Acceptable Use

Attachment to the Information security and Information and records management policies

NZQA

Mana Tohu Mātauranga o Aotearoa
New Zealand Qualifications Authority

NZQA Quality Management System Supporting Document

Purpose

The Acceptable Use standards provide additional direction on how to comply with the Information security, and Information and records management policies.

Scope

It is mandatory for anyone using the NZQA network, IT equipment, and user accounts to meet the requirements in this supporting document.

These requirements apply to all NZQA ICT infrastructure.

The requirements apply to all information and data created, received, stored, and maintained by NZQA staff and contractors that provides evidence of how NZQA conducts business.

Requirements

1 ICT Infrastructure

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

1.2 NZQA infrastructure must not be used to carry out non-NZQA business activities for personal gain.

1.3 NZQA infrastructure must not be used 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).

1.4 Personal use of NZQA's infrastructure must be limited to ensure that staff productivity and normal running of NZQA's business is not adversely impacted.

1.5 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.

1.6 Use of NZQA infrastructure is monitored for security and system management purposes, and to check compliance with policy and guidelines.

1.7 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 effort basis.

1.8 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

[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.

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

Chief Information Officer (CIO). All changes will be implemented in accordance with the ICT Change Management policy.

1.9 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, 'anonymisers' 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.

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

2 Equipment

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

2.2 NZQA equipment must be configured before use by authorised IS 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.

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

3 Authentication

3.1 All NZQA system users (staff and contractors) must be individually identified using appropriate registration and authentication mechanisms.

3.2 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.

4 Laptops and other Portable Storage Devices

4.1 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, PDAs (personal digital assistants) and smart phones such as Apple iPhones and Android.

4.2 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.

4.3 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).

4.4 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.

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

4.6 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.

4.7 When travelling, laptops should be carried as hand luggage rather than checked in; and kept in the boot of the car rather than left visible.

5 Internet use

5.1 Accessing sites that may compromise NZQA's security, are inappropriate for the workplace, or could harm NZQA's reputation is not permitted.

For example, the following types of sites must not be visited:

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

5.2 Access to internet sites that pose an elevated level of risk to the organisation will be limited or blocked, as determined by the Chief Information Officer (CIO) and/or Manager People and Capability.

5.3 Dynamic content evaluation may block inappropriate or unsafe content (even on legitimate sites).

6 Email and Messaging

6.1 Personal email accounts must not be used for conducting NZQA business.
To access a document after hours, use appropriate NZQA systems including NZQA web solutions or the NZQA Remote Access Facilities.

6.2 Messages or documents must not be forwarded to (non-NZQA) personal email accounts.

6.3 NZQA email and messages are automatically captured and stored for disaster recovery purposes, Official Information Act requests, and Privacy Act requests.

6.4 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 NZQA's records management system to ensure compliance with the Public Records Act.
Ensuring messages are captured and stored is the responsibility of the person who created or received them.

6.5 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 or Privacy Act.

6.6 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.

6.7 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.

6.8 When considering releasing blocked email, users must comply with the same requirements in 6.7.

7 NZQA Information

7.1 Refer to the Information and Records management policy.

7.2 All information and data created, received, and maintained by NZQA staff and contractors that provides evidence of how NZQA conducts business:

- is a public record,
- must be managed according to the requirements of the Public Records Act,
- remains the property of NZQA.

7.3 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).

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

7.5 Any disclosure of NZQA information is subject to New Zealand law, and all relevant laws must be complied with in the publication of, or granting access to, NZQA information. Examples that apply are the Privacy Act 2020 and the Education and Training Act 2020.

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

7.7 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 the Information Management Team for approval before storing or processing NZQA information.

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

8 Classified Information

8.1 All NZQA staff and contractors must be aware of the Information Classification guidance provided by Protective Security and classify all documents and emails they create appropriately.

8.2 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.

8.3 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.

8.4 SEEMail provides message body encryption of email to Government agencies. 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.

8.5 Non NZQA approved messaging systems should not be used for transmission of any classified information.

9 Desktop Security

9.1 Refer to the Clear desk for classified information policy

9.2 Passwords must not be shared with or disclosed to others. Care must be taken to ensure that passwords cannot be readily accessed.
Refer to the Password Standard.

9.3 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.

10 Remote Access

10.1 When using remote access facilities including webmail and VPN, you must ensure that security requirements advised in this standard and in related NZQA policies and processes are not breached.

10.2 Requirements stated in these standards and related policies and processes must be met when using non-NZQA equipment including public kiosks and shared use home equipment.

10.3 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.

10.4 Material classified as SENSITIVE must not be accessed, downloaded, stored, or processed on non-NZQA equipment.

10.5 Material subject to the Privacy Act must not be accessed on public access or untrusted equipment.

11 Public Comment

11.1 NZQA staff and contractors have obligations under NZQA's Code of Conduct and the Code of Conduct for the Public Sector.

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

11.3 Messages must not be posted 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.

11.4 NZQA staff and contractors must not be seen to attribute personal opinions or beliefs to NZQA, for example through expressing personal opinions or beliefs when using NZQA email.

12 Reporting a Breach

12.1 Anyone discovering a breach of these requirements (or the requirements of the Information security, and Information and records management policies), or suspecting that a breach may have taken place, must immediately alert their manager. Breaches that must be reported include, but are not limited to, any loss, damage, accidental disclosure, or unauthorised access to NZQA equipment or information.

12.2 Loss of any equipment or device containing NZQA information must be reported, even if temporarily misplaced.

12.3 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.

13 Consequences of not meeting these requirements

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

Related Documents / Links

Password standard

Information and records management policy

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/ Shall	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.