

# ICT Acceptable Use Policy

## Purpose

The purpose of this policy is to set out the acceptable usage of the Ministry's ICT Assets required by all Users.

## Application and responsibilities

### Application

This policy will apply to:

- All Users of Ministry ICT Assets.
- Visitors to the Ministry who have authorised use of the Ministry's Wi-Fi network.
- All Ministry ICT Assets.

### Responsibilities

The following roles have specific responsibilities under this policy:

Role	Responsibilities
Delegated authorities	As set out in the <a href="#">Instrument of Delegation</a> .
Managers	<ul style="list-style-type: none"> <li>• Monitoring compliance with this policy.</li> <li>• Ensuring Service Requests are completed for all user access requirements including a 'Delete' Service Request when users leave the Ministry.</li> <li>• Confirming annually that this policy is complied with when completing the Audit and Risk control self-assessment survey.</li> <li>• Ensuring any security breaches are reported to SEC and Service Centre immediately.</li> </ul>
Users	<ul style="list-style-type: none"> <li>• Using Ministry ICT Assets across all networks in accordance with this policy.</li> <li>• Any use made of their Ministry User accounts, including unacceptable and unauthorised use.</li> <li>• Management of Public Work Areas and Apple ID or BlackBerry ID User accounts themselves by mobile device holders. The Ministry and <a href="#">Service Centre</a> will support the device and Secure Work Area.</li> <li>• Reporting of any ICT security breach or suspected breach, any potential risk to ICT security or misuse of the Ministry's ICT Assets to the User's manager and the <a href="#">Service Centre and SEC</a> immediately.</li> <li>• Reporting of any damaged, lost, stolen or compromised Ministry ICT Assets to the User's manager, <a href="#">Service Centre and SEC</a> immediately.</li> <li>• Familiarising themselves with this policy and the Ministry's <a href="#">ICT Acceptable Use Standard</a>.</li> </ul>

Approved: August 2017	Policy owner: Chief Information Officer
Next review: August 2018	Policy contact: Service Centre, IMD

Sponsor / Host of visiting Wi-Fi Users	<ul style="list-style-type: none"> <li>• Informing and ensuring visitors using the Ministry's Wi-Fi adhere to this policy and the ICT Acceptable Use Standard.</li> <li>• Only connecting to the Ministry's Wi-Fi if they have been authorised in accordance with the relevant policies and forms regarding mobile electronic devices</li> <li>• Disconnecting from the guest Wi-Fi outside Ministry conference/meeting rooms.</li> </ul>
--	---

## Context

The Ministry's ICT Assets are owned by the Ministry and provided to Users to carry out their day to day work. The information held on Ministry ICT Assets is a valuable resource vital to the Ministry's ability to carry out its work and protect New Zealand's knowledge at the appropriate security levels.

## Principles

The Ministry's ICT Assets will be used in accordance with the following principles:

- Ministry's ICT Assets are used in an acceptable, ethical and lawful way.
- Disruptions to Ministry information management services and activities are minimised.
- Ministry security is not jeopardised.
- Users must protect the integrity of the Ministry's ICT Assets and the information stored against loss, damage, disruption, unauthorised disclosure and misuse.
- All information transacted through a Ministry system is considered to be owned by or under custodianship of the Ministry.
- All access to and use of Ministry systems may be monitored, collected, and provided to relevant third parties, for information assurance purposes.

## Policy statements

### ICT Asset security and access

- The security of the Ministry's ICT Assets must be protected at all times.
- Users will only access the Ministry's ICT Assets, data or information, when they are authorised to do so and when they have a "Need to Access".
- Users will adhere to the Ministry's standards to ensure the security of Ministry ICT Assets.

### ICT Asset use

- The Ministry's ICT Assets must not be used for any illegal activity, commercial purposes, political purposes, misrepresentation or in a way that would contravene the Ministry Code of Conduct.
- Users will use the Ministry's ICT Assets in a way that minimises any impact on the functionality of the Ministry's systems and the access of other Users.
- Personal use of the Ministry's ICT Assets in accordance with the Ministry's culture and values is acknowledged within acceptable limits. Incidental personal use of the Ministry's ICT Assets in accordance with the Ministry's standards is acceptable.

## Exceptions management and consequences of policy breach or non-compliance

Any deviation from this policy must be approved in advance by the appropriate authority as defined in the Instrument of Delegation. If this is not specifically defined in the Instrument of Delegation, then the Deputy Chief Executive of the relevant division where the deviation is to occur must approve any deviation in advance. The deviation must be notified to the policy owner and sponsor, and the Divisional Manager, Audit and Risk.

Approved: August 2017	Policy owner: Chief Information Officer
Next review: August 2018	Policy contact: Service Centre, IMD

Unauthorised breaches of this policy may be viewed seriously by the Ministry as a breach of the Code of Conduct. The Code of Conduct states that “employees are expected to fully comply with Ministry policies in their work”. Depending on the circumstances, failure to comply with this policy may be a breach of the Code of Conduct and may result in disciplinary action, up to and including dismissal. Any such breaches should be notified to the policy owner and sponsor and the Divisional Manager, Audit and Risk.

## Related content

### Related Ministry standards, processes, procedures and guidelines

This policy is directly linked to the following **standards**, **processes** and **guidelines**:

#### **Standards:**

- [ICT Acceptable Use Standard](#)
- [Mobile Device Security Standards](#)
- [ICT Administrator Standard](#)

#### **Processes:**

- [Service support](#)
- [On-board and induct – new and existing staff](#)
- [Manage mobile devices](#)
- [Publish to digital media](#)
- [Audit mobile apps](#)

#### **Guidelines:**

- [Ministry Wi-Fi Guest Network Guidelines](#)

#### **Templates and forms:**

- [Wellington Wi-Fi Authorisation form](#)

### Other related Ministry documents

The following Ministry documents are also relevant/related to this policy:

- [Privacy Policy](#)
- [Security Policy](#)
- [Ministry Communications, Pay TV and Internet Policy](#)
- [Ministry HR Manual](#)
- [Ministry Code of Conduct](#)
- [Head Office Security Instructions](#)
- [Post Security Instructions](#)
- [Security Classifications Guidelines](#)
- [Instrument of Delegation](#)
- [Information Systems Security Policy](#)

### Relevant legislation and regulations

The Ministry must comply with the following legislation/regulations:

- [Human Rights Act 1993](#)
- [Privacy Act 1993](#)
- [Copyright Act 1994](#)
- [Trade Marks Act 2002](#)
- [Unsolicited Electronic Messages Act 2007](#)

Approved: August 2017	Policy owner: Chief Information Officer
Next review: August 2018	Policy contact: Service Centre, IMD

- [Films, Videos and Publications Act 1993](#)
- [Crimes Act 1961](#)
- [Public Records Act 2005](#)
- [Official Information Act 1982](#)
- [Electronic Transactions Act 2002](#)

### National standards

The Ministry must comply with the following relevant New Zealand government requirements, manuals and standards.




- [NZ Information Security Manual \(NZISM\)](#)
- [Protective Security Requirements \(PSR\)](#)
- [www.censorship.govt.nz](http://www.censorship.govt.nz)
- [Information and Records Management Standard](#)

### Related training

The Ministry provides the following training related to this policy:

- Induction Security Briefing
- IMD Induction Training (Wellington)
- IMD New Starter e-learning (Posts)
- Information Management Training (e-learning)

### Policy governance

<b>Document type</b>	Policy
<b>Classification</b>	Unclassified
<b>Special Access Requirements</b>	None
<b>Division</b>	IMD
<b>Sponsor</b>	Deputy Chief Executive P&O
<b>Policy owner</b>	Chief Information Officer, IMD
<b>Policy contact</b>	Service Centre, IMD
<b>Original publication</b>	September 2009
<b>Approved</b>	August 2017
<b>Next review</b>	November 2020
<b>Approval and peer review</b>	<p>[Embed emails providing evidence of approval and peer review]</p> <div style="display: flex; justify-content: space-around; align-items: flex-start;"> <div style="text-align: center;">  <p>Peer Review Email.msg</p> </div> <div style="text-align: center;">  <p>RE ICT Acceptable Use - Policy Owner Ap Standards - Sign-off</p> </div> <div style="text-align: center;">  <p>RE IMD Policy and Standards - Sign-off</p> </div> </div>

### Glossary and acronyms

Relevant terms relating to this policy can be found in the [glossary](#).

Approved: August 2017	Policy owner: Chief Information Officer
Next review: August 2018	Policy contact: Service Centre, IMD

<b>Term</b>	<b>Definition</b>
ICT	Information, Communication and Technology.
Information Systems (ICT)	All equipment, hardware, software, tools and utilities associated with information technology and the operation/delivery of information technology to the Ministry.
Ministry ICT Assets	All Ministry owned ICT assets including, but not limited to networks, hardware, firmware or software, and including production, test or development systems. Further examples of Ministry owned ICT assets include desktops (standalone or networked), laptops, mobile devices, servers, firewalls, networks, printers, MFDs, internet booths, applications, networks, telephony systems (including PABX and mobile phones) and any other equipment which processes data in the Ministry.
Need to Access	When there is a legitimate business requirement to access.
Public Work Area	A separate work area on some mobile devices for publically available information.
Secure Work Area	A secure work area on a mobile device that connects to the Ministry's network. This work area may hold information up to and including RESTRICTED.
User of Ministry ICT Assets	Anyone who is authorised to use, access or support the Ministry's ICT Assets. This includes Ministry staff (open tenure, fixed term and locally engaged), contractors, consultants and authorised staff from other agencies.

## Appendix: Policy improvements

**This section is not published.**

The following improvements have been identified that should be considered during future reviews.

<b>Section</b>	<b>Improvement description</b>	<b>Comments</b>
Roles and Responsibilities	Ideally the responsibilities would be summarised in the policy with the detailed responsibilities being held in the related standard	The Policy & Standard are 1:1 relationship. But people may not read both documents.
Roles and Responsibilities - Sponsor/Host of Visiting Wifi Users	Ideally this would link to the relevant authorisation forms. However, if there are a number of forms with various uses, we may need to refer to these generically and direct people to the Service Centre if they need help.	Staff at posts may not use the form as it was initially developed for use in Wellington.
Principles	Need to also review the login description to ensure it accords with the updated documents	

Approved: August 2017	Policy owner: Chief Information Officer
Next review: August 2018	Policy contact: Service Centre, IMD

Section	Improvement description	Comments
Mobile Device Security 'Policy' and Standard	We understand that these are currently owned by Security. Ideally they would be incorporated into the ICT Acceptable Use Policy and Standard and/or the ISSP as appropriate	

Approved: August 2017	Policy owner: Chief Information Officer
Next review: August 2018	Policy contact: Service Centre, IMD

## Appendix: Policy asset links

Any policy asset links indicated to, will display in the right-hand navigation on the Business Process Portal page in order to create useful links to the next level of content:

<b>Title</b>	<b>Link/URL</b> (active link or state 'within this document')	<b>Security classification</b>	<b>LES LAN extreme threat compatible</b> (Yes/No)	<b>Show on the right hand?</b> (Yes/No)
<b>Related Ministry standards, processes, procedures and guidelines</b>				
ICT Acceptable Use Standard	<a href="http://bportal/Policies/ICTAcceptableUse/Pages/ICT-Acceptable-Use-Standard.aspx">http://bportal/Policies/ICTAcceptableUse/Pages/ICT-Acceptable-Use-Standard.aspx</a>	Unclassified	n/a	Yes
Manage mobile devices	<a href="http://bportal/IMD/ManageMobileDevices/">http://bportal/IMD/ManageMobileDevices/</a>	Unclassified	n/a	Yes
Ministry Wi-Fi Guest Network Guidelines (Te Aka link)	<a href="http://teaka/homepagetabs/srv/IMD/Pages/MFAT-Guest-Wi-Fi.aspx">http://teaka/homepagetabs/srv/IMD/Pages/MFAT-Guest-Wi-Fi.aspx</a>	Unclassified	n/a	Yes
Mobile Device Security Standard	<a href="http://o-wln-gdm/Activities/PoliciesandProcedures/RiskManagement/Mobile%20device%20standards.docx">http://o-wln-gdm/Activities/PoliciesandProcedures/RiskManagement/Mobile%20device%20standards.docx</a>	In-confidence	n/a	Yes
On-board and induct – new and existing staff	<a href="http://bportal/HR/Onboardinductstaff/">http://bportal/HR/Onboardinductstaff/</a>	Unclassified	n/a	No
Publish to digital media	<a href="http://bportal/CMD/DesignPublishCommMaterials/PublishDigitalMedia/">http://bportal/CMD/DesignPublishCommMaterials/PublishDigitalMedia/</a>	Unclassified	n/a	No
Service support	<a href="http://bportal/IMD/ServiceSupport">http://bportal/IMD/ServiceSupport</a>	Unclassified	n/a	No
Audit mobile apps	<a href="http://bportal/IMD/AuditMobileApps">http://bportal/IMD/AuditMobileApps</a>	Unclassified	n/a	Yes
<b>Other related Ministry documents</b>				
Privacy Policy	<a href="http://bportal/AuditRisk/Pages/Privacy.aspx">http://bportal/AuditRisk/Pages/Privacy.aspx</a>	Unclassified	n/a	No
Security Policy	<a href="http://bportal/Policies/Security">http://bportal/Policies/Security</a>	Unclassified	n/a	No

Approved: August 2017	Policy owner: Chief Information Officer
Next review: August 2018	Policy contact: Service Centre, IMD

<b>Title</b>	<b>Link/URL</b> (active link or state 'within this document')	<b>Security classification</b>	<b>LES LAN extreme threat compatible</b> (Yes/No)	<b>Show on the right hand?</b> (Yes/No)
Ministry Communications, Pay TV and Internet Policy (Te Aka link)	<a href="http://teaka/CEO/HRS/publishing/Documents/2378366-v2-Communication%20Devices%20Pay%20TV%20and%20Internet%20Policy.doc">http://teaka/CEO/HRS/publishing/Documents/2378366-v2-Communication Devices Pay TV and Internet Policy.doc</a>	Unclassified	n/a	No
Approved mobile apps (Te Aka link)	<a href="http://teaka/homepagetabs/srv/IMD/Pages/Mobile-Apps.aspx">http://teaka/homepagetabs/srv/IMD/Pages/Mobile-Apps.aspx</a>	Unclassified	n/a	No
Ministry HR Manual (Te Aka link)	<a href="http://teaka/CEO/HRS/hrkiosk/Pages/HR-Resources-home.aspx">http://teaka/CEO/HRS/hrkiosk/Pages/HR-Resources-home.aspx</a>	Unclassified	n/a	No
Ministry Code of Conduct	<a href="http://o-wln-gdm/Activities/PoliciesandProcedures/layouts/DocIdRedir.aspx?ID=POLP-17-28">http://o-wln-gdm/Activities/PoliciesandProcedures/layouts/DocIdRedir.aspx?ID=POLP-17-28</a>	Unclassified	n/a	No
Head Office Security Instructions	<a href="http://o-wln-gdm/Activities/PoliciesandProcedures/RiskManagement/Head%20Office%20Security%20Instructions.docx">http://o-wln-gdm/Activities/PoliciesandProcedures/RiskManagement/Head%20Office%20Security%20Instructions.docx</a>	Unclassified	n/a	No
Post Security Instructions (Te Aka link)	<a href="http://teaka/homepagetabs/srv/SEC/Pages/Post%20Security%20Instructions.aspx">http://teaka/homepagetabs/srv/SEC/Pages/Post%20Security%20Instructions.aspx</a>	Unclassified	n/a	No
Security Classifications Guidelines	<a href="http://o-wln-gdm/Activities/ReferenceLibrary/InformationManagement/Visio-Security%20Classification%20definitions%20and%20examples.pdf">http://o-wln-gdm/Activities/ReferenceLibrary/InformationManagement/Visio-Security%20Classification%20definitions%20and%20examples.pdf</a>	Unclassified	n/a	No
Instrument of Delegation	<a href="http://bportal/FormsandTools/OtherContent/Instrument%20of%20Delegation.docx">http://bportal/FormsandTools/OtherContent/Instrument%20of%20Delegation.docx</a>	Unclassified	n/a	No
<b>Relevant legislation and regulations</b>				
Human Rights Act 1993	<a href="http://www.legislation.govt.nz/act/public/1993/0082/latest/DLM304212.html">http://www.legislation.govt.nz/act/public/1993/0082/latest/DLM304212.html</a>	n/a	n/a	Yes
Privacy Act 1993	<a href="http://www.legislation.govt.nz/act/public/1993/0028/latest/DLM296639.html">http://www.legislation.govt.nz/act/public/1993/0028/latest/DLM296639.html</a>	n/a	n/a	Yes

Approved: August 2017	Policy owner: Chief Information Officer
Next review: August 2018	Policy contact: Service Centre, IMD



<b>Title</b>	<b>Link/URL</b> (active link or state 'within this document')	<b>Security classification</b>	<b>LES LAN extreme threat compatible</b> (Yes/No)	<b>Show on the right hand?</b> (Yes/No)
Copyright Act 1994	<a href="http://www.legislation.govt.nz/act/public/1994/0143/latest/DLM345634.html">http://www.legislation.govt.nz/act/public/1994/0143/latest/DLM345634.html</a>	n/a	n/a	Yes
Trade Marks Act 2002	<a href="http://www.legislation.govt.nz/act/public/2002/0049/latest/DLM164240.html">http://www.legislation.govt.nz/act/public/2002/0049/latest/DLM164240.html</a>	n/a	n/a	Yes
Unsolicited Electronic Messages Act 2007	<a href="http://www.legislation.govt.nz/act/public/2007/0007/latest/DLM405134.html">http://www.legislation.govt.nz/act/public/2007/0007/latest/DLM405134.html</a>	n/a	n/a	Yes
Films, Videos and Publications Act 1993	<a href="http://www.legislation.govt.nz/act/public/1993/0094/latest/DLM312895.html">http://www.legislation.govt.nz/act/public/1993/0094/latest/DLM312895.html</a>	n/a	n/a	Yes
Crimes Act 1961	<a href="http://www.legislation.govt.nz/act/public/1961/0043/latest/DLM327382.html">http://www.legislation.govt.nz/act/public/1961/0043/latest/DLM327382.html</a>	n/a	n/a	Yes
Public Records Act 2005	<a href="http://www.legislation.govt.nz/act/public/2005/0040/latest/DLM345529.html">http://www.legislation.govt.nz/act/public/2005/0040/latest/DLM345529.html</a>	n/a	n/a	Yes
Official Information Act 1982	<a href="http://www.legislation.govt.nz/act/public/1982/0156/latest/DLM64785.html">http://www.legislation.govt.nz/act/public/1982/0156/latest/DLM64785.html</a>	n/a	n/a	Yes
Electronic Transactions Act 2002	<a href="http://www.legislation.govt.nz/act/public/2002/0035/latest/whole.html">http://www.legislation.govt.nz/act/public/2002/0035/latest/whole.html</a>	n/a	n/a	Yes
<b>National standards</b>				
NZ Information Security Manual (NZISM)	<a href="https://www.gcsb.govt.nz/publications/the-nz-information-security-manual/">https://www.gcsb.govt.nz/publications/the-nz-information-security-manual/</a>	n/a	n/a	No
Protective Security Requirements (PSR)	<a href="https://www.protectivesecurity.govt.nz/">https://www.protectivesecurity.govt.nz/</a>	n/a	n/a	No
www.classificationoffice.govt.nz/	<a href="https://www.classificationoffice.govt.nz/">https://www.classificationoffice.govt.nz/</a>	n/a	n/a	No

Approved: August 2017	Policy owner: Chief Information Officer
Next review: August 2018	Policy contact: Service Centre, IMD

<b>Title</b>	<b>Link/URL</b> (active link or state 'within this document')	<b>Security classification</b>	<b>LES LAN extreme threat compatible</b> (Yes/No)	<b>Show on the right hand?</b> (Yes/No)
Information and Records Management Standard	<a href="https://archives.govt.nz/manage-information/resources-and-guides/statutory/information-and-records-management-standard">https://archives.govt.nz/manage-information/resources-and-guides/statutory/information-and-records-management-standard</a>	n/a	n/a	No

Approved: August 2017	Policy owner: Chief Information Officer
Next review: August 2018	Policy contact: Service Centre, IMD