Identification

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title:</td>
<td>ICT Acceptable Use Policy (Juvenile Justice NSW)</td>
</tr>
<tr>
<td>Document No:</td>
<td>D14/361784</td>
</tr>
<tr>
<td>Business Centre:</td>
<td>Information Technology Services</td>
</tr>
<tr>
<td>Governance Area:</td>
<td>Service Strategy</td>
</tr>
<tr>
<td>Process:</td>
<td>Policy Management</td>
</tr>
<tr>
<td>Owner:</td>
<td>Chief Executive, Juvenile Justice NSW</td>
</tr>
<tr>
<td>Date of Effect:</td>
<td>30 July 2014</td>
</tr>
<tr>
<td>Contact:</td>
<td>Manager, Information Security</td>
</tr>
<tr>
<td>Next Review:</td>
<td>Feb 2016</td>
</tr>
<tr>
<td>Classification:</td>
<td>Unclassified</td>
</tr>
</tbody>
</table>

Acceptance

<table>
<thead>
<tr>
<th>Role</th>
<th>Name</th>
<th>Signature</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>ITS Governance:</td>
<td>Joy Gault</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Document Owner:</td>
<td>Valda Rusis</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Review by</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>23 July 14</td>
<td>Derek Winter</td>
<td>Minor amendments</td>
</tr>
<tr>
<td>16 July 14</td>
<td>Satoshi Yasuda</td>
<td>Draft from JJ ECD Policy</td>
</tr>
</tbody>
</table>

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

1. Objective 3
2. Scope 3
3. General Requirements 4
   3.1 Principles 4
   3.2 Protecting Information Confidentiality 5
   3.3 Corporate Records 5
   3.4 Access to Information 6
   3.5 Personal Use 6
   3.6 Monitoring and Surveillance 6
   3.7 Email Filtering and Quarantine 7
   3.8 Clients’ Use of Agency ICT Services 7
4. Acceptable Use 8
   4.1 Email Use 8
   4.2 Internet Access 9
   4.3 Telephones 9
   4.4 Mobile phones 10
   4.5 Fax machines 11
5. Compliance 11
6. Reporting breach / inappropriate use 12
1. Objective

Juvenile Justice (the Agency) employees must be efficient, economical and ethical in their use and management of public resources. Information and Communication Technology (ICT) services including PCs, telephony, electronic mail (email), and Internet access are provided for business purposes. All employees, including contractors, have a responsibility to ensure their proper use of these services.

The purpose of this policy is to:

- Increase awareness of restrictions on the use of the Agency’s ICT services
- Detail what is considered acceptable use and the consequences of breaches
- Identify the process for reporting policy breaches and/or inappropriate use
- Improve productivity through efficient and responsible behaviour

This policy should be ready in conjunction with the Agency’s Code of Conduct, Dignity and Respect Policy and Guidelines and the Department of Justice’s Information Security Policy.

2. Scope

This policy applies to all permanent, temporary and contract employees of Juvenile Justice, NSW.

The policy is principally concerned with the use of the ICT services and devices listed below. However, the principles contained in this policy, are equally applicable to any other facilities, technology, application systems and data provided by the Agency for business use:

- Computers (PCs, laptops, tablet devices etc.)
- Telephony services, including fax machines
- Email and Internet services
- Mobile phones / smartphones
3. General Requirements

3.1 Principles

The use of the Agency’s ICT services must be:

- Economical and efficient
- Ethical
- Professional in line with the Agency’s business purposes and goals
- Responsible
- In accordance with Australian and NSW laws, Regulations and Acts

Employees should refer to the following Agency and departmental policies and guidelines in regards to acceptable use and expected behaviours:

- Code of Conduct
- Dignity and Respect Policy and Guidelines
- Department of Justice Information Security Policy

The Agency’s information systems must not be used to create, distribute, access or store information or data in a manner that:

- Is detrimental to the reputation of the Agency
- May reasonably be found to be offensive, obscene, threatening, abusive or defamatory
- May result in unlawful victimisation, discrimination, harassment or vilification
- Is deliberately misleading or deceptive
- May result in criminal penalty or civil liability
- Is in conflict with the Agency’s commitment to the community

All employees are responsible for reading and complying with requirements set out in the Department’s Information Security Policy. Employees should give particular attention to the following sections of the policy:

4. Principles
5. Compliance
6. Security roles and responsibilities
7.2 Acceptable use of assets
11.2.2 Password management

Nothing in this policy over-rides the rights of accredited union delegates to use the Agency’s ICT services and electronic communication devices in accordance with the conditions contained in properly constituted industrial instruments or other legislation.
The Agency reserves the right to audit and remove any illegal material from its computer resources without notice. Any identified use of ICT equipment or services that are considered to be inconsistent with the Agency’s policies will be investigated. Inappropriate use may result in the Agency initiating disciplinary action in accordance with the Government Sector Employment (GSE) Act 2013 and GSE Rules 2014.

3.2 Protecting Information Confidentiality

Employees must comply with the Agency’s information classification and labelling policies and guidance on information protection.

Emails that are sent to external addresses are delivered over public networks (the Internet) and may be subject to unauthorised interception, copying or modification en route to the intended recipient. As a consequence, careful consideration should be given before emailing commercial or confidential information to external parties. Employees should also be alert to the risk that other electronic communications, such as phone calls, may be subject to unauthorised or illegal interception, tracing or recording.

Particular care must be taken to ensure that passwords or personal identity numbers (PIN) protection are used to prevent unauthorised access to mobile devices (e.g. mobile telephones, laptop computers and tablet PCs). Further information is available from Records Management and ITS Security.

3.3 Corporate Records

Employees should be aware of the need to preserve electronic records of business communications and care should be taken before deleting any electronic business communication. It is important to remember that business communications sent electronically become official records subject to the same standards of record keeping that apply to paper records. They can be subpoenaed or “discovered” during legal processes.

These records must be readily accessible to meet business and accountability requirements and be capable of being downloaded or stored in hard copy with other paper based file records. If the record has administrative, legal, research, evidential or financial/accounting value, it should be printed and filed.
3.4 Access to Information

Access to the Agency’s information is restricted to authorised users through the use of individually assigned user-ids and passwords. Employees are accountable for their access to and use of the Agency’s information and systems and must ensure that their passwords are kept secret at all times.

3.5 Personal Use

The NSW Government is committed to the development of a responsive and flexible public sector, and acknowledges that family and community responsibilities impact on work. The Agency accepts that on occasion its ICT services and associated electronic communication devices may need to be used for personal reasons. Such use should be infrequent and brief, and should not involve activities that might be questionable, controversial or offensive. This includes gambling, accessing chat lines, transmitting inappropriate jokes, and sending junk programs or mail.

Personal use does not extend to the sending of non-business related written material to any political organisation.

Personal use of the Agency’s ICT services and communication devices is not considered private, and employees do not have the same personal privacy rights as they would have when using non-agency devices or services.

3.6 Monitoring and Surveillance

The Workplace Surveillance Act 2005 governs the monitoring and surveillance of email, Internet and computer use and requires that employees are notified of monitoring and surveillance activity.

The Agency may monitor, copy, access or disclose any information or files that are stored, processed or transmitted using agency equipment and services. The Agency may monitor on a random or continuous basis to:

- Identify or prevent the download, installation or use of unauthorised software
- Ensure compliance with the Agency’s policies
- Investigate conduct that may be illegal or adversely affect the Agency or its employees
- Prevent inappropriate or excessive personal use of the Agency’s resources.
At the point of login to the Agency’s network, employees are required to acknowledge an ‘Acceptable use of Internet/Email/Computer’ statement by clicking ‘Yes’ (refer below).

3.7 Email Filtering and Quarantine

The Agency has applied an email filtering system including anti-virus, anti-spam and contents control. Emails with prohibited attachments are intercepted by this email filter system and the user will be notified. As per the Act, notifications will not be sent for emails that are believed to be spam (as defined by the Spam Act 2003 of the Commonwealth), or believed to contain viruses, other malware, or offensive and harassing material.

3.8 Clients’ Use of Agency ICT Services

Clients are not permitted to use the Agency’s Internet or email services.

Clients must only use the Agency’s phones under close supervision or under the control of the monitoring system or equivalent (refer to the Operation Manual for further details).
4. Acceptable Use

4.1 Email Use

1. Avoid sending large attachment to a large group of recipients.

2. Email is not an appropriate form to seek a formal approval requiring a written signature for an intended course of action.

3. Do not forward junk email or chain letters.

4. Email is not considered as an official record management system. Archive email document with the Agency’s Record Management System.

5. Add an official styled signature to your email.

6. Consider using Blind Carbon Copy (BCC) when sending an email to a large group of people to protect the privacy of recipients.

7. Broadcast messages (group email to all Agency users) are used for announcements and notifications.

   The ability to send broadcast messages is limited to Office of Chief Executive, Policy and Government Relations, and IM&T business managers. Broadcast messages sent to limited group such as Regions, Centres or Central Office staff only may be sent at the discretion of senior executives (e.g. Regional Directors, Centre Managers, CO Directors etc.).

8. Do not open spam emails – simply delete them.

9. Do not click any link in spam emails.


11. Never call a telephone number found in a spam email.

12. Never reply to a spam email (even to unsubscribe).

13. When in doubt, always try to access an organisation via an official channel (via company’s official telephone number or website etc.) rather than clicking links or URLs in a spam email message.

14. Open email attachments only if you know the sender and you are expecting it.

15. Do not use your Agency email address to subscribe to or access fee based services for personal use. Emails sent by these services may be automatically blocked as spam.
16. Do not expect email delivery to be instant. Delays or non-delivery of email may be the result of a system failure, incorrect addressing, blocking by the Agency based on content or email size, or blocking by the recipient organisation.

17. The Agency’s email traffic and its contents are monitored, logged and archived. Email records are owned by the Agency and subject to investigation by the HR Professional Standards Branch upon receipt of an authorised request by a supervisor or line manager.

4.2 Internet Access

1. The Agency’s employees have access to a limited number of pre-approved Internet sites. Additional access may be requested using and IT Request form and must be approved via Category 3 delegation.

2. In limited circumstances, a special level of Internet access may be approved by a Category 1A delegation with support from a Category 3 delegated officer.

3. Employees must not download unauthorised software, games, large files for example, image, music or video files, or access live broadcast media such as radio or television streams.

4. Caution must be exercised when entering into online purchasing arrangements on behalf of the Agency and prior authorisation must be obtained.

5. Employee use of the Internet use must be consistent with the Agency’s Code of Conduct, which also has guidance on reporting misuse of Agency resources.

6. Access to the Internet must be via officially approved mechanisms only.

7. Employee Internet access is subject to logging and periodic review and these records may be used in support of analysis and investigation.

8. Employees are required to report inappropriate use in their workplace to their supervisor, senior officer, HR Professional Standard Branch, ITS Service Hub or ITS Security.

4.3 Telephones

It is recognised that there may be occasions where employees may need to make short, personal telephone calls using the Agency’s telephones, both fixed lines and mobiles, in order to deal with urgent personal or domestic matters. (It should be
emphasised that calls to mobile telephone numbers are particularly expensive and that these should be kept to an absolute minimum). Wherever possible, non-urgent calls should be made during scheduled breaks or outside of the normal working day to ensure that they do not interfere with work requirements.

Equally, it is legitimate to receive personal calls about domestic matters and arrangements, and occasional, short, non-urgent calls can be received providing they do not interfere adversely with work requirements.

Use of the Agency’s telephones which is deemed to be excessive (i.e. outside of the limits defined above), defamatory, obscene or otherwise inappropriate is forbidden. Misuse may lead to disciplinary action being taken against the employee concerned.

Where the Agency has grounds to suspect inappropriate use of its telephones, it reserves the right to monitor the destination and length of out-going calls and the source and length of in-coming calls.

At no time are the Agency telephones to be used to make international calls, unless the person making the call has been authorised to access International Direct Dialling services by an appropriately delegated officer as defined in the Agency's Administrative, Financial and Human Resources Delegations Manual.

4.4 Mobile phones

Mobile telephones (including smartphones) are provided solely to assist with meeting the Agency's business objectives - these phones are not a perk of office or an entitlement. Mobile phones are typically provided to selected officers that are required to be on call, for use in emergencies, and for remaining in contact with key staff members when they are away from their usual place of work.

It is recognised that there may be some circumstances where a mobile phone may need to be used for other than a business purpose. Calls to an employee’s home would generally fall into this category. Employees who use mobile phones for private purposes must pay for such use.

Use of mobile phones in a manner that is deemed to be inappropriate, illegal or which has the potential to damage the Agency’s reputation may lead to disciplinary action and/or criminal proceedings being taken against the employee.
Employees should note that the use of a handle held mobile telephone while driving is an offence under the Motor Traffic Act and the Agency is not responsible for any fines incurred.

4.5 Fax machines

Facsimile correspondence should be handled with the normal courtesy, discretion and care afforded the Agency’s other electronic communications.

Employees receiving any material, which is offensive, obscene, threatening, intimidating or pornographic, or who observe any actual or perceived misuse of the Agency’s facsimile services should report the incident to their Manager.

Employees must be fully aware of the requirements of handling sensitive and security classified information over fax machines and must comply with the Agency’s information classification, labelling and protection policies and guidelines.

Please contact Records Management or ITS Security if assistance is required.

5. Compliance

The Agency prohibits inappropriate use of ICT services and employees will be held personally liable for all legal and financial consequences arising from their inappropriate use of these services.

Where potentially inappropriate use is identified, employees may be required to provide an explanation of their actions. If the conduct is deemed to be contrary to this policy formal disciplinary action may be initiated in accordance with the Government Sector Employment (GSE) Act 2013 and associated GSE Rules (2014).

Where inappropriate use is identified, the Agency may also:

- Notify the Independent Commission Against Corruption if there are reasonable grounds for believing the matter concerns corrupt conduct
- Notify the Police if it is reasonably believed a criminal offence has been committed.

If an alleged inappropriate use of the Internet or Email is notified as a protected disclosure, normal procedures for protected disclosures should be followed.
6. Reporting breach / inappropriate use

All employees have a responsibility to report breaches of this policy and/or inappropriate use. The following steps to be followed:

- Notify their supervisor or manager.
- Manager may contact ITS Service Hub for non-sensitive IT issues, or the HR Professional Standard Branch may be contacted directly if it is a matter of work behaviour / professional conduct.

Upon request from HR Professional Standard Branch, ITS Security may provide evidence such as email record data, email and internet logs and analysis reports etc. Confidentiality and the ‘need to know’ principle will apply throughout any investigation.

- For IT security matters, the ITS Security team can be contacted directly for advice.