Acceptable Use **Attachment to the Computer and information security and Information and records management policies**	NZQA NEW ZEALAND QUALIFICATIONS AUTHORITY MANA TOHU MĀTAURANGA O AOTEAROA QUALIFY FOR THE FUTURE WORLD KIA NOHO TAKATŪ KI TŌ ĀMUA AO!
NZQA Quality Management System Supporting Document	

Purpose

The Acceptable Use requirements provide direction on how to comply with the Computer and information security, and Information and records management policies.

Scope

The requirements in this supporting document are mandatory for all NZQA staff and contractors.

Requirements

1 Use of NZQA ICT Infrastructure

1.1 Principle

NZQA information and communications technology ("infrastructure")[1], is provided for NZQA business purposes.

1.2 Infrastructure and Internet Use

NZQA staff and contractors must not use NZQA infrastructure to carry out non-NZQA business activities for personal gain.

NZQA staff and contractors must not use NZQA infrastructure for or to support any illegal activity, including:

- Accessing or downloading material (e.g. music, pictures, movies or software) that is objectionable or unlicensed
- Downloading material for the purposes of malicious activity (e.g. hacking)

Staff and contractors are expected to use their judgement and to avoid sites that pose a security risk to NZQA through the possible introduction of malicious content, sites that are inappropriate for a work environment, and/or sites that may bring NZQA into disrepute. For example, the following types of sites should not be visited:

- Gambling, pornography, hacking or dating
- File sharing sites that host unlicensed software
- Sites that are likely to contain offensive material

NZQA staff and contractors must limit personal use of NZQA's infrastructure and ensure that staff productivity and normal running of NZQA's business is not adversely impacted.

On direction from the Chief Information Officer (CIO) or Manager People and Capability, Internet sites that pose an elevated level of risk to the organisation may be limited or blocked. Additionally NZQA uses dynamic content evaluation that may block inappropriate or unsafe content (even on legitimate sites).

Regardless of restrictions placed on use of the Internet, staff and contractors must ensure that they act in accordance with the Code of Conduct at all times. Use of NZQA infrastructure is monitored for security and system management purposes, and to check compliance with policy and guidelines.

---

[1] "Infrastructure" includes but is not limited to computer equipment, desktop and mobile telephones (including smartphones), portable computing devices, software, operating systems, storage media, user and email accounts, wired and wireless networks, mobile and broadband connections and Internet access.

1.3 Public Comment

NZQA staff and contractors are not permitted to use NZQAs infrastructure to make discriminatory, defamatory, disparaging or harassing comments about NZQA, Government policies, processes or people.

NZQA staff and contractors must not post messages on blogs, newsgroups, websites or similar from an NZQA account or email address unless done as part of business duties, and with the approval of an NZQA Deputy Chief Executive.

Staff and contractors must not attribute personal opinions or beliefs to NZQA.

If personal opinions or beliefs are expressed, the person must not expressly or implicitly represent themselves as a representative or an employee/contractor of NZQA - for example by expressing personal opinions or beliefs when using NZQA email.

NZQA staff and contractors are reminded of their obligations under NZQA's Code of Conduct and the Code of Conduct for the State Services. Particularly the requirements to:

- Maintain the political neutrality required to enable us to work with current and future governments
- Carry out the functions of our organisation, unaffected by our personal beliefs
- Support our organisation to provide robust and unbiased advice
- Respect the authority of the government of the day
- Avoid any activities, work or non-work related that may harm the reputation of our organisation or of the State Services.

1.4 Email and Messaging Use

NZQA staff and contractors must not solicit for personal gain or knowingly use NZQA email or messaging to send:

- Spam or chain letters
- Material that could be considered offensive or harassment
- Emails with forged headers or content
- Malicious software

Where facilities are provided to release blocked email, users must take care to comply with acceptable use requirements.

NZQA email and messaging accounts may be accessed by the organisation at any time for business reasons. NZQA staff and contractors should have no expectation of the privacy or confidentiality of personal emails or messages sent or received over the NZQA email or messaging system, for example, emails may be required to be disclosed under the Official Information Act.

The 'All Staff' or 'All Level' group email addresses shall only be used for sending email messages that are work related. Use of the 'All Staff' email group requires DCE approval.

1.5 Equipment and Network Use

Only approved equipment[2] may be connected to NZQA infrastructure. Staff and contractors must check with Information Services (FirstCall Support) before connecting equipment not supplied by Information Services. This requirement is not intended to limit proper use of external websites (e.g. the secure extranet and NZQA webmail), publically accessible networks (e.g. public Wi-Fi) or as otherwise specified in this document.

[2] "Equipment" includes but is not limited to computers, laptops, tablets, printers, accessories, cell phones, portable storage devices and modems.

The CIO may approve the use and/or connection of specific non-NZQA devices. Such devices may be subject to configuration requirements as for NZQA equipment (see below). Approval to connect non-NZQA equipment does not constitute any assurance that the equipment will work with NZQA infrastructure. Any support provided will be on a best efforts basis.

NZQA staff and contractors must not install any non-approved or non-NZQA-licensed software or applications on to any NZQA device. Installation of software may only be performed by Information Services staff, or other staff by approval of the Chief Information Officer (CIO). All changes will be implemented in accordance with the ICT Change Management policy.

Only approved software and hardware may be installed on or connected to the NZQA network.

NZQA staff and contractors must not deliberately attempt to access information or resources to which they have no authorisation.

NZQA equipment must be configured before use by authorised staff in accordance with standards established by the CIO. This configuration may include the use, for example, of anti-virus software, encryption, monitoring and remote wipe utilities, personal firewalls, screensavers and/or password authentication.

NZQA may require that equipment be returned to Information Services from time to time for re-configuration, maintenance or upgrades.

NZQA staff and contractors must not knowingly disrupt or interfere with the configuration or normal running of NZQA networks, devices and other infrastructure.

NZQA security devices, software and configuration must not be modified, uninstalled or bypassed, except by authorised personnel. This includes the use of web-based proxies, 'anonimisers' or other methods of bypassing NZQA security controls to get to blocked or restricted websites. Antivirus, encryption, firewalls or any security related software must not be disabled unless this is carried out by authorised IS staff.

2 Handling NZQA Information

2.1 Principles

Information relevant to the conduct of NZQA's business should be shared openly within NZQA, across the NZQA lines of business, and with other government agencies, unless there is good reason to restrict access (such as the need to restrict classified information to those with a need to know, or to protect personal information covered by the Privacy Act).

The disclosure of NZQA information is subject to New Zealand law, and all relevant laws must be complied with in the publication of or granting of access to NZQA information. In particular, personal information about learners is subject to the Privacy Act and may not be disclosed without proper authority.

NZQA information must only be accessed or altered by authorised persons.

All data that is created on NZQA systems, remains the property of NZQA.

All information created, received and maintained by NZQA staff and contractors that provides evidence of how NZQA conducts business is a public record and must be managed according to the requirements of the Public Records Act.

NZQA's Retention and Disposal Authority and the Archives New Zealand General Disposal Authorities identify how long NZQA records must be retained for and the authorised disposal actions (destruction or transfer to Archives New Zealand).

Any disposal of NZQA records that does not comply with the retention timeframes or approved disposal actions will breach the Public Records Act.

2.2 General Requirements

NZQA information must be stored and processed on NZQA-approved systems, infrastructure and NZQA approved cloud services only. For example, the use of Google Docs is not approved, but Microsoft Office 365 is. In case of doubt, check with Information Services (FirstCall Support) for approval before storing or processing NZQA information.

NZQA information, regardless of format or location, must be adequately described and stored so that identification and retrieval is reliable, complete and timely.

NZQA information must be retained for the length of time specified in the Retention and Disposal Schedule or General Disposal Authorities. Disposal must be managed or authorised by the Records Management Advisor.

NZQA information must not be disclosed to those who do not have appropriate authorisation. Care must be taken to avoid accidental disclosure of NZQA information.

System users must be individually identified using appropriate registration and authentication mechanisms. Accounts, passwords and other credentials (e.g. VPN tokens and other two factor authentication tokens) must only be used by the individual to whom they were assigned.

2.3 Information Classification

All staff and contractors must be aware of the Information Classification guidelines in the Security Policy and classify all documents and emails they create appropriately. See the *Definitions* section at the end of this document for an explanation of the information classification terms.

For further guidance on information classification, see the Guidelines for Protection of Official Information wall chart or contact Information Services (Firstcall Support) or the Chief Information Security Officer.

If national security material (information classified RESTRICTED or above) is identified or received, the Chief Information Security Officer must be consulted on the appropriate way to handle the information.

2.4 Email and Messaging Security

Information classified IN CONFIDENCE should not be sent externally, unless encrypted. Information subject to the Privacy Act or classified SENSITIVE must not be sent externally, unless encrypted.

SEEMail provides transparent encryption of email to many Government agencies[3]. To trigger SEEMail encryption, use the keywords [in confidence] or [sensitive] in the subject or email body (not case sensitive, and with the square brackets). SEEMail will reject email marked as classified if sent to organisations not using SEEMail.

To access a document after hours use appropriate NZQA systems including NZQA webmail or the NZQA Remote Access Facilities. Messages or documents MUST NOT be forwarded to (non-NZQA) personal email accounts.

Other messaging systems such as instant messaging should not be used for transmission of classified information.

NZQA email is automatically captured and stored for disaster recovery purposes. Other forms of messaging (including instant messaging) must be used for informal internal communication only, and not for conducting or recording business activities.

Messages containing information that is evidence of business activity (and thereby becomes a record) must either be saved to the relevant file or sent as email and saved in the appropriate records management system (e.g. the S:/drive) in order to ensure

[3] Some government agencies, notably Careers and the Teachers Council, do not use SEEMail, so email to them from NZQA is unencrypted.

compliance with the Public Records Act. Ensuring messages are captured and stored is the responsibility of the person who created or received it.

2.5 Desktop Security

Passwords must not be shared with or disclosed to others. Care must be taken to ensure that others are not able to access passwords. For example, writing a password down on a piece of paper (even if hidden under your keyboard) is not an acceptable level of security.

To avoid accidental disclosure, classified information must be appropriately secured when not in use. Paper documents classified IN CONFIDENCE must not be left visible when leaving your desk. SENSITIVE information must be secured in a locked cabinet. Computers must have their screens locked when unattended.

2.6 Portable Storage Devices

Portable storage devices (PSDs) are any portable device that can store information, including but not limited to: USB sticks, cell phones, iPods, iPads, netbooks, laptops, portable hard drives, MP3 players, PDAs (personal digital assistants) and smart phones such as iPhones and BlackBerries.

Any material classed as IN CONFIDENCE must be encrypted if it is placed on a portable storage device. Material subject to the Privacy Act or classed as SENSITIVE must not be placed on a portable storage device without approved encryption. Information Services (FirstCall Support) can assist with encryption.

Portable storage devices must be registered in the Portable Storage Device register which is held by Information Services. Portable storage devices must be accounted for at all times, and any loss of a device must be reported (see Reporting a breach below).

Unregistered portable storage devices may be temporarily connected to the NZQA network solely when receiving information from another organisation. For example, it is acceptable to use an unregistered USB stick to load and display a presentation or accept data from another organisation. NZQA information must not be stored on unregistered devices.

All NZQA information and records created or received on portable storage devices must be saved into the appropriate NZQA records management system.

The CIO may limit the use of certain portable storage devices or specify which types may be used for storing NZQA information and/or connecting to the NZQA network.

2.7 Laptop Security

Laptops should be secured to a docking station or desk with an approved security cable or other approved locking mechanism when in the office. When travelling, they should be carried as hand luggage rather than checked in and kept in the boot of the car rather than left visible. Information Services will supply locking mechanisms for NZQA equipment where required.

Note that laptops are classed as portable storage devices and therefore subject to the restrictions in section 2.6 above.

2.8 Remote Access

When using remote access facilities including webmail and VPN, staff and contractors must ensure that security restrictions are not breached. Particular care must be taken when using non-NZQA equipment including public kiosks and shared use home equipment.

Material classified as IN CONFIDENCE should not be downloaded, stored or processed on non-NZQA owned equipment. Where this is unavoidable, the material must be completely removed after use. See table below for specific handling requirements.

Material subject to the Privacy Act or classified as SENSITIVE must not be accessed, downloaded, stored or processed on non-NZQA equipment.

HANDLING CLASSIFIED INFORMATION

<table>
<tr><th>Activity</th><th>Unclassified</th><th>IN CONFIDENCE</th><th>Privacy Act Related</th><th>SENSITIVE</th></tr>
<tr><td>NZQA Email to external organisations and people.</td><td>Ok</td><td colspan="2">Ok if using SEEMail – otherwise encrypt separately before sending. Ensure recipient is authorised to receive.</td><td>Encrypt separately. Ensure recipient authorised.</td></tr>
<tr><td>NZQA instant messaging system (internal)</td><td>Ok but ensure business records are captured separately.</td><td colspan="3">Do NOT use for classified or personal information.</td></tr>
<tr><td>Paper information on desktops</td><td>Ok</td><td colspan="2">Ensure information is not visible when leaving desk area.</td><td>Remove to a secure area or lockable file cabinet.</td></tr>
<tr><td>Info. stored on NZQA portable storage devices and laptops</td><td>Ok</td><td>Should be encrypted.</td><td colspan="2">Personal or SENSITIVE information must be encrypted.</td></tr>
<tr><td>Use of public access or untrusted PCs (e.g. web café or airport lounge)</td><td>Avoid if possible.
Delete files after use.
Do NOT use webmail.</td><td colspan="3">Do NOT access classified information from public or untrusted devices.</td></tr>
<tr><td>Use of own home PC</td><td colspan="2">Ensure PC is configured according to latest IS guidelines.
Delete files after use.</td><td colspan="2">Do NOT access personal or SENSITIVE information from non-NZQA equipment (see exceptions below)[4].</td></tr>
<tr><td>Use of non-NZQA PC in a managed corporate environment[5]</td><td colspan="2">Take care that you are working in a properly managed corporate environment. Delete files after use.</td><td>Take care with personal information and consider risks of inadvertent release.</td><td>Do NOT access SENSITIVE information from non-NZQA equipment.</td></tr>
<tr><td>Use of NZQA webmail</td><td colspan="2">Do NOT access from public or untrusted PCs[6].
Clear browser cache after use on non-NZQA PCs.</td><td rowspan="2">Do NOT access from public access or home PC equipment.</td><td rowspan="2">Do NOT access from non-NZQA equipment.</td></tr>
<tr><td>Use of NZQA Remote Access Facilities to access internal applications or networks</td><td colspan="2">Avoid accessing from public or untrusted equipment.
Do not save classified files locally.</td></tr>
</table>

[4] This restriction is not intended to prevent proper use of NZQA external websites including the secure extranet.

[5] "Managed corporate environment" is taken to mean an environment that you can reasonably expect to be secure (e.g. another NZ Government agency).

[6] This restriction applies because it may not be obvious that an email is IN CONFIDENCE until it has been opened (and therefore downloaded to the untrusted PC). .

Use of NZQA **Remote Access Facilities** remote desktop ("terminal services")	Take care when using public or untrusted PCs. Do NOT save files locally.	Do NOT access from public access PCs	Do NOT access from public access or home PCs.

2.9 Reporting a Breach

If you discover a security breach, or suspect that a breach may have taken place, you must immediately alert your manager. Breaches that must be reported include, but are not limited to, any loss, damage, accidental disclosure or unauthorised access of NZQA equipment or information. Loss of any equipment or device containing NZQA information must be reported, even if temporarily misplaced. Refer to 10.3.7.3 Investigate security breach.

If it is inappropriate to alert your immediate manager, for instance if you suspect your manager of deliberately breaching security, the incident or suspected incident must be reported to your manager's manager or to the Chief Security Officer or CIO. The protected disclosures processes in group 11.4.7 in Promapp may be used if you have information about a serious wrongdoing by or in NZQA.

2.10 Consequences of Violation

Any employee or contractor found to have violated these guidelines may be subject to disciplinary action, up to and including termination of employment or contract.

Related Documents / Links

Information and records management policy

Computer and information security policy

Definitions

For the purposes of this document, unless otherwise stated, the following definitions apply.

Staff and contractors	All permanent and fixed term staff, contractors, and consultants providing products and services to NZQA.
Classified information	Information that has a security classification assigned on the basis of the damage that would result from unauthorised disclosure. NZQA information security controls and infrastructure are designed to deal with information requiring protection for public interest and personal privacy reasons (i.e. IN CONFIDENCE and SENSITIVE).
Information classified as IN CONFIDENCE	This is information which if disclosed would prejudice the maintenance of law and order, impede the effective conduct of government, or affect adversely the privacy of its citizens. Examples in the NZQA context may include board, ministerial and cabinet papers, contracts and tender documents, and personal information.
Information subject to the Privacy Act	The Privacy Act deals with collecting, holding, use and disclosure of personal information and unique identifiers. For NZQA, this would include the personal data NZQA holds on learners. To ensure privacy is protected, NZQA places additional restrictions on the handling of personal information.
Information classified as SENSITIVE	This is information which if disclosed would damage the interests of New Zealand or endanger the safety of its citizens. Examples in the NZQA context may include information relating to budget appropriations or negotiation of agreements with other countries.
Must	This requirement is mandatory.
Should	This requirement is to be followed unless a good reason exists to act otherwise.
Approved	Approved means formally approved by the CIO or their delegate and registered in an appropriate register or standards document.