

CONNECTING
THE SECTOR

**Education Sector Authentication & Authorisation
(ESAA)
Operations Policy**

VERSION: FINAL (March 2011)

© Ministry of Education, 2007

Table of Contents

1.	Introduction	2
1.1.	Purpose	2
1.2.	Who should read this document?	2
2.	Overview	3
3.	Contextual Framework	4
3.1.	Scope	4
3.2.	Components	4
3.3.	Compliance	4
3.4.	Statement of Limitation	5
3.5.	Basis of the ESAA System Policy	5
4.	Trust	6
4.1.	Core Concepts for Establishing an Identity	6
4.2.	ESAA Trust Level Relationship with EOI Confidence Levels	6
4.3.	Trusted Referees	7
4.4.	Authentication of Unknown Identities	7
4.5.	ESAA EOI Criteria	8
4.6.	An Organisation's Trust Level	9
4.7.	An Application's Trust Level	9
4.8.	Authorisers & Access Control	9
4.9.	Role Provisioning	9
4.10.	ESAA Administrator	10
4.11.	Change in Trust Level	10
5.	Privacy	11
5.1.	Collection of Personal Information	11
5.2.	ESAA User-ID	11
5.3.	ESAA Enabled Applications	11
5.4.	Intermediary Applications – Student Management Systems (SMS)	11
5.5.	Retention of Personal Information	12
5.6.	Disclosure of personal information	12
6.	Security	13
6.1.	e-GIF Information Classification	13
6.2.	Overview of Security Architecture	13
6.3.	Operational and Network Security	13
6.4.	Identity based security	14
6.5.	ESAA System Administrator and ESAA Administrators	15
6.6.	Retention of EOI documentation	15
6.7.	User Security	15
6.8.	User Violation	16
6.9.	Change Control	17
6.10.	Compliance	17
7.	Management of the ESAA Environment	18
7.1.	Education Sector ICT Shared Services Oversight Sub-Committee	19
7.2.	MoE SaBS – Sector and Business Services	19
7.3.	MoE BaSIS – Business and Sector Information Systems	19
7.4.	Vendor	19
8.	Responsibility	20
8.1.	Application Owner's Responsibilities are to:	20
8.2.	Organisation's Responsibilities are to:	20
8.3.	Users Responsibilities are to:	20
9.	ESAA Stage 2	21
9.1.	Pilot Distribution model	21
9.2.	Pilot Federation model	21
9.3.	Government Logon Service (GLS) Integration	21
10.	Appendices	22
10.1.	Appendix A – Identity Roles	22
10.2.	Appendix B – Identity Objectives described in the DIA Standard	24
10.3.	Appendix C - ESAA Trust Level Relationship with EOI Objectives	24
10.4.	Appendix D – User Setup and Access Request Form	24
10.5.	Appendix E – Authoriser Setup Form	24
10.6.	Appendix F – Overview of MoE Operational Security Policy	25
10.7.	Appendix G - Conditions of Use	26

1. Introduction

The vision of New Zealand's ICT Strategic Framework for Education¹ is "to improve learner achievement in an innovative education sector, fully connected and supported by the smart use of ICT". The ESAA system is an open, standards-based solution, engineered to support a seamless link to the Education Sector online services, independent of the entry point into the sector networks.

The ESAA solution is an identity management system that enables user authentication, authorisation and single sign-on to online services. Users can logon to an online service with a single user name and password and traverse seamlessly between ESAA enabled applications without the need to log out of one application and repeat the log on process to access another application.

The Evidence of Identity process, assigning users a trust level appropriately aligned with the user's access requirements, is pivotal for the ESAA model to pave the way to Circles of Trust that effectively creates a virtual sector. Additionally, a common approach and acceptance of consistent security and privacy practices is essential across the spectrum of ESAA stakeholders.

Representatives from the Education Sector Agencies provide leadership to maintain sector and public trust in the security and management of electronic information, and aims to ultimately improve learner achievement.

The ESAA solution is the future model for the implementation of Circles of Trust via federated identities (the process of a user authentication across multiple organisations); thereby realizing the goal of a collaborative Australasian, and potentially, a wider community.

1.1. Purpose

Due to the diverse dimensions of the privacy, trust and security components impacting identity management, authentication and authorisation, it is necessary to establish a "shared zone of acceptance" around privacy and security practices.

The ESAA Operations Policy specifies policy and standard practices necessary to develop a security conscious culture for organisations wishing to benefit from the ESAA service.

1.2. Who should read this document?

- An employee(s) of an organisation responsible for initiating and enforcing the security and privacy processes necessary to comply with the policies described in this manual.
- An employee(s) of an organisation appointed the role as a Trusted Referee for the purpose of verifying a new user's identity.
- An employee(s) or an organisation appointed the role of an Access Authoriser and/or Role Authoriser for the purpose of authorising access.
- An employee(s) of an organisation nominated to liaise with the ESAA Administrator through the Sector Service Desk with regard to audit issues.
- An employee(s) of an education agency involved in the management and oversight of the ESAA service.
- Sector Service Desk – Ministry of Education.

¹ www.minedu.govt.nz/goto/ictframework

2. Overview

The investment in Information and Communications Technology (ICT) is planned and co-ordinated through New Zealand's ICT Strategic Framework for Education (Strategic Framework). The objective of the Strategic Framework is to improve learner achievement through the smart use of ICT. The Strategic Framework is aligned with, and supports the e-Government and National Digital Strategies and the international e-Framework for Education and Research².

The Education Sector is moving from a model of relatively standalone education providers towards an ICT-enabled networked, collaborative environment for learners, teachers, providers and agencies. The ESAA system is a key component of the Strategic Framework, as it addresses the fundamental issue of authentication. The ESAA system is an identity management, authentication, authorisation and single sign-on service. The ESAA system aligns the Education Sector with industry and government security protocols and shall support a seamless link to relevant Education Sector online applications, independent of the entry point into the sector networks – ultimately providing a secure, single sign-on for all Education Sector online applications.

The ability to transact seamlessly across the Education Sector with one logon (username) and password removes the need for users to repeatedly log in and out of various applications across the Education Sector using multiple password and user names. Additionally, the ESAA system allows self-provisioning for authorised applications, i.e. users shall be able to register themselves once and use this online registration process many times to access numerous applications across the Education Sector.

The facility of a single sign-on through the ESAA system will result in:

- Reduced time and inconvenience for users to complete transactions;
- Improved security and privacy through the reduction in use and re-use of passwords across online applications;
- Improve the flow of information among individuals, groups, government agencies and the Education Sector as whole.

The Education Sector has a legal and ethical obligation to ensure that privacy of individuals and the quality and integrity of electronic information is not compromised. Maintaining privacy and security of electronic information is compounded by the complexity and variety of stakeholders and systems involved. A Circle of Trust is established effectively to create a virtual sector, characterized by shared privacy and security principles, rules and expectations.

Compliance with the Operations Policy is required by all participants that use, or provide ESAA enabled services to:

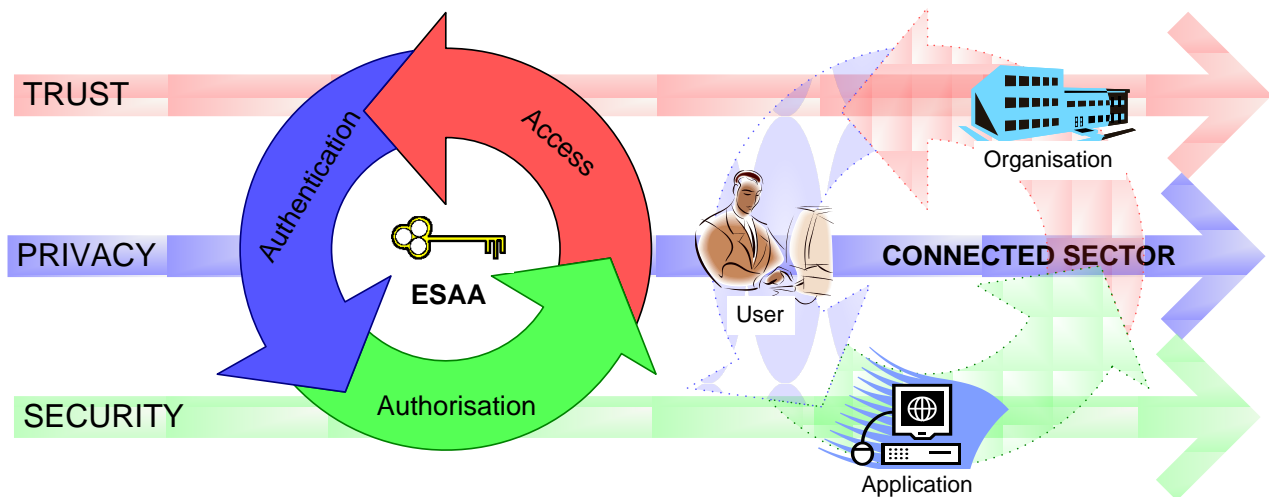
- Achieve private and secure access to online education resources;
- Enhance privacy and security collaboration between education providers;
- Provide the foundation to create a culture of privacy and security awareness.

² www.e.govt.nz/
www.digitalstrategy.govt.nz
www.e-framework.org

3. Contextual Framework

3.1. Scope

The Operational Policy applies to all education providers and solution providers that interface with the ESAA system, and their respective users of ESAA enabled online applications. The principles of trust, privacy and security are key factors that build trustworthiness and a security conscious culture that protects the exchange of electronic information in the connected sector.



3.2. Components

Service providers are interpreted as the organisations that provide education and or an application.

ESAA stakeholders are...	Defined as....
Organisations	Government agencies, Tertiary Education Organisations (TEOs) and Education Providers (including schools, tertiary education organisations, ICT vendors, etc).
Application Owners	The individual responsible for the application and is located within a TEO, an agency or Education Provider.

Any one individual may at various times access online applications as any of the three categories of a user.

Users of the ESAA system are...	Defined as....
Agency employees	Employees of government agencies with the Education Sector.
Sector employees	Education Sector users, generally those with administrative roles within schools and other education providers.
Other education sector participants	Learners or teachers who access information related to their studies either formal or informal.

3.3. Compliance

Compliance with the Operations Policy is required by those who provide ESAA enabled services and the users of these services.

3.4. Statement of Limitation

The architecture strategy for the ESAA system provides for three models for employing the identity management service (directory service);

- Centralised directory service – all users and their profiles shall be stored and managed within a centralised directory. Users shall be registered by a central administration team.
- Distributed directory service – an instance of the ESAA system is distributed across organisations. Users may be registered by administration teams within each organisation. User profiles shall be managed and stored within both a central (master) directory and distributed directories located at the organisation.
- Federated directory service – Each organisation shall operate its own identity management system (these need to be compliant with the ESAA supported international standards SAML2 and Shibboleth 1.3). Users shall be registered by administration teams within each agency. Each user shall have several profiles stored within directories of each organisation with which they have contact.

This document includes policy for the centralised directory service. It does not include policy applicable to ESAA distribution and federation models; these policies will be incorporated into ESAA stage 2 (refer to ESAA2 - section 10).

3.5. Basis of the ESAA System Policy

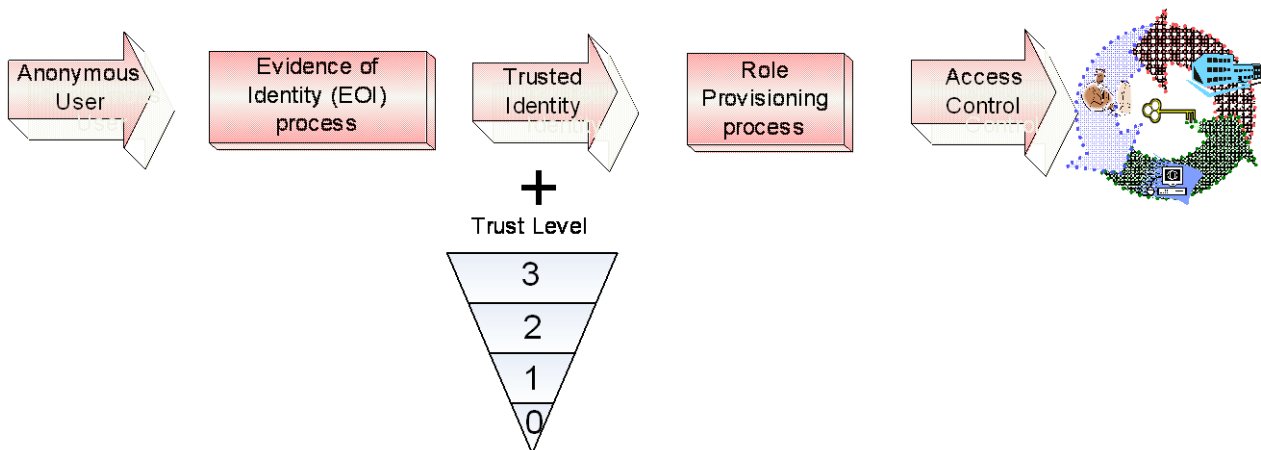
ESAA Policy has incorporated and adopted policy and standard practices consistent with:

- Government legislation:
 - Privacy Act 1993
- Department of Internal Affairs (DIA)
 - Evidence of Identity Standard
The DIA is custodian of the Evidence of Identity standard, which outlines the approach to assessing identity-related risk that should be applied by New Zealand State Sector Agencies delivering services to the public
- State Services Commission
 - e-Gif – E-government Interoperability Framework – a collection of policies and standards endorsed for New Zealand government information technology (IT) systems
 - Guide to Authentication Standards for Online Services
 - Authentication Key Strengths Standard
 - Data Formats for Identity Records Standard

4. Trust

The principle of trust is built into the ESAA technology through the use of trust levels assigned to organisations, applications and users. By the members agreeing to comply with quality security and privacy practices, trust is strengthened, which achieves a standard necessary for a virtual sector to exist. In order to authorise a new user access to an application, it is necessary to establish:

- Trust level for individual identities,
- Roles appropriate to the rights and privileges existing within an application.



An identity (a user or application) remains un-trusted until such time as they undergo a recognised Evidence of Identity (EOI) process i.e. one that is traceable, repeatable and auditable. The EOI requirements will depend on the level of confidence in the identity that is required for the particular service. A trust level between zero and three must be assigned to all registered users, applications, organisations and authorisers. Access control is enforced through the establishment and definition of business roles, which have minimum trust levels.

4.1. Core Concepts for Establishing an Identity

Verifying an individual's identity involves a number of components, each of which achieves a different purpose. The EOI requirements will depend on the level of confidence in the identity that is required for the particular service.

- Evidence of identity – to determine that the identity exists, and living (objectives A & B),
- Presenter links to the identity – that the person claiming the identity is who they say they are, and that they are the only claimant to the identity (objective C & D),
- Presenter uses identity – that the claimant is operating under the identity in the community (objective E).

Refer to Appendix B– Identity Objectives as described in the DIA Standard for further explanation.

4.2. ESAA Trust Level Relationship with EOI Confidence Levels

The level of identity-related risk is determined by analysing the range of consequences that can occur if access is given to an individual who claims an identity that is not their own. The table below illustrates the relationship between the risk category, Evidence of Identity (EOI) confidence levels and ESAA Trust levels³.

Risk Category...	Evidence of Identity Confidence Level...	ESAA Trust Level...
Nil identity-related risk - referred to as 'anonymous' or pseudonymous' service.	<ul style="list-style-type: none"> • None required 	0

³ Guide to Authentication Standards for Online Services (<http://www.e.govt.nz/standards/e-gif/authentication/guide-to-auth-standards>)

Risk Category...	Evidence of Identity Confidence Level...	ESAA Trust Level...
Low level of identity-related risk consequence in the service.	<ul style="list-style-type: none"> Evidence of Identity is genuine and individual claiming identity uses it in the community. Evidence of Identity accepted on 'face value'. 	1
Moderate level of identity-related risk consequence in the service.	<ul style="list-style-type: none"> Evidence of Identity is genuine and individual claiming identity uses it in the community. Individual is confirmed as the genuine claimant of the identity. Evidence of Identity accepted on 'face value'. 	2
High level of identity-related risk consequence in the service.	<ul style="list-style-type: none"> Evidence of Identity is genuine and individual claiming identity uses it in the community. Individual is confirmed as the genuine claimant of the identity. Evidence of Identity is verified by third party. 	3

Appendix C – ESAA Trust Level Relationship with EOI objectives.

- 4.2.1. An identity remains un-trusted until such time as they undergo a recognised Evidence of Identity (EOI) process (i.e. one that is traceable, repeatable and auditable).
- 4.2.2. Since no single identity document (e.g. passport) satisfies the identity objectives required to ascertain a level of confidence and trust, additional evidence of identity within the community is necessary.

4.3. Trusted Referees

Trusted referees are a vital component of the EOI process. A Trusted Referee is a person who confirms that, to their knowledge; the presenting identity information corresponds to that individual and achieves the identity objectives for the associated trust level.

- 4.3.1. The CEO of the Organisation (or equivalent) is deemed a Trusted Referee and can appoint a suitable person to act as Trusted Referee for the EOI process, and as a point of contact should there be a discrepancy in the identity information supplied for the registration process.
- 4.3.2. A Trusted Referee must have personal knowledge of the individual being identified and be trusted by the organisation.
- 4.3.3. An internal trusted referee shall undergo the EOI process to establish a level of trust in the ESAA system.

4.4. Authentication of Unknown Identities

The EOI process is applied to all unknown identities, namely:

- 4.4.1. Users: Process by which an organisation establishes confidence in an individual's unknown identity.
- 4.4.2. Authorisers: Process of the Application Owner assigning members of an organisation the role of an Access Authoriser and or Role Authoriser, who in turn can nominate (internal) Trusted Referees.

The outcome of the EOI process is a trust level assigned to each party:

- 0 (zero) or no trust,
- 1 – low
- 2 – moderate
- 3 – high trust

4.5. ESAA EOI Criteria

Identity related documents are categorised into two groups in the EOI process; documents are required from both groups⁴.

4.5.1. Group 1 to prove identity exists

4.5.2. Group 2 to prove identity is used in the community.

ESAA Eoi Criteria	Trust Level 1 With or without photo	Trust Level 2 One identity document to include a photo of the applicant	Trust Level 3
<p>Group 1 – Identity exists</p> <ul style="list-style-type: none"> • NZ Passport • Overseas passport • NZ Emergency Travel Doc ETD • NZ Refugee Travel Doc • NZ Certificate of Identity (Passports Act 1992) • NZ Certificate of Identity (Immigration Act 1987) • NZ Firearms Licence / Firearms Dealers Licence • NZ Birth Certificate • NZ Citizenship Certificate <p>If the documents supplied above indicate the applicant has changed name by marriage/deed poll etc) then include one or more of the documents below which demonstrate the name change.</p> <ul style="list-style-type: none"> • NZ Marriage Certificate • NZ Civil Union Certificate • Change of Name by Statutory Declaration • Change of Name by Deed Poll • NZ Divorce Papers • Certificate of Annulment 	<p>1 x Identity Document (originals/copies)</p>	<p>1 x Identity Document (originals/certified copies)</p>	<p>1 x Identity Document (originals/certified copies)</p>
AND			
<p>Group 2 – Identity is used in the community</p> <ul style="list-style-type: none"> • International Driving Permit • NZ Driver Licence • Confirmation of Permit Status • Community Services Card • Electoral Roll Record • Student Identity cards & employee Identity cards • 18+ Card (valid) • Utility bill • Teacher’s Registration Certificate 	<p>1 x Identity Document (originals/copies)</p>	<p>1 x Identity Document (originals/certified copies)</p>	<p>2 x Identity Document (originals/certified copies)</p>

⁴ Evidence of Identity Standard – Identity Objective – see Appendix A

4.6. An Organisation's Trust Level

An Organisation's trust level is based on the strength of their EOI process.

4.6.1. The Organisation's EOI process will be evaluated to determine the trust level.

4.6.2. The maximum trust level assigned to a user is limited to the Organisation's trust level.

4.7. An Application's Trust Level

The trust level for an application is determined by the sensitivity of the information held within the application, which dictates the user's minimum trust level required to access the application.

4.7.1. Application Owners must perform a risk analysis to determine the sensitivity and confidentiality of the electronic information contained in their application.

4.7.2. The Application Owners determine the appropriate trust level necessary to access their application.

4.8. Authorisers & Access Control

Authority begins with the Application Owner, who can nominate members of an organisation, suitable in rank, to act in the capacity as an Access Authoriser and/or Role Authoriser. Appendix A further details the Identity Roles in the ESAA system.

4.8.1. It is the discretion of the Application Owner to set the authority level required for the application, i.e. Access Authoriser, Role Authoriser or no approval.

4.8.2. The Access Authoriser can nominate a Role Authoriser specific to an organisation.

4.8.3. The Access Authoriser can provision business roles to any user in any organisation.

4.8.4. The Role Authoriser can provision business roles to any user within their organisation.

4.9. Role Provisioning

Role Provisioning is the process for assigning the user roles (permission types) within ESAA enabled applications. Role provisioning allows greater flexibility and control for users accessing ESAA-enabled applications and the information contained therein.

Type ...	Defined as....
Access rights	Lower level permissions, e.g. create, read, update, display.
Business roles	A defined role in the Education Sector, e.g. teacher, principal, comprised of a collection of functionalities, which are mapped to a person's job title.
Security roles	A group of access rights that are mapped to a specific functionality within an application.

4.9.1. Users must be provisioned with the appropriate business roles for an ESAA enabled application, unless no approval is required.

4.9.2. The Access Authoriser and Role Authoriser authorises the level of access necessary for the user.

4.9.3. The highest trust level assigned to a security role dictates the minimum trust level of the business role, which in turn must correspond to the trust level assigned to the application.

4.10. ESAA Administrator

4.10.1. The creation, maintenance and termination of an ESAA identity for a user shall be undertaken by an ESAA Administrator.

4.10.2. ESAA Administrators must have a Trust Level 2.

4.10.3. An ESAA Administrator can be nominated as a Access Authoriser to act on behalf the Application Owner.

4.11. Change in Trust Level

4.11.1. Once a user is a trusted identity, the EOI process is repeated if their identity has expired within the ESAA system due to inactivity or the user requests further access roles requiring a higher trust level than the user already has.

4.11.2. A change in trust level shall require the user to repeat the EOI process to ensure that the relationship between identity-related risk and confidence levels are safe.

4.11.3. A change in the trust level of an application or related business roles doesn't affect existing users who already have been provisioned the business role.

5. Privacy

All information collected and retained within the ESAA system environment, either in hard copy or stored, is regarded as confidential and subject to the provisions of the Privacy Act. The design feature of the ESAA system allows all users to have one "identity" to access multiple applications, meaning only one set of personal data needs to be provided rather than multiple sets. This, along with the centralised storage of personal data, protects privacy.

The ESAA system collects the minimum personal information necessary to:

- Register an identity;
- Manage access;
- Audit and report incidences.

5.1. Collection of Personal Information

- 5.1.1. The user shall be made aware of the reasons why personal information is collected.
- 5.1.2. Personal attributes (name, date of birth etc) are used exclusively to provide evidence of identity.
- 5.1.3. Personal information supplied must be initiated by the individual.
- 5.1.4. The EOI process shall gather the minimum information needed to establish the level of confidence required to mitigate risk associated with provision of the requested access to an application.
- 5.1.5. Activating a user's role in the ESAA system is permitted only when the personal information collected, is complete and accurate.

5.2. ESAA User-ID

- 5.2.1. Users shall be identified electronically with a unique user-id.
- 5.2.2. The user-id shall be automatically generated and managed by the ESAA system.
- 5.2.3. Each user's access rights shall be linked to their user-id.
- 5.2.4. The user-id shall be disabled based on a significant period of inactivity.
- 5.2.5. The link between a user's traits and their user-id is only stored with the ESAA system.

5.3. ESAA Enabled Applications

- 5.3.1. User credentials are transacted between the ESAA system and the user.
- 5.3.2. The only information transported between the ESAA system and applications are attributes authorised for the application to use (i.e. no identifying information can be sent between applications).

5.4. Intermediary Applications – Student Management Systems (SMS)

- 5.4.1. User credentials may be passed through intermediary applications (SMS) to the ESAA system and must be via secure channels.
- 5.4.2. A SMS must not store password and user-id of end users. The only information permitted is the information used for authentication purposes between SMS and the ESAA system.
- 5.4.3. Intermediary applications must collect username and password using secure channels.
- 5.4.4. Application credentials must not be used by users when entering the logon screen.

5.5. Retention of Personal Information

- 5.5.1. Original EOI documentation submitted in the EOI process to the Trusted Referee is returned to the applicant within two weeks. EOI documentation retained in this period must be securely stored. Copies of EOI documentation are to be retained by the Trusted Referee.
- 5.5.2. Individuals are entitled access to their personal information retained in the ESAA system.
- 5.5.3. Authorised access is required to view personal information stored on the ESAA directory.

5.6. Disclosure of personal information

- 5.6.1. Identity formation stored within the ESAA system shall not be disclosed to any person who is not a member of ESAA support or third parties, unless authorised to do so by the user or required by law.

6. Security

The principle of security encompasses the controls in place to safeguard Information and Communication Technology (ICT) and user's access to applications.

6.1. e-GIF Information Classification

The e-GIF is a collection of policies and standards endorsed for New Zealand government information technology (IT) systems. Information that needs protection is classified as either:

IN-CONFIDENCE	Information relating to an identifiable individual not intended for the public domain; commercially sensitive information that needs protection from unauthorised access.
IN-CONFIDENCE special handling	User's password and challenge phrase information held by any online application.
UNCLASSIFIED	All other information that is not covered above.

All electronic information within the ESAA framework is deemed IN-CONFIDENCE special handling.

6.2. Overview of Security Architecture

Security Category...	Scope...	Responsibility...
Operational	Protect the MoE infrastructure supporting ESAA	MoE - Development Team
Network	Protect communication channels between the MoE and the organisations	MoE - Information Systems Group
Identity –based	Control access to information	MoE - Sector and Business Services Unit

6.3. Operational and Network Security

- 6.3.1. The ESAA system is housed at the Ministry of Education (MoE) and inherits the security controls and standards stipulated by the MoE Operational Security Policy, which is compliant with e-Gif and NZ Security in the Government Sector (SIGS) standards. Refer to Appendix F.
- 6.3.2. The security controls supporting the application is the responsibility of the organisation housing the application. The expected minimum is SIGS or NZ SIT 400, a supporting publication to SIGS is the Protective Security Manual, which provides implementation guidance.⁵

⁵ SIGS – www.security.govt.nz
NZ SIT 400 – www.gcsb.govt.nz

6.4. Identity based security

The following table illustrates the components of identity-based security and the supporting controls that ensure security.

Security Methods ...	Supporting Controls ...
<p>6.4.1. User Provisioning</p> <p>This is the initial registration of an identity in the ESAA system. An individual provides evidence to register their identity and gains an accepted trust/confidence level within the ESAA system.</p>	<ul style="list-style-type: none"> ● All identities undergo EOI process. ● Identity documents are sighted and verified by a Trusted Referee. ● Appropriate trust levels/confidence levels are assigned per EOI criteria.
<p>6.4.2. Role Management</p> <p>This is the entitlement/access privileges that an individual has for accessing a particular application, resource or information.</p>	<ul style="list-style-type: none"> ● All identities undergo EOI process to gain a trust level. ● The EOI trust level matches the classification of information for which they require access. ● The access privilege is authorised by a Role Authoriser. ● Only the targeted audience has access to confidential, private or sensitive information.
<p>6.4.3. Authentication (key)</p> <p>An individual is authenticated in the ESAA system at each login attempt when they have entered a valid username and password.</p>	<ul style="list-style-type: none"> ● A unique username is issued for every registered identity in the ESAA system. ● Usernames are not deleted or re-used in the ESAA system. ● Users are given three login attempts before their account is locked. ● Password construction: <ul style="list-style-type: none"> ○ Minimum 7 characters. ○ Must contain characters from at least 3 of the following sets; lowercase, uppercase, digits, punctuation and special characters. ● Password management: <ul style="list-style-type: none"> ○ Users are forced to change their single use password at their first successful login. ○ Passwords expire after 180 days. Application credentials have a longer expiration date. ○ Users are forced to set their challenge response questions and answers at their first successful login. ● Encryption technology <ul style="list-style-type: none"> ○ Authentication information shall be protected during transit between the ESAA system and the application through channel encryption. ○ Channel encryption shall use Government Communications Security Bureau approved encryption technology conforming to requirements of SIGS and NZSIT 400.⁶

⁶ SIGS – www.security.govt.nz
NZ SIT 400 – www.qcsb.govt.nz

Security Methods ...	Supporting Controls ...
<p>6.4.4. Authorisation</p> <p>Access controls/policies are assigned to specific attributes or groups of attributes within the ESAA system, which enable authorised access to specific online information, resources or services.</p>	<ul style="list-style-type: none"> ● The individual must satisfactorily complete the EOI process to gain a trust level and is issued a unique username and password. ● Access privileges are authorised by the Application Owner or a duly delegated person. ● Control access to data using role-based control to assign application and data access rights to users based on their roles and privileges.

6.5. ESAA System Administrator and ESAA Administrators

Administrative access to ESAA infrastructure shall be restricted to those authorised individuals (system administrators) who are responsible for monitoring and or maintaining the ESAA system.

ESAA Administrators are responsible for registration, provisioning of users and act as the first point of contact with the user for any ESAA system queries.

- 6.5.1. ESAA System Administrators and ESAA Administrators shall undergo the EOI process for a Trust Level 2.
- 6.5.2. Administrative access to ESAA infrastructure is limited to individuals with the relevant responsibility, training and experience.
- 6.5.3. ESAA System Administrators and ESAA Administrators shall be granted administrative accounts with the minimum rights required to support their allocated functions. Administrative accounts (those with elevated privileges) shall not be used by individuals for non-administrative purposes.
- 6.5.4. The concept of need-to-know, a security principle, states that the ESAA Administrator should have access only to information needed to perform a particular ESAA function, and shall be applied when evaluating authorisation rights and privileges.

6.6. Retention of EOI documentation

- 6.6.1. All EOI documentation is destroyed in a secure manner after two months.
- 6.6.2. The User Setup and Access Request forms are archived according to the Ministry of Education's Retention Schedule for seven years. Restricted access is limited to authorised staff.

6.7. User Security

Security is quickly compromised through negligent behaviour of users, therefore organisations must ensure personnel are briefed and understand the responsibilities of using ESAA applications. The user is educated in the basics of security as detailed in the User Guide⁷ and the must accept the conditions of use when registering as a user of the ESAA system.

General Use

- 6.7.1. The user must sign and agree with the Acceptance of Conditions for the ESAA system during the registration process.
- 6.7.2. Users must not look at, change, delete or tamper with files or programmes that they are not authorised to access
- 6.7.3. Access to ESAA resources is restricted only to those who have authorisation to do so.

⁷ www.steo.govt.nz

- 6.7.4. Users shall take all reasonable steps to prevent the misuse or unauthorised access to their computer system or ESAA resources.
- 6.7.5. User must ensure their computer system has appropriate anti virus software installed.
- 6.7.6. Users must avoid the use of public shared computers such as internet cafes.

Password Construction

- 6.7.7. Passwords must be constructed according to rules which will be advised and enforced by the system and may be changed from time to time.
- 6.7.8. Users are required to change their allocated password at initial login.
- 6.7.9. The system will enforce password expiry with a frequency that may be changed from time to time.
- 6.7.10. Entering an incorrect username or password a consecutive number of times will lock a user's account.
- 6.7.11. Passwords shall not be re-used; a new password shall be constructed each time it is changed.
- 6.7.12. Administrators using application logins are required to change the allocated password at initial login.
- 6.7.13. For Administrators using application logins, the system will enforce password expiry with a frequency that may be changed from time to time.
- 6.7.14. Applications shall not store ESAA passwords in an un-encrypted form.

Password Protection

- 6.7.15. Sharing of (user) passwords, usernames or accounts is prohibited.
- 6.7.16. Users must not reveal their username or password to another person; a legitimate ESAA Administrator will not ask for a user's password.
- 6.7.17. Passwords must not be written on sticky notes, desk pads and calendars.
- 6.7.18. Users must not store their username/password in a file on their computer.

Challenge Response Questions and Answers

The first time a user logs into the ESAA system they are required to set challenge questions and answers. Should a user forget their password, they can re-set it by answering their challenge questions.

- 6.7.19. Users are required to choose different challenge questions from the list of available questions.
- 6.7.20. Users are required to enter different challenge responses for every challenge question selected.
- 6.7.21. Entering incorrect challenge responses, a consecutive number of times, will lock a user's account.

6.8. User Violation

The ESAA business owner reserves the right to monitor IT resources, including individual login sessions particularly where:

- 6.8.1. There are reasonable grounds to suspect a user is abusing ESAA login and resources.

6.8.2. It is required to be by New Zealand law.

6.8.3. There are reasons related to ESAA systems maintenance/performance issues.

Any violation of service use may constitute a breach of the conditions of use, which the user agreed to on registration, and action shall be taken appropriate to the seriousness of the breach. The Ministry of Education, Sector and Business Services (SaBS), is responsible for dealing with any violation of service use and shall liaise with the organisation's authoriser to ensure that appropriate action is taken.

6.8.4. Access to applications shall normally be revoked during the investigation of an incident, which shall be considered on a case-by-case basis.

6.8.5. Disciplinary action may include restriction or termination of a user's access to the ESAA system.

6.8.6. In special circumstances, compensation for improper use may be required.

6.8.7. Should an account be re-enabled, a written agreement shall be required; signed by the user and the authoriser that acknowledges the understanding and acceptance of the outcome of any further breach of the conditions of use.

6.9. Change Control

Any modifications to the ESAA system shall follow the change control process established for ICT shared services.

6.10. Compliance

Non-compliance with the standards described in the Operations Policy erodes the values of trust, privacy, and security necessary to achieve a connected sector.

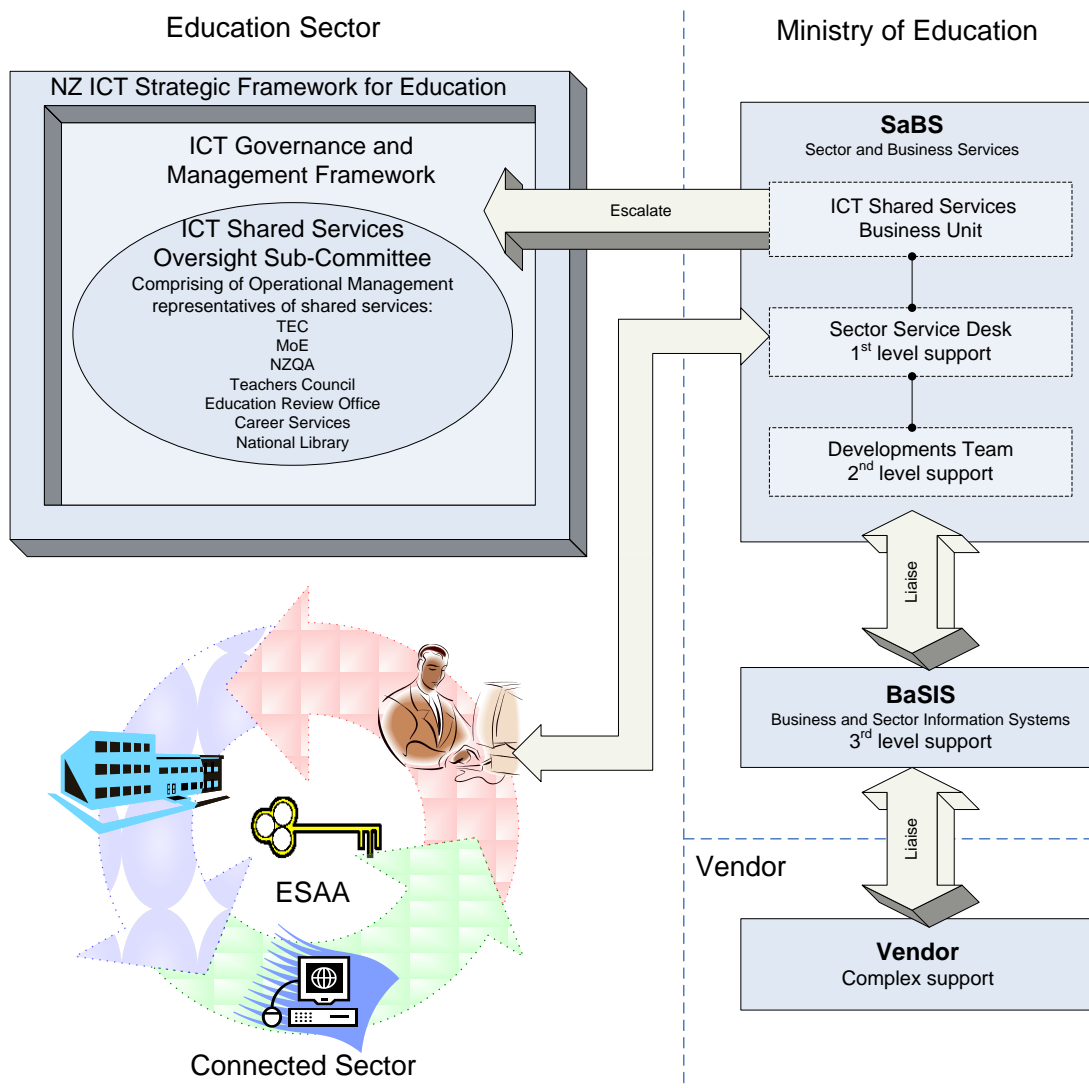
6.10.1. Organisations and ESAA enabled applications are subject to audit to ensure standards described in this code are adhered to.

6.10.2. A full investigation shall be performed for any breach of privacy or security and reported to the Education Sector ICT Shared Services Oversight Sub-Committee.

7. Management of the ESAA Environment

The ESAA system is a key component of the Education Sector Architecture Framework (ESAF) and the New Zealand ICT Strategic Framework for Education.

The diagram below illustrates the composition of the management, oversight and administration of the ESAA environment.



A framework for the operational management of Education Sector ICT Shared Services has also been established which defines:

- Incident management process, i.e. service delivery, 1st, 2nd and 3rd level support;
- Change release and patch management
- Service level management, i.e. maintenance of agreements
- Governance
- Shared Services communications across the Education Sector.

This framework is available from the Sector Service Desk, MoE (sector.servicedesk@minedu.govt.nz; 0800 422 599).

7.1. Education Sector ICT Shared Services Oversight Sub-Committee

Oversight for the ESAA environment is provided by members nominated from each of the Education Sector agencies. Responsibilities include:

- 7.1.1. Review and endorse any recommendations for new entrants (either organisations or new applications) that wish to utilise the ESAA service.
- 7.1.2. Provide an escalation point for any issues or risks that arise from the operational management of the ESAA service, including a breach to privacy and security policies.

7.2. MoE SaBS – Sector and Business Services

MoE SaBS operates as the administrative arm of the Oversight Sub-Committee. Responsibilities include:

- 7.2.1. Perform audit function of organisations and applications using the ESAA system to ensure identity security practices are compliant with the identity-based security outlined in Section 7.
- 7.2.2. Escalate any violation of privacy and security impacting ESAA's information and resources.
- 7.2.3. Evaluate and recommend proposed new entrants (either organisations or applications) that wish to utilise the ESAA service.
- 7.2.4. Provide first level technical support.
- 7.2.5. Administrate the EOI process for new users that wish to utilise the ESAA system.
- 7.2.6. Manage relationship with ESAA's vendor.
- 7.2.7. Escalate any violation of use of username and password impacting ESAA's information and resources.

7.3. MoE BaSIS – Business and Sector Information Systems

MoE BaSIS shall provide third level technical support.

7.4. Vendor

The vendor shall provide complex technical support.

8. Responsibility

The stakeholders in the ESAA environment must take responsibility to endorse and implement security and privacy policy and procedures for user provisioning, authentication, authorisation and access control.

8.1. Application Owner's Responsibilities are to:

- 8.1.1. Ensure appropriate controls (manual and electronic) exist to ensure the integrity of electronic information that is stored and in transit.
- 8.1.2. Ensure proper risk analysis performed to determine the authentication factors necessary to satisfy the trust level required for the application.
- 8.1.3. Nominate an authoriser to perform the duties of Access Authoriser, Role Authoriser and Trusted Referee defined in the EOI process.
- 8.1.4. Perform regular audits to ensure that privacy and security controls are in place over their application that satisfies the standards of the privacy and security policies.
- 8.1.5. Ensure that staff understand and comply with security requirements.
- 8.1.6. Liaise with the Sector Service Desk.
- 8.1.7. Ensure that the standards of use for their application are understood, and enforced through an agreement with the user.

8.2. Organisation's Responsibilities are to:

- 8.2.1. Ensure the ESAA EOI process is followed.
- 8.2.2. Satisfy the criteria around the various roles of an Authoriser, and ensure that they are aware of their duties.
- 8.2.3. Ensure that access rights and privileges granted to a user align with their purpose for accessing online applications.
- 8.2.4. Perform regular audits to ensure satisfactory privacy and security controls are in place.
- 8.2.5. Ensure that staff understand and comply with security requirements.
- 8.2.6. Liaise with the Sector Service Desk.

8.3. Users Responsibilities are to:

- 8.3.1. Complete the EOI process to become a trusted identity in the ESAA system.
- 8.3.2. Receive appropriate authorisation for access levels.
- 8.3.3. Acknowledge and accept conditions to use ESAA enabled applications described in the User Guide.
- 8.3.4. Follow password construction and management rules.
- 8.3.5. Follow password and access rules.

9. ESAA Stage 2

ESAA Stage 2 shall leverage users, processes and technology instigated in ESAA Stage 1 to achieve the education agencies' long-term vision of "improving learner achievement in an innovative education sector, fully connected and supported by the smart use of ICT".

Education sector agencies shall further support the shift towards this vision by piloting Circles of Trust and federated identity across the Education Sector. Distributed instances of the ESAA system and Federation allow various parties and their identity infrastructures to interoperate.

9.1. Pilot Distribution model

Distribution architecture permits both centralised and localised components of the ESAA service directory. Each organisation shall have access to both local applications and centralised ESAA applications for administration and reporting.

9.2. Pilot Federation model

Federation architecture shall provide access control in situations where the user's identity is not asserted by the ESAA system itself. It is anticipated that the ESAA service shall need to federate using federated protocols such as Shibboleth and/or SAML (Security Assertion Markup Language). Shibboleth, a project of Internet2/MACE, is developing architectures, policy structures, practical technologies, and an open source implementation to support inter-institutional sharing of web resources subject to access controls.

9.3. Government Logon Service (GLS) Integration

Integration of the ESAA system with GLS provides users a single point of entry to online government services.

Federation introduces new security challenges and the ESAA Operations Policy shall be modified accordingly.

10. Appendices

10.1. Appendix A – Identity Roles

Identities Involved...	Defined as...	Criteria ...	Rights...
Applicant	A person applying for an initial or increased ESAA trust level role rights.	<ul style="list-style-type: none"> • An employee of an education provider. • A user of online services. • Identity established at the respective education provider. 	No rights
User	The set of people and organisations registered and authenticated to use online services.	<ul style="list-style-type: none"> • An employee of an education provider. • A user of online services. • Identity established at the respective education provider. 	Access application per trust level assigned in the EOI process.
ESAA Administrator Sector Service Desk – 1st level support & team lead.	First level support for all ESAA system users.	<ul style="list-style-type: none"> • Employed within the Sector Service Desk – MoE. 	<ul style="list-style-type: none"> • Set up user account in the ESAA system; • Assign and activate trust level in the ESAA system; • Role provision in the ESAA system.
ESAA System Administrator	Second level support for all ESAA system users. One who can perform all functions within the ESAA system.	<ul style="list-style-type: none"> • Employed within the Sector Service Desk – MoE. 	Super-user functions in the ESAA system.
Trusted Referee (1)	<ul style="list-style-type: none"> • The Organisation's CEO. • A trusted identity who has been assigned authority as a Trusted Referee to confirm and verify EOI documentation within their organisation by their organisation's CEO. 	<ul style="list-style-type: none"> • Authenticated to trust level 2 and above. • Must work for a Trusted Identity Provider. • Must work for the same organisation as the person whose identity they are confirming (except for ESAA Admin staff) 	Authorise trust levels limited to their organisation's trust level.
Trusted Referee (2)	A Trusted Referee who is external to an organisation i.e. registered accountant, Justice of the Peace, Doctor, Lawyer, Board of Trustees Chairperson, School Principal, Minister of Religion, Kaumatua.	<ul style="list-style-type: none"> • Must not be related or a partner/spouse of the applicant or residing at the same address. • Must be a registered professional with an accessible contact address and phone number. 	Validate identity.

Continue...

Identities Involved...	Defined as...	Criteria ...	Rights...
Role Authoriser	A trusted identity who has been assigned specific authority as a role authoriser in the context of their own organisation by an Access Authoriser or Application Owner.	<ul style="list-style-type: none"> ● Authenticated to trust level 2 . ● Must work for a trusted organisation that is at Trust Level 2 or higher. 	Authorise role requests for their organisation.
Access Authoriser	A trusted identity who has been assigned specific authority of an Access Authoriser by the Application Owner.	<ul style="list-style-type: none"> ● Authenticated to trust level 2. ● Must work for a trusted organisation that is at Trust Level 2 or higher. 	<ul style="list-style-type: none"> ● Request new security and business roles; ● Authorise role requests; ● Nominate and authorise a Role Authoriser across organisations; ● Authorise Role Authoriser rights for organisations.
Application	An online service.	<ul style="list-style-type: none"> ● Education Sector online service. ● Security criteria are satisfied as defined in the Security Policy. ● Trust level assigned based on risk analysis by Application Owner. 	N/A
Application Owner	An Access Authoriser who has been identified as the owner of an application.	Deemed application owner	<ul style="list-style-type: none"> ● Perform risk analysis to determine the trust level for their application. ● Request new security and business roles; ● Authorise access to all users (regardless of the organisation they belong to); ● Delegate the role of an Access Authoriser or Role Authoriser roles.
Organisation	<ul style="list-style-type: none"> ● Government Agency, Tertiary Education Organisation and Education Providers. ● The organisation that supplies online services. 	Provider of online services.	N/A

10.2. Appendix B – Identity Objectives described in the DIA Standard

Identity Objectives...	Determines...
A	Identity exists (i.e. that the identity is not fictitious).
B	Identity is living.
C	The person is linked to the identity.
D	A level of confidence that the person is the sole claimant of the identity for the services requested.
E	A level of confidence of the presenter's use of the identity in the community.
N	A level of confidence of the legitimate use of the presented name. Demonstrated by Marriage Certificate, Change of Name by Deed Poll.

10.3. Appendix C - ESAA Trust Level Relationship with EOI Objectives

Trust Level Objectives for...	Satisfies EOI Objectives...
Trust Level 1	<ul style="list-style-type: none"> • Identity exists (objective A) • Presenter is the sole claimant of the identity (objective D) • The presenter uses the identity (objective E)
Trust Level 2	<ul style="list-style-type: none"> • Identity exists (objective A) • Presenter is the sole claimant of the identity (objective D) • The presenter uses the identity (objective E) • The presenter 'links' to the identity (objective C)
Trust Level 3	<ul style="list-style-type: none"> • Identity exists (objective A) • Identity is a living identity (objective B) • The presenter 'links' to the identity (objective C) • Presenter is the sole claimant of the identity (objective D) • The presenter uses the identity (objective E)

10.4. Appendix D – User Setup and Access Request Form

Available from www.steo.govt.nz

10.5. Appendix E – Authoriser Setup Form

Available from www.steo.govt.nz

10.6. Appendix F – Overview of MoE Operational Security Policy

Security Controls documented in MoE Operational Security Policy ...	Objectives ...
Physical and environmental	Mitigate risk to computer hardware and software that may arise from adverse environmental impacts or unauthorised physical access.
Configuration management	Ensure that all components of the IT infrastructure are operated consistently in a secure manner and with best practice as defined by manufacturers. .
Change Control	Manage risks associated with changing business environments and new or updated technologies.
Malicious Content	Protect against risks associated with malicious code.
Network Management	Ensure that electronic information is protected when in transit.
Backup and archive	Protect the availability of systems and data from both accidental and malicious damage from system failure.
Monitoring and Audit	Provide an audit trail of security events
Access Control	Mitigate risk of inappropriate disclosure of electronic information.
Incident Response	Counteract interruptions to day-to-day business activities.

10.7. Appendix G - Conditions of Use

Below are the Conditions of Use described in Section 4 of the User Guide⁸.

These conditions of use apply to your accessing Education Sector online services. Please read them before signing the Acceptance of Conditions for ESAA. You are responsible for reviewing these conditions, and on accessing any Education Sector online service, you are deemed to have agreed to these conditions.

Security

You are responsible for ensuring that you use your access to ESAA enabled services in a manner which does not contravene theirs, or ESAA's security policies. Further, you agree that you will:

- Take all reasonable steps to prevent someone misusing or gaining unauthorised access to your computer system.
- Ensure your computer system has appropriate anti virus software installed.

Privacy

ESAA complies with the Privacy Act 1993 and is committed to respecting the personal privacy of individuals who use Education Sector online services. You agree:

- We can collect information about the ways in which you use ESAA. We will ask you for this information or we will obtain it from our records.
- All information you give is correct and complete.
- We may monitor / record calls made between you and the Tertiary helpline to maintain and improve the quality of ESAA.

You may ask to see information that we have about you and you may ask us to correct any errors. We will hold the information securely and will not disclose it to any person or organisation without your authority, unless required or authorised to do so by law.

Disclaimer

The Education Sector, while making reasonable efforts to ensure the accuracy and completeness of information and material, assumes no responsibility for the accuracy, reliability or completeness of that information or material. In addition, the Education Sector is entitled at any time, without prior notice, to change the conditions of use for accessing online services.

Your Responsibilities

You have an important role to play in the secure use of online services. You are responsible for your own behaviour when accessing online services. The following outlines rules and recommendations for online service use, password construction and management and challenge response guidelines.

General Use

- You must not send frivolous, obscene or defamatory messages.
- You must not look at, change, delete or tamper with files or programmes that you are not authorised to access.

Passwords

A password within ESAA must:

- Have a minimum of 7 characters, and
- Contain 3 of the following – Lowercase, Uppercase, Digits, Punctuation, and Special character.
- Be changed regularly.
- Be easily remembered, but difficult to guess.

You must not:

- Write passwords on sticky notes, desk pads, calendars, or store online.
- Share your user name and password with another person.

Challenge Responses

The first time you logon to Education Sector online services you are required to set challenge response questions and answers. Challenge responses allow you to uniquely identify yourself and change your own password online should you forget it.

⁸ www.steo.govt.nz

You must not:

- Reveal your password or challenge response answers to any other person.

You will never be asked for your password or challenge response answers by a legitimate ESAA administrator.

Breach of Conditions of Use

Any breach of the conditions of use, which you signed to on registration, will be dealt with appropriate to the seriousness of the breach.

Access to online services will normally be revoked during this investigative period and each incident will be considered on a case-by-case basis.

Minors

If you are under 18 you are encouraged to seek advice before accepting these conditions. Please do not accept these conditions if you do not understand any part of them.

These conditions are considered to be fair and reasonable. Should any of the conditions of use not be considered 'fair and reasonable', the condition will be reviewed and possibly amended to reflect the original intention.

In some circumstances the parents, legal guardians or employer of minors (those under 18 years of age) will also be asked to sign the Acceptance of Conditions of Use alongside the person wishing to have access to online services. The parent, legal guardian or employer of the minor, will then also be responsible for ensuring that the conditions of use are adhered to.