WENTWORTH
INSTITUTE

Document:	**Records Management and Security Procedure**	
Approved by: Executive Management Team	**Version:** 1.3	**Date:** 29.3.2016

1. Overview

Senior management of Wentworth Institute ("WIN") have a legal responsibility to protect the organisation's physical and electronic records (including IT infrastructure) and the information WIN holds.

The creating, securing and retention of records is part of WIN's overall knowledge management system.

WIN keeps records to:

- provide an historical record of WIN's operations, activities and decision-making;
- provide evidence of business transactions and decisions, for purposes of accountability;
- enable WIN to find the right information easily and comprehensively;
- identify areas for improvement and/or expansion;
- enable WIN to meet its legal and regulatory requirements for data management and reporting.

2. Types of records

2.1 Student records

A separate paper-based file is created for each student and an electronic record is also created in the student database *RTOManager*. The paper and electronic student files combined are known as the "student record".

The Registrar maintains student records.

The student record contains as a minimum:

- the completed *Application Form;*
- enrolment details;
- any agreement with the student;
- any information relating to request for, and granting of, advanced standing or credit;
- results for each assessment event in a subject;
- the final mark and grade for each subject;
- details of payments and refunds;
- copies of testamurs and academic transcripts issued;
- any notes made by the academic /administrative staff about the student (including any disciplinary matters, requests, correspondence and grievances).

The entire student record is maintained for a period of at least 2 years from graduation (or when the student otherwise ceases to be a student).

Financial records relating to a student are kept for a minimum of 7 years.

Student results for each subject are retained indefinitely to enable the re-issue of a qualification and transcript if required.

In the event of WIN's closure, student records will be transferred to TEQSA, or as prescribed by regulation.

Students may access information on their files as per the *Privacy and Personal Information Procedures*.

Third party access is only permitted when required by law or with the express permission of the student (as outlined in the *Privacy and Personal Information Procedures)*.

2.2 Staff records

The Finance Manager maintains staff records.

Each staff member has a file created and maintained for the purpose of archiving:

- recruitment paperwork;
- employment conditions / letter of offer / employment agreement;
- position description
- evidence of participation in the staff induction process;
- certified copies of qualifications claimed;
- verification of experience;
- professional development activity.

Original documentation must be sighted to verify the authenticity of qualifications. Copies on file must indicate the date sighted and by whom (refer *Staff Recruitment, Induction, Professional Development, Appraisal and Promotion Policy & Procedure*, section 2.5).

Disciplinary action or details of grievances in which the staff member is a respondent may also be noted in the staff file.

Staff may access information on their files on request to the Finance Manager.

Third party access is only permitted when required by law or with the express permission of the relevant staff member.

2.3 Financial records

The Finance Manager maintains financial records.

Financial records are maintained on MYOB.

Financial records are created, secured, archived and retained consistent with contractual and legal requirements.

Financial and contractual records must be kept for a minimum of 7 years.

3. Record security and access

WIN takes seriously its obligations under privacy legislation to safeguard all confidential information. WIN will also ensure that anyone acting on its behalf maintains appropriate confidentiality. As such, it is a requirement that records are held in a secure environment and safeguarded against loss, damage or unauthorised access. Only authorised staff will be granted access to student and staff records.

This section should be read in conjunction with WIN's *Privacy and Personal Information Procedures.*

3.1 Physical records

Physical records are kept in secure areas or locked filing cabinets and access is only available to authorised personnel.

3.2 Electronic records

WIN has its own server and maintains a secure computer network. Each user has their own password which allows them access to appropriate functions and files within the system.

The IT Manager is responsible for the restriction of access to and security of electronic records.

4. Version management

In the interests of enhancing knowledge management, WIN has implemented a system for managing the versions of certain documents - refer section 4.4 of the *Quality Assurance Framework*.

5. Record retention and disposal

Records will be retained and secured according to the following retention periods:

- General business records (including financial records): 7 years.
- Student records: 2 years after the student ceases to be a student except for enough data to re-issue a qualification and transcript to be kept in perpetuity.
- Staff records: 5 years after the staff member ceases to be a staff member.

6. Security of electronic data

The breakdown of key IT infrastructure, either by mechanical means or human intervention can become a critical incident if proper safeguards are not put in place to ameliorate the impact of such a breakdown.

6.1 Preventions against data loss

In relation to IT Infrastructure WIN ensures that the following preventions are implemented:

- External backup: a Microsoft Windows Server Backup program for each server backup into a dedicated Seagate Expansion Desktop USB Drive. The server backup includes the image of the server OS, user data, system state and system registry details. This is performed Monday, Tuesday, Wednesday, Thursday and Friday;

- Each server has RAID 1 redundancy setup on System OS drive and Raid 5 redundancy on Data drive to prevent loss of data in the event of hard drive failure;
- Off site backup each Friday to two separate USB hard drives to be taken offsite by CEO and IT manager;
- Systems to be backed up include but are not limited to:
  - file server
  - mail server
  - production web server
  - domain controllers
  - test web server
- Backup testing monthly (includes user data stored on the hard drive, system state data and the registry);
- The ability to restore data from backups is tested at least once per quarter;
- Monthly full backups using a separate monthly backup drive which is kept at the CEO's home.
- Surge protectors are employed to minimise the effect of power surges on electronic equipment;
- Servers and essential equipment are protected with an Uninterruptible Power Supply (UPS);
- An effective alarm system and accessible fire extinguishers are installed in the case of a fire;
- Anti-virus software, firewalls and other security measures are employed;
- Archives are made at the end of every December;
-
- User account data associated with the file and mail servers are archived two months after a staff member has left WIN.

.

The computer network is maintained by a programmed regimen of maintenance by the IT Manager who is well qualified to undertake this task.

6.2 Security safeguards

6.2.1 Protection against in-house intrusions includes:

- Wireless LAN, password encrypted WPA method, changed regularly.
- All internet in and out filtered by proxy server, and monitored.
- Bandwidth control - distributed to each client PC, speed modulated according to needs.
- Locked server room.
- Access to the server room is prohibited without permission from the IT Manager.
- Security cameras on all floors.

6.2.2 Protection against external intrusions includes:

- Installation of anti-virus on each server, with regular updates.
- All servers and client PC's are firewalled.
- Firewall enabled routers and network equipment.
- All staff and students have a WIN email address.

If there is any specific threat or intrusion of any kind or attack from external sources, it can be tracked and recorded by the proxy server and webserver for the IP address. Such attacks be investigated further and action will be taken.

6.2.3 In the case that equipment is damaged or data is compromised:

- There are backups of data, software and hardware.
- There are several servers that connect to each other and are able to replicate automatically. Student database; user account details, and server information will be shared automatically amongst the servers, in case one is down, the other will take over.
- Disaster recovery is planned & implemented for the client-server environment.