and forward it to the Service Desk. This process must be followed regardless of the licence type of the software (e.g. free trial, freeware, etc.).

Monitoring

Staff using Legal Aid NSW information systems and assets for internet and electronic communications are monitored at all times.

Employee use of information systems and networks constitutes consent to:

- Monitoring of the systems owned by Legal Aid NSW
- Legal Aid NSW management right of access to information gathered from monitoring
- Disciplinary action against staff members who use Legal Aid NSW information systems and assets in a manner which contravenes policies.

8. Social Media

Staff must abide by the Legal Aid NSW Social Media Policy, including but not limited to:

- Following the staff policies of Legal Aid NSW including the Code of Conduct and Policy on use of Internet and Email
- Acting lawfully when using social media
- Making sure personal online activities do not interfere with job performance
- Making it clear that personal views expressed are your own and not the views of Legal Aid NSW
- Not disclosing Sensitive or Security Classified information obtained through work
- Exercising sound judgement when distributing messages or posting content on third party sites such as LinkedIn, Twitter, Facebook, Myspace, Flickr and more.

Staff who wish to engage in social media on behalf of Legal Aid NSW must first obtain prior approval from the Executive Unit with approvals required from relevant Directors and the CEO.

With appropriate approval, the creation of social media accounts on behalf of Legal Aid NSW should be done with a Legal Aid NSW email address and shall be under the ownership of Legal Aid NSW.

9. Incident Reporting

Staff must report information security incidents, breaches and weaknesses to their manager and the Legal Aid NSW Service Desk in a timely manner.

Information security incidents may include but are not limited to:

- Suspicion that a user account has been used by someone else
- Unauthorised access to a secure area by a third party
- Breach of confidentiality, misuse of Legal Aid NSW Information Assets
- Suspicious approach or persuasion to disclose passwords or other sensitive information
- Loss or theft of portal media or physical documentation
- Illegal material accessed or stored on Legal Aid NSW IT resources
- Computer virus or malware
- Misaddressed emails or communication containing sensitive information
- Unauthorised changes to Legal Aid NSW Information Assets.

Staff must report lost or stolen computing devices including personally owned devices accessing Legal Aid NSW information services to the Legal Aid NSW Service Desk immediately.

Contact

Please contact the service desk if you have any further questions.

Service Desk

Email: servicedesk@legalaid.nsw.gov.au

Phone: 9219 5988

10. Acknowledgement Agreement

Please sign below in acknowledgement of your understanding of, and agreement with the above policy and guidelines.

Name: _____

Position Title _____

Signature: _____ **Date:** _____

Name of Manager: _____

Position Title: _____

Signature: _____ **Date:** _____