Policy and Procedures -

Memorandum of

Agreement

**Technical Conditions of Use**

**Draft 4**

***Premise****: If schools share private data in any way there needs to be a code of technical conduct. This is that document of understanding.  
It is expected that a MoE will be published at some time that will replace this document.*

*This document should be as a goal rather than a perfect implementation document.*

Tel +64 4 499 2267 // Fax +64 4 499 5596 // info@catalyst.net.nz // www.catalyst.net.nz

**1: General**

This document is considered to be part the Loop contract between schools and the Loop.  
1.1: This document is often called a Loop Network Acceptable Use Policy (LAUP)

1.2: In the event of a dispute the main School-Loop contract takes precedence over this Technical responsibilities document.

1.3: All material of an offensive and illegal manner (e.g. Copyright restrictions) is strictly prohibited from being imported, stored, viewed or distributed via the Loop's resources.

1.4: The authoritative primary source for End User credentials will be the individual

Schools user Directory Systems. If this is not available then the Loop’s User Directory Systems will be used.

1.5: In order for a service or provider to ‘Trust’ both the school and/or the Loop they must be assured that both are utilising good practice. Good practice in relation to the configuration, operation and security of the schools network system.

**2. Responsibilities**

**2.1. Identity Provider Service** (the service the Loop provides)

**2.1.1. Encryption**

All communication (SSO/UDI/IAM) is carried out over HTTPS/SSL/TLS

**2.1.2. Single Sign On – Access and Trust Policy**

2.1.2.1. Identity and Access management (IAM) in the Loop is based on the devolution of the authentication responsibility to the schools. The Authentication of the user is performed at the schools user directories. Once a user is authenticated as a valid user, the Attribute Release containing the user credentials is trusted throughout the Federation.

2.1.2.2. The Loop's IAM service is responsible for the Single Sign On (SSO) service which manages authentication and authorisation queries that is communicated with the schools user directory.

2.1.2.1. The SSO Service will also manage the 'Where Are You From' (WAYF) protocol to identify the school that the User is to be authenticated from.

2.1.2.2. Multi user sessions (aka multiple users) are permitted (aka multiple users) … although service providers may apply their own restrictions.

2.1.2.5. Each Access Release token has an expiry time of 24 hours.

2.1.2.6. A separate unique user access name will be issued by the school if the user has a different concurrent role. (Aka schools will require multiple identities for users **IF** they have different roles within the school)

2.1.2.7: A user working from different schools will have separate unique user access name for each school.

2.2.2.8 The expectation is that this process will be managed via the SMS or ‘Black box”. The expectation is that when a user is added, suspended or deleted via the SMS or Blackbox then it will become effective within 30 mins.

**2.2. Identity Management Expectations**

**2.2.1. Authentication - Authoritative Source**

2.2.1.1. The primary authoritative source for user credentials will be the schools network User Directory Systems. The secondary source shall be the Loops network user directory system.

2.2.1.2. User credentials and attributes must be promptly kept current and accurate.

2.2.1.3. The school must ensure that sufficient logging information is retained so that a particular End User can be associated with a given session.

**2.2.2. Identity Authentication**

2.2.2.1. User accounts must be unique for the organisation.

2.2.2.2. User who is no longer permitted access and privileges to the schools network system must have their access revoked (locked) promptly.

2.2.2.3. User accounts should not be re-issued for at least 24 months.

**2.2.2.3 Granting Access and Identity Establishment**

2.2.2.3.1. Schools should have a documented process for vetting users and issuing credentials to Service Providers' services or resources.

2.2.2.3.2 Schools must use reasonable endeavours to teach users how to use their credentials safely and securely.

2.2.2.3.3 All user records in the schools user directory should be reviewed and updated annually.

.

**2.2.4. Login Password**

Password allocation and management is the responsibility of the school with the following expectations ...

a) Passwords are to be no less than 8 characters and no more than 16 characters, and must include a minimum of 2 digits and 2 letters;

b) Passwords must not be dictionary words.

c) A *Prohibited Password List* is to be applied.

d) Force password changes at least after 1 term.

e) Force new users to re-enter password on first login.

f) Access is locked after 3 failed login attempts.

g) User name must not be pre filled.

h) Passwords should not be saved on client machines or browser clients;

i) User name to be displayed on entry, and password entry to be non display.

j) Last login date and time should be displayed after password verification.

k) Passwords kept in a file for verifying the authenticity of the user must be encrypted.

**2.3 Security Expectations**

The following are guidelines for data, software and environment security that all Participants need to consider in their ICT infrastructure plans and policies.

**2.3.1. Data**

**2.3.1.1. Malicious Software**

2.3.1.2 All media and email must be scanned for malicious software such as viruses and spyware.  
2.3.1.2. It is encouraged that cryptographic controls and digital signatures be used during data exchanges, particularly over the internet and email.

2.3.1.3 Encryption should be used where applications support it and there is no degradation of service delivery.

**2.3.2 Software**

2.3.2.1. Apply secure networks and firewalls. Implement appropriate network management controls and policies.

2.3.2.2. Ensure latest updates to anti-malware software.

2.3.2.3 Apply user network connection closure after 1 hour of inactivity.

2.3.2.4. Allow only approved software to be installed on the servers.

**2.3.3 Physical Environment**

2.3.3.1. Secure physical access to servers to authorised personnel only.

2.3.3.3. Access rights to terminated staff to be removed immediately.

2.3.3.4. Access rights to restricted areas to be reviewed regularly.

**2.3.4. Disaster Recovery**

2.3.4.1. Servers must have an uninterrupted power supply (UPS).

2.3.4.2. Backup of applications and user directories to be done regularly and rotated.

2.3.4.3 Ensure off site backup storage for monthly backup media.

2.3.4.4. A Disaster Recovery plan must be documented and known to authorised personnel.

**2.4 SMS Expectations** <<under development>>

**2.4.1. Encryption**

All communication is carried out over ...

**2.4.2. SMS – Access and Trust Policy**

**2.5 Parental Portal Expectations** <<under development>>

**2.51. Encryption**

All communication is carried out over ...

**2.5.2. Parental Portal – Access and Trust Policy** <<under development>>