SHERIDAN
INSTITUTE OF HIGHER EDUCATION

Information Management Policy Handbook

Comprising the following policies:

1. *Use of Personal Information Policy*
2. *Information Quality Policy*
3. *Security of Information Policy*
4. *Organisational Records Management Policy*
5. *Acceptable Use of Information and Communications Technology Policy*
6. *Electronic Learning Management System Policy*

Policy Area: Information Management

Approval: Principal

Signature: Date:

TABLE OF CONTENTS

HANDBOOK INTRODUCTION

1. PURPOSE & PRINCIPLES

This Information Management Policy (IMP) Handbook is a set of policies brought together to set minimum standards and policy direction in relation to confidentiality, integrity availability and the management of risk relating to information. The handbook should be treated as a 'living document' which will be reviewed often,as advances in information and communications technology can quickly render current practice out of date.

The Principal and the Australian Baptist Education Inc (ABE) Director of Information and Communications Technology (ICT) are responsible for:

- monitoring, maintaining and improving compliance with appropriate legal and regulatory requirements.
- developing, maintaining and monitoring the integrity of information to ensure that it is of sufficient quality for use within the purposes it was collected.
- developing appropriate resilience and recovery arrangements for systems, based on assessed risks to information and its perceived value, to ensure that availability of information is not compromised.
- Acquisition and development of new ICT resources.
- educating and continually raising awareness of all staff about the issues and impacts related to failing to manage information and the consequent responsibilities they have.
- pro-actively monitoring and reducing risks to information.

2. SCOPE AND MANAGEMENT FRAMEWORK

This Handbook covers all aspects of information, including, but not limited to:

- Personal information including student, staff and researcher information
- Organisational information

This Handbook covers all aspects of *handling* information, including but not limited to:

- Information held in structured record systems (paper & electronic)
- Transmission of information (fax, email, post, telephone, skype, instant messaging, social media)
- Retention and disposal of information
- Staff conduct relating to the use of information in any form

The Handbook covers all information held, created or accessed by employed staff, or any other party, performing activities in conjunction with the business of the organisation.

Audience

The IMP Handbook is a compilation of policies. The Handbook is not designed for all staff to read and be familiar with. It is designed for managers to read and reference.

The Handbook has been broken into individual policies so managers can identify and read the sections most relevant to them.

The policy sections are as follows:

- **Use of Personal Information Policy** – This generally relates to managers of front line staff who handle identifiable information on a day to day basis and covers the requirements to comply with the duty of confidentiality, including situations where confidentiality can be breached legally.
- **Information Quality Policy** – This sets out the principles relating to the collection of information to ensure that information is complete, accurate, relevant and timely. Managers involved in service re-design/improvement or review should use these principles when considering the information requirements.
- **Securing Information Policy** – Whilst the 'physical' security aspects are everyone's responsibility to adhere to, this section is set out for those working on system design, implementation and management, covering all aspects ranging from physical location of equipment/information storage through to planning system capacity. This is clearly the technical element of the Handbook, designed for IT managers/Senior IT staff.
- **Management of Organisational Records** – This sets core policy for creation, storage and disposal of organisational records and links very much to the corporate/records management function of an organisation. There are also policy statements relating to IT services with regard to electronic document storage.
- **Acceptable Use of Information and Communication Technology** – This sets out policy on the use of phone, email, fax, skype, instant messaging and social media by all staff. It is therefore a key element for line managers to ensure their staff are acting correctly.

A. Information risk management 'policy'

The approach to information risk is built in where relevant to the IMP. As an overview the key risks are covered as follows:

- Inappropriate disclosure of data by staff – Use of Personal Information policy.
- Action taken based on inaccurate data – Information Quality policy.
- Loss of information – Security of Information policy.
- Alteration of data – Information Quality, Security and Acceptable Use of Systems policies.
- Destruction of data – Security of Information, Records Management and Acceptable Use of Systems policies.

B. Responsibilities for information management

Primary responsibility for information management

The Principal is the senior accountable officer for the enforcement of the policy. The Principal is supported by the Director of ICT.

Information management responsibilities in other roles

Information System management

Each information system is overseen by the Director of ICT. The role of the manager is to implement the system-related processes that govern:

- management of access to the system
- audit of user activity
- system data validation processes (input, internal & output)
- system administration & supplier support (where applicable)

The Director may recommend to the Principal the delegation of some aspects of information management to a member of staff who shall be identified as the manager of that information.

Physical security responsibilities

The operation of general physical security such as door locks, entry controls will be the responsibility of **all staff** as it relates to all assets, not just information assets. Assessment and promotion of physical security is the responsibility of the Principal.

Line managers will be responsible for:

- Managing requests for access to systems, by authenticating the roles and access requirements of staff.
- Ensuring staff are educated and aware of their responsibilities.
- Monitoring staff compliance with policies.
- Liaison with the Principal and the Director of ICT when developing or amending processes for handling information.

The Principal has responsibility to ensure:

- Management of staff personal data.
- Identity checks for new staff .
- Ensuring staff are aware of and attend a training that includes core information management education.

The Principal may delegate some or all of these roles to a member of staff (such as an HR Director).

Academic & Operational Governance

Key staff in these areas are responsible for facilitating the requirements of information management policies in their areas and ensuring that requirements are practical within the context of academic services and operational activities.

Risk Management

The Principal and Director of ICT are responsible for ensuring that any incident/weakness and risk related to information is not considered in isolation and is an integral part of Sheridan's approach to risk management and that, where required, expert support of the administration is engaged to advise on incidents.

Review and update of information management policies:

The Board of Directors will schedule a regular review of Information Management Policies.

Reviews may also be initiated as a result of the following occurrences:

- Major policy breach within the community
- Identification of new threats or vulnerabilities
- Significant organisational restructuring
- Significant change in technical infrastructure

C. Incident management

Reporting incidents and near misses

Any incident, near miss or potential weakness in processes relating to the use of information, such as a breach of confidentiality or mistake due to inaccurate or unavailable information, will be reported via Sheridan's overall 'incident reporting' process. Staff will be informed via education sessions. Information management will be integrated with the incident reporting and risk management process, so as to identify the information related components of any incidents or near misses.

Reporting technical/software failures

If a user is unable to access information due to a system related issue this should be reported to the ABE IT helpdesk for resolution. In addition, if a system-related issue puts either service user care or organisational safety at notable risk then it should also be reported via the 'incident reporting' process.

Learning from incidents

Changes determined as a result of an incident, near miss or weakness will be communicated to relevant staff as part of the process to manage the incident. This may include team briefings, newsletters and/or education programmes.

Investigating misuse of systems (including forensic readiness)

If misuse of systems by students is suspected, the IT Department will be contacted at the earliest opportunity and will determine if there is a need to preserve electronic evidence.

If misuse of systems by staff or researchers is suspected, the Principal or the Director of ICT will be contacted at the earliest opportunity and will in conjunction with the IT Department, determine if there is a need to preserve electronic evidence.

Specialist forensic IT support may be engaged in any situation where illegal activity is suspected.

Disciplinary process and removal of access rights

Any investigation which determines that organisational policy has not been followed will be subject to Sheridan's formal corrective and termination policy. Access to systems for staff under investigation or disciplinary process may be suspended on the request of the Principal in consultation with the Director of ICT. Separate legal proceedings may also be necessary.

Where evidence is required for internal or external support of action against an individual, the processes for collection will incorporate the following minimum standards:

- Retrieval of paper information will note who withdrew it, when it was withdrawn and incorporate procedure to ensure it is not tampered with. For example the use of an

academic or personnel record in investigation will record who requested and received the record, any copies of the original that were made, and who witnessed this activity.
- Electronic audit trails will be examined where possible to provide evidence.
- Depending on the severity of the issue specialist computer forensic support may be engaged.

D. Information classification

Information will be classified in one of three categories:

Personally identifiable - Where the information relates to one or more identifiable individuals to a greater or lesser extent. The same principles will be applied to information on deceased individuals. Some personally identifiable data may be disclosable under freedom of information legislation, however no such information will be published or provided without first checking relevant exemptions.

Public information – Information that is not 'personally identifiable' is generally accessible and either actively published or provided on request. By default all 'non personal' records will be classed as public. However if senior staff responsible for any information have reasonable concerns about the publication or provision of information, then a considered view will be taken as to whether the information should be classed as organisationally sensitive.

Organisationally sensitive – This classification will only be used for information that can be justified as exempt from freedom of information legislation. Any information determined as 'sensitive' will not be routinely published but, if requested, the validity of the classification should be checked. This may include financial information, procurement documents (particularly those where disclosure could affect the process or commercial interests of parties) and draft public policy. The sensitivity is likely to be time limited. Responsibility for classification of information into these categories lies with the originator or owner.

Confidentiality

Student records and staff personnel information on any media will be routinely treated as **confidential**. Corporate records will be deemed public unless labelled.

3. Appendix: Document History and Version Control

Document Title:	Information Management Policy Handbook
Source Documents:	In the formation of this policy, Sheridan directly sourced ideas and phrasing from the publications listed below:

- *Australian College of Theology, Handbook for Registrars, Teachers, Moderators and Examiners*, 9th ed., 2010.
- *Curtin University Record-keeping Plan* 2008. Retrieved 31st January 2011 from http://uim/local/docs/secure/curtin_recordkeepingplan.pdf
- *George Washington University, Records Management Policy* 2004. Retrieved 5th May 2011 from

http://my.gwu.edu/files/policies/RecordRetentionINTERIM.pdf

- *Government of South Australia, Records Management Disaster Planning Toolkit*. Retrieved 5th May 2011 from http://www.archives.sa.gov.au/files/management_guidelines_ARM_disastertoolkit.pdf
- N*HS South Gloucestershire Information Governance Management System*, March 2010. Retrieved 5th May 2011 from http://www.sglos-pct.nhs.uk/informationgovernance/Information%20Governance%20Policies%20_IGMS_%20v3%201%20final%20nov%202009%20s%20glos.pdf
- *UTS Records Management Plan Template*, University Records, Governance Support. Retrieved 5th May 2011 from www.**records**.**uts**.edu.au/forms/**records**-**management**-plan.docx

Associated Internal Documents:

Associated External Documents

Authorised Officer: Chairperson, Board of Directors

Approved by: Mr Michael Smith

Date of Approval: 11 Mar 2020

Date of Next Review: Mar 2021

Version Number	Version Date	Authorised Officer	Amendment Details
1.00	30 May 2011	N/A	Draft prepared for Sheridan College and Vose College of Higher Education
2.00	30 May 2011	N/A	Revised for Sheridan College
2.10	02 Mar 2013	Chairperson, Board of Directors	Submitted to TEQSA for Sheridan College HEP registration: Attachment 7.5a
3.00	18 Mar 2020	Chairperson, Board of Directors	Updated during policy review

[PAGE LEFT BLANK
INTENTIONALLY]

SHERIDAN COLLEGE
PERTH | WESTERN AUSTRALIA

Use of Personal Information Policy

Legal compliance and core staff responsibilities with regard to information use

Policy Area: Information Management

Approval: Chairperson, Board of Directors

Signature: Date:

USE OF PERSONAL INFORMATION POLICY

1. MANAGING PERSONAL INFORMATION – LEGAL COMPLIANCE

The following forms of organisational record need to be securely retained for statutory or regulatory requirements, including defence against potential civil or criminal action.

- Student records
- Staff records (employment contracts, staff reviews etc)
- Financial records (orders, receipts, invoices etc)
- Public accountability records (board minutes, papers etc)

Many records will be required to be kept for a number of years, therefore Sheridan will ensure that technology change does not make important records inaccessible. This will be either by maintaining relevant technical standards, or by the transfer of data at the relevant time to new technology and media.

A. Principles governing protection of personal information

All processing of personally identifiable information must be considered in line with the tests and principles below:

a. Necessity test – The first consideration given to any collection, recording or sharing of information will be whether the individual(s) need to be identified and what data needs to be used. If no identifying information is required, then none should be used. All items of data used must be justifiable. It maybe necessary to 'pseudonymise' data by replacing clear identifiers with a code or reference number that allows data to be linked.

b. Use of information shall be fair and lawful.

c. Personal data shall be obtained only for specified and lawful purposes, and shall not be used for other purposes that the individual is unaware of.

d. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

e. Personal data shall be accurate and where necessary kept up to date.

f. Personal data shall be processed in accordance with the relevant legal provisions.

g. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental destruction of, or damage to, personal data.

h. Personal data should not be transferred to a country or territory outside the economic area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

2. Employment Confidentiality Agreements and Job Description Responsibilities

A standard statement on responsibilities for handling information appropriately will be included in all job descriptions and employment contracts.

It should be noted these responsibilities are required in perpetuity beyond the length of the staff member's employment. Terms and conditions will also state the responsibilities extend to all places and all times, including outside the work environment.

Staff not directly employed by Sheridan

Casual staff, contractors and others, (including volunteers), not covered by an employment contract, are required to enter into a confidentiality agreement prior to being given access to information processing facilities. All such staff will be informed about the need and method for maintaining confidentiality; regardless of what access their role gives them to information.

3. Core Responsibilities of Staff

This section briefly outlines the responsibilities for all staff with regard to handling information to ensure information is handled appropriately.

- Inform service users what information they are recording, why it is being used, who has access and who it will be shared with during the course of their education.
- Inform students, staff and researchers about how information is used generally at Sheridan.
- Address any concerns service users may have about the use of their information.
- Liaise with department managers and the Academic Principal when service users make requests to restrict the use of their information.
- Protect student, staff and researcher information when using communication methods.
- Share information appropriately and legally.
- Staff will not extract or use personal data unless necessary.
- Ensure that confidential information is not left lying around when unattended. Paper and computer media should be stored in suitable lockable cabinets when not in use. Sensitive information on removable media and portable devices must be secured through one or more restricted access technologies.
- Maintain and follow processes required to ensure accuracy, completeness and timeliness of information. (see section 4).
- Protect electronic information by:
    a. Keeping passwords confidential
    b. Avoid keeping records of passwords

c. Change passwords if you think someone else knows it
d. Select passwords that are easy to remember, but not based on anything easy to guess.
e. Change passwords at first log on as appropriate.
f. Unattended personal computers and terminals should configured with security mechanisms to prevent unauthorised access.
g. Ensure that only individuals who need to know information can see it on either a desk or a screen (i.e. Not have screens visible to the public, not display details of other service users during consultations etc).

Given the public nature of the education environment, these policy elements are crucial to the appropriate handling of information. Failures of these policies in areas open to the public will by their nature be public. The impact of an incident may have serious implications for the organisation and even the well being of individuals.

4. Education and Awareness

The Principal will ensure that all staff receive appropriate education about handling information via the following programme of provision:

Induction – The organisation will ensure that all newly employed staff receive basic guidance in organisational policy in relation to information governance as part of an overall organisational induction.

Regular 'Essentials' update training for any staff member – The Principal, or designated staff member, will provide a form of annual update for all staff. As a baseline all staff will attend a detailed information management course every two years, with interim activities supplementing as the annual update.

Fundamentals – Where it is identified a member of staff needs more education following from induction a detailed fundamentals course is provided.

System training – All user training on systems will include details and education on appropriate policy and procedure elements for that system. These will focus on both security and data quality elements.

Individual development – Where as a result of a performance review, a member of staff requires more detailed training, this may be negotiated with the Principal.

Awareness activities – newsletter articles, workshops, leaflets, posters and other awareness materials will be used to ensure all staff are kept aware of their responsibilities.

5. Appendix: Document History and Version Control

Document Title:	Use of Personal Information Policy
Source Documents:	In the formation of this policy, Sheridan directly sourced ideas and phrasing from the publications listed below: ▪ *Australian College of Theology, Handbook for Registrars, Teachers, Moderators and Examiners*, 9th ed., 2010.

- *Curtin University Record-keeping Plan* 2008. Retrieved 31st January 2011 from http://uim/local/docs/secure/curtin_recordkeepingplan.pdf
- *George Washington University, Records Management Policy* 2004. Retrieved 5th May 2011 from http://my.gwu.edu/files/policies/RecordRetentionINTERIM.pdf
- *Government of South Australia, Records Management Disaster Planning Toolkit*. Retrieved 5th May 2011 from http://www.archives.sa.gov.au/files/management_guidelines_ARM_disastertoolkit.pdf
- N*HS South Gloucestershire Information Governance Management System*, March 2010. Retrieved 5th May 2011 from http://www.sglos-pct.nhs.uk/informationgovernance/Information%20Governance%20Policies%20_IGMS_%20v3%201%20final%20nov%202009%20s%20glos.pdf
- *UTS Records Management Plan Template*, University Records, Governance Support. Retrieved 5th May 2011 from
- www.**records**.**uts**.edu.au/forms/**records**-**management**-plan.docx

Associated Internal Documents:

Associated External Documents

Authorised Officer: Chairperson, Board of Directors

Approved by: Mr Michael Smith

Date of Approval: 11 Mar 2020

Date of Next Review: Mar 2021

Version Number	Version Date	Authorised Officer	Amendment Details
1.00	30 May 2011	N/A	Draft prepared for Sheridan College and Vose College of Higher Education
2.00	30 May 2011	N/A	Revised for Sheridan College
2.10	02 Mar 2013	Chairperson, Board of Directors	Submitted to TEQSA for Sheridan College HEP registration: Attachment 7.5a
3.00	18 Mar 2020	Chairperson, Board of Directors	Policy review for Board of Directors

SHERIDAN COLLEGE
PERTH | WESTERN AUSTRALIA

Information Quality Policy

Principles for complete, accurate, relevant and timely information

Policy Area: Information Management

Approval: Chairperson, Board of Directors

Signature: Date:

INFORMATION QUALITY POLICY

Principles for complete, accurate, relevant and timely information.

1. REQUIREMENTS FOR QUALITY INFORMATION

Sheridan shall operate policy and processes to ensure that information is of good 'quality'. Quality is defined as information that is 'complete, accurate, relevant, available and timely'.

2. COLLECTION OF INFORMATION

Data collection processes (electronic and paper) will have rule-based data input designed into them along the following guidelines:

- *Value ranges* – Where software and systems permit, acceptable ranges will be indicated on paper forms and built into systems so that only values within the determined range will be accepted.
- *Invalid characters* – Paper collection forms will indicate where the required collection is either numeric or character based. Staff will ensure that data collection fields are correctly filled out.
- *Missing or incomplete data* – Paper forms will indicate where items of data must be completed in relation to the collection purpose of the form. Electronic systems will feature rules (that may allow local configuration) that indicate to users when required data items have not been completed before data can be saved.
- *Identifiers* – A Student Number will be used as the common identifier on all student records and correspondence. The organisation will ensure processes around data collection and transfer, capture and use the student number. Local identifiers are permitted.

Each entry system will have a checklist of core processes for data collection that is linked to training guides. These will be reviewed periodically or as a need arises via feedback/quality monitoring and incidents. These will be based on the feedback process managed by the Academic Principal, covering items such as registering and amending student details, attendance and outcomes, removal of students and general management.

Responsibility for review and development of input/collection validation will by default lie with the relevant information manager.

Line managers of staff will have default responsibility to ensure their staff are aware of processes and procedures relating to the quality of data.

3. Rule-Based Processing of Information

This control generally applies to electronic systems and relates to any 'automated' process that takes inputted data and processes it into another form, such as creating a result from a calculation run on two data fields.

Elements of an information system that run an internal process on data will be specified in developments and tested before system acceptance. Checks will be run as part of change control and system acceptance procedures when system developments affect any of the internal processing.

Standard system reports or processes will be checked so that if they have a running order this is maintained.

4. Authenticating Data (on Systems, and in Messages)

Data items in paper format will be subject to rules and guidelines detailed in student record policies and procedures for ensuring identification of the author. Typically reliance is on a dated signature of staff completing forms or records.

Data items in electronic format will be attributed to the User ID recorded in any audit trail relating to the creation, viewing, amendment or deletion of data.

5. Validation of Information Displayed or Extracted

Despite implementation of controls on both data collection/input and internal system processing, data cannot be entirely relied on without further checks on 'output'. For the purpose of this policy output is defined as follows:

- Regular or ad-hoc reports compiled from summary of information on multiple records.
- Viewing and use of individual records (both paper and electronic) for delivery and management of care.

Information analysis staff will be responsible for running regular validation checks on reports. Confirmation of the validity will require input from the system owners.

Typically reports can be validated by comparison with other data/reports.

Use of individual records (paper and electronic) within the delivery and management of care will be checked as part of a regular programme by individual departments.

Staff line managers will have a default responsibility to ensure their employees are familiar with processes/procedures around handling data output, especially with regard to interpretation.

6. Checking Student Details (Demographics)

All departments with direct contact with students will ensure that their administrative processes include checking the detail of student records, such as name, address, date of birth, etc with the students themselves. For example students should be asked to confirm their details when applying for transcripts of marks. At a first appointment, all details must

be checked to ensure that the correct record is selected or created. The majority of details should be checked at other appointments in order to pick up any changes or previous errors.

Students (and others making enquiries) must be asked to confirm demographic details to staff, rather than staff informing them of the details (such as address) and asking if it is correct. This is to ensure that student demographics are not disclosed inappropriately to others (such as ex partners), and that students can choose how to confirm details to staff, if they are perhaps unhappy about informing staff of details verbally in open public areas.

If students express concern about being regularly asked to confirm their details they should be informed that standard checks are in place to ensure that mistakes are not made in relation to their care.

7. APPENDIX: DOCUMENT HISTORY AND VERSION CONTROL

Document Title: Information Quality Policy

Source Documents: In the formation of this policy, Sheridan directly sourced ideas and phrasing from the publications listed below:

- *Australian College of Theology, Handbook for Registrars, Teachers, Moderators and Examiners*, 9th ed., 2010.
- *Curtin University Record-keeping Plan* 2008. Retrieved 31st January 2011 from http://uim/local/docs/secure/curtin_recordkeepingplan.pdf
- *George Washington University, Records Management Policy* 2004. Retrieved 5th May 2011 from http://my.gwu.edu/files/policies/RecordRetentionINTERIM.pdf
- *Government of South Australia, Records Management Disaster Planning Toolkit*. Retrieved 5th May 2011 from http://www.archives.sa.gov.au/files/management_guidelines_ARM_disastertoolkit.pdf
- N*HS South Gloucestershire Information Governance Management System*, March 2010. Retrieved 5th May 2011 from http://www.sglos-pct.nhs.uk/informationgovernance/Information%20Governance%20Policies%20_IGMS_%20v3%201%20final%20nov%202009%20s%20glos.pdf
- *UTS Records Management Plan Template*, University Records, Governance Support. Retrieved 5th May 2011 from
- www.**records**.**uts**.edu.au/forms/**records-management**-plan.docx

Associated Internal Documents:

Associated External Documents

Authorised Officer: Chairperson, Board of Directors

Approved by: Mr Michael Smith

Date of Approval: 11 Mar 2020

Date of Next Review: Mar 2021

Version Number	Version Date	Authorised Officer	Amendment Details
1.00	30 May 2011	N/A	Draft prepared for Sheridan College and Vose College of Higher Education
2.00	30 May 2011	N/A	Revised for Sheridan College
2.10	02 Mar 2013	Chairperson, Board of Directors	Submitted to TEQSA for Sheridan College HEP registration: Attachment 7.5a
3.00	18 Mar 2020	Chairperson, Board of Directors	Policy update for Board of Directors

SHERIDAN
INSTITUTE OF HIGHER EDUCATION

Security of Information Policy

Ensuring appropriate access and availability of information during the development, maintenance and operation of systems

Policy Area: Information Management

Approval: Chairperson, Board of Directors

Signature: Date:

SECURITY OF INFORMATION POLICY (INC. FORENSIC READINESS)

This policy covers a number of aspects, generally defined as 'information security'. The policy sets out provisions to deal with:

- Data loss including inappropriate disclosure on media and permanent loss to the organisation
- Unavailability of data from malicious software and user actions
- System based controls to allow appropriate access to information

1. PHYSICAL & TECHNICAL SECURITY

A. Secure working areas

Open Public area – Areas where the public are allowed to move freely, such as corridors, waiting areas. Security based on general security arrangements, such as staff vigilance. IT equipment will only be placed in these areas if absolutely necessary. Security equipment (cables, cages etc) will be used where equipment may be left unattended.

Any data stored directly on devices in these areas will be secured through one or more restricted access technologies.

Controlled Public area – Areas which the public can be present in, but only following authorised access by staff, such as classrooms and the library. Once within these areas, control over the public is again via staff vigilance. IT equipment will only be placed in these areas if absolutely necessary. Security equipment (cables, cages etc) will be used as appropriate if equipment is to be left unattended at all. Data stored directly on devices in these areas will be secured through one or more restricted access technologies.

Staff only areas – No member of the general public is allowed access, except on special controlled occasions, when they are accompanied at all times by a member of staff. No additional physical security will generally be needed for IT equipment in these areas.

Access restricted areas (access to specific staff only) –Any area designated a restricted access area requires one or more physical security access mechanisms.

All areas - Within any area there should be the facility to protect information assets. Such facilities may be lockable offices or filing cabinets. Use of these facilities within a department should be determined and implemented, including the training of staff.

This should be subject to regular review to ensure adequate protection for the information, but appropriate availability to those that need it, when they need it.

Guidance for departmental evaluation:

- External signage for non-educational buildings, offices and other areas should only give minimum indication of purpose.
- Personal and sensitive information on paper should always be secured in lockable filing cabinets (or similar).
- Doors and windows should be locked when unattended, with external protection considered for windows, particularly at ground level.
- All members of staff should wear ID badges at all times. Visitors should be issued with visitor passes.
- Third party support services should only be granted restricted access to controlled/secure areas, which should be authorised and monitored.
- All data should be stored on the network server. Data is not to be stored on a local terminal unless approved by the IT department. Any personal data stored on a local drive or device must be subject to one or more restricted access technologies.

B. Security, installation & maintenance of equipment

The following guidance points must be considered when positioning equipment and used if possible:

- Computer screens and paper records should be positioned to reduce the risk of overlooking during their use. Screen shields and folders should be routinely used in 'open public' areas.
- Equipment should be sited away from overlooked windows (unless additional window protection is in place).
- Equipment should be sited away from sources of heat, explosion, water, dust and electromagnetic radiation. This includes items such as radiators (heat and water), chemical and gas storage.
- 'Critical' equipment such as servers, network infrastructure should be sited in an appropriately controlled environment, in terms of temperature, humidity and cleanliness.
- Eating & drinking must not be allowed near 'critical' equipment and must be actively discouraged near other equipment. Staff causing damage to equipment may be responsible for the cost of repair or replacement.
- Equipment should only be installed by IT department staff.
- The IT department are responsible for all IT equipment maintenance purchased via their department. They are not responsible for maintenance of personal IT equipment used at Sheridan.

C. Power supplies

Power supply to equipment should be routinely considered in all new installations.

Existing power supply should be regularly reviewed.

Critical systems & infrastructure must be provided with power supply protection.

As a minimum this must be UPS (Uninterruptible Power Supply) for the Server. This is required so that in the event of a power failure, the system can be shut down in an orderly manner, whilst continuity activity (fallback plans) are invoked. UPS equipment must be regularly checked to ensure it has adequate capacity (battery life) and tested in line with the manufacturers recommendations.

For critical systems, consideration should be given to the use, extension or installation of locally generated power. This should be formally risk assessed and documented.

D. Cabling security

Due to the nature of the premises, as with many educational institutions, full implementation of cabling security is not currently possible. The following defines minimum requirements for all installations, and additional minimum requirements for new builds (not new installations into old premises).

Existing premises:

Power and telecommunication lines should be protected by ducting from source to socket(s)

New build premises:

Power and telecommunications lines should be underground/under floor and not routed through public areas, where appropriate.

All installations of power and cabling must be protected from environmental threats.

E. Asset registers & secure disposal of equipment

The IT department will maintain an asset register of all IT equipment, including detail on all purchases and disposals.

A procedure for the identification and processing of equipment that is no longer required for its current function will be implemented. Where equipment is to be reused within another location in the organisation, any data will be erased, using tools that overwrite the data. Should the previous owner have any data stored on the PC as opposed to network storage, they are responsible for ensuring that any data they wish to keep is copied to an appropriate storage facility prior to the overwrite.

Equipment that is to be 'donated' to other organisations (such as charities or recycling schemes) or disposed of, will have the hard disc wiped by the use of overwriting tools,

Sheridan will correctly and safely dispose of equipment. This may require financing the treatment and disposal of items.

F. Protection against malicious software

Sheridan sets the following controls as policy to address the risk of reduced integrity and availability of its information assets:

- All software installed on organisational assets to be appropriately licensed.
- Authorisation must be gained from the IT department prior to acquisition and installation of any software.
- IT dept are responsible for software and systems to prevent, detect and correct threats (such as viruses and malware).
- Procedures for reporting and handling virus attacks & recovering from them to be implemented, including immediate reporting of any suspicion of virus.
- Awareness of malicious 'hoax' attacks and procedure for handling them, including reporting to IT helpdesk.
- Staff awareness of above controls and their responsibilities.

The last bullet is perhaps the most important, as it is staff vigilance that will ensure only licensed software is used and that email attachments are dealt with appropriately.

G. Network management & security

Where possible, responsibility for Sheridan's network should be segregated from responsibility for computer operations. Responsibility of control over Sheridan's network should be formally allocated to the appropriate person within the IT department (typically Computer Services Manager or Network Manager).

The 'network manager' is responsible for implementation of appropriate controls. Network service security in the organisation will be fully documented, reviewed and updated. Routing controls based on positive source and destination address checking should be implemented where possible.

Users will only be provided with direct access to the services that they have been specifically authorised to use. Access to services will, by default, be covered by the user registration control for access to systems, (see section 2).

2. Access Control

A. User access control & management

Controlling access to information is one of the key elements of organisational compliance with relevant legislation.

System access control policy statements:

The following statements are the rules that will be applied to controlling access to any information system within the organisation, by employed staff and third parties.

Line managers must ensure that due consideration is given to application of controls detailed below by appropriate staff.

- Access to systems and information on a need to use and need to know basis.
- Access controls will be based on user roles and organisation(s).
- Access controls and authorised users will be reviewed regularly.

- Where there is clear or potential benefit then access will be permitted. Where there is no conceivable benefit access will be restricted.
- As a general rule, administration staff should see minimal student data, accepting there some administration roles that need student information and that some student information can be inferred by administration data.
- Where possible all systems will feature control based on the principle of 'legitimate relationships' where there is a link between the student, the service and its staff. Unless there is a relationship such as a referral to a service, users will only see basic information, generally limited to demographics. Creation of relationships by referral or 'self claimed' in emergency/urgent situations will be subject to audit checks.
- Allocation and use of privileges (feature that allows a user to override normal controls) will be restricted and controlled. They will be allocated on a 'need to use' basis and on an 'event-by-event basis'. Record of allocation will be kept by the IT Department.

Granting & maintaining user access

All multi-user systems will have a formal process for requesting and removing access.

Formal records of all users, past and present, will be kept. The process for a system can be combined with that of others or kept separate.

Processes will include:

- Allocation of a unique User ID. The use of generic User IDs is only permitted in limited circumstances and must be agreed by the Director of Information Technology and the Principal who will control the circumstances under which these are used.
- Authorisation of the access request from the line manager who is responsible for confirming the provisional user has a 'need to use' and 'need to know' the information contained within the system that is accessible via their user role.
- Notification to the user of their responsibilities under this and associated policy, and their acceptance of those via the employee's signature or formal response.
- Confirmation to the staff who create the access that the requirements of the process are complete before the access is created and issued.
- Access change request procedure, authorised by line management, usually on the basis of changed role or enhanced responsibilities
- Access revocation procedure, authorised by line management, initiated by user leaving or other request for revocation such as a role change.
- All procedures to grant and manage user access will be integrated with Human Resources processes for induction and departure, role changes and temporary absence.
- The IT Department will conduct a review of unused accounts on a regular basis.
- The IT Department will conduct reviews of active accounts in relation to lists of leavers to identify any account still in use after a staff member has left. Any accounts

found to have been accessed without authorisation will be investigated and appropriate action taken.

B. User password management

Password allocation will be managed via formal processes as part of user registration and account maintenance. The processes will:

- Require users to agree to a statement to not share or record passwords
- Promote 'quality' passwords that are not easy to guess
- Re-issue forgotten passwords following positive identification of the user, if necessary via a face to face meeting, where ID is checked.

C. Remote access and other external connections

Any access to systems via personal devices connected directly to the Sheridan network, or computers not directly connected to the Sheridan network will be considered remote access or an 'external' connection, and governed by remote access security technologies or protocols.

D. System access control requirements

Log on procedures within systems will disclose the minimum information possible about the system to prevent unauthorised users being provided with log on details. The following are minimum standards for systems to meet, where possible:

- A general warning notice that access should only be by authorised users will be shown at the commencement of log on procedures.
- When an error occurs with a log on attempt, systems will not detail what is incorrect (i.e. will not display a message such as 'incorrect password', they will simply report a phrase such as 'log-on details incorrect').
- Systems will only allow a limited number of incorrect log on attempts and will record all details connected with these log on attempts.

All information systems will feature password control. As with log on procedures, the following policy elements will be applied to all systems, unless evaluation finds that cost or system architecture does not support it. In such circumstances the statements will be applied to replacement systems.

Standards for quality passwords:

- User selection of passwords will include a confirmation procedure to check for user error when inputting the new password
- Passwords will be a minimum length and complexity as determined by the IT Department.

Passwords will be stored using one or more restricted access technologies.

E. Application access control principles

Some Sheridan systems will have system utilities that may be capable of overriding system and application security measures. Use of these functions/utilities will therefore be restricted to the minimum practical number of authorised personnel.

F. Monitoring system access & use

Systems will be capable of logging events that have a relevance to potential breaches of security. These logs will be kept for a minimum of two years (or longer where required by a record retention schedules). The logs will cover the following events as a minimum standard:

- Log on attempts – recording User Ids, dates and times and success/failure of attempt.
- Creation and amendment of data – recording User Ids, dates and times – and deletion of data
- Where possible views of data.

Each system management role will develop procedures for monitoring the use of each system. Regular standard processes to examine failed access attempts, data manipulation spot-checks and any other logged system event will be a part of management of each system.

Users will be informed of monitoring activity during training on each system. The organisation reserves the right to suspend, limit or remove access from any user suspected or convicted of misuse.

G. Third party access requirements & outsourcing

Any requirement to access information by someone who is not a member of staff will be considered 'third party' access. The requirement and associated risks will be documented and assessed for control.

Where risks from third party access have been identified, contractual arrangements will be put in place to manage the risks. The manager of the contract will ensure this is undertaken with advice from the Principal.

A standard 'Confidentiality/Non-disclosure' agreement is available for use or adoption into contracts.

Off-site access to systems – 'Network' access for suppliers or partner organisations will be via an approved connection.

In addition to the above, the elements that will be included in any outsourcing/support arrangement are:

- Identification, awareness and understanding of responsibilities (inc legal compliance requirements)
- Service level agreements on availability of service (accessibility of information), integrity (quality checks) and confidentiality
- The right of audit.

3. Systems Development and Data Collection

A process for assessing new information processing functions will be used.

New information collection – Where personal information is to be collected via an existing tool, that isn't a new bespoke system, or new functionality for an existing system, then the Principal must be contacted and assess that the collection and methods meet with legal requirements. For example, the use of Excel or Access to record personal information. The Principal will periodically audit the use of such tools to ensure all data collections are recorded via revising information flow maps and asset registers.

New systems – Any requirement for a new system, regardless of size & cost will be put through the process for assessment.

Significant new function (of existing system) – It is important to draw distinction between new function and change to existing system function. Both will have impact on information, however changes to existing functions are covered by the policy controls and processes associated with change control (see 5.3.3).

Separating operational and development facilities

Development of supplied systems – Where the contracted supplier controls the development environment, overall compliance with higher education standards will be sought in contractual arrangements. This will include controls over staff access to development and live environments and development tools.

In-house developed systems – In line with supplied systems, the following elements must be considered and applied if possible:

- Development environments will ideally run on different processors, or in different domains or directories
- Compilers, editors and system utilities should not be accessible from operational systems when not required.
- Rules for transfer of software/code from development to operational status should be defined, including reversal procedures & linkage to change control.
- *On-site 'Test' environments of supplied & in-house developed systems* – Each system will evaluate the feasibility of a 'test' environment. This will be used for training, system update testing and functionality development testing. Access request and control policy/procedures for each system where there is an 'onsite test' environment will incorporate requirements for user access to that as well.

A. Requirements analysis and specification

The Principal will be involved in the development of new information system functionality (inc new systems and development to existing systems) and processes to ensure that all governance requirements are included:

Security – Security controls required will reflect the business value of the information assets based on risk assessment of failure of a system or absence of the information to the organisation.

Confidentiality – The Information Governance lead will ensure that compliance with relevant legislation and duty of confidentiality are paramount concerns during system and process developments.

Integrity/Quality – In line with compliance with the fourth data protection principle, data quality will be a specific element of system/process analysis and specification.

B. Capacity planning and acceptance

The IT department (and any other responsible for system capacity) will monitor system capacity. This will include network bandwidth, storage capacity and system response times.

The departmental/area 'system managers' will provide details of their requirements of the systems, in terms of total number of users, expected volumes of concurrent usage, peak usage timings and system development requirements.

The IT department(s) will advise and guide on the required resources, lead times and costs of the co-ordinated development plan.

Acceptance of developments

New systems, existing system upgrades/new versions will only be installed following the definition of formal acceptance criteria.

The following are controls that should be considered:

- Performance and capacity requirements (in terms of response times & other capacity elements
- Preparation and testing of routine operating procedures (such as standard reports etc)
- Testing of security controls (passwords, usernames, information access controls)
- Business continuity arrangements & tests
- Training provision to all appropriate staff, including education/communication of upgrades

C. Change control and outsourced development

All changes to existing systems will be subject to change control procedures that will evaluate the potential impact of change on system security, data quality and availability elements. Two forms of changes are covered:

- In built system functions, such as switches for mandatory fields or user definable code lists.
- Vendor controlled changes, where alteration to software code is required, for the addition of new data collection, processing or functionality

Change requests will be made via an authorisation process controlled by system management and system owners. Following receipt of request, system management will undertake analysis of the impact of changes. Significant change proposals that have not originated from the user base will be tested with users prior to commitment to change. System management and the user base will create a set of formal acceptance criteria for each change.

Where a system has a test environment all changes will be carried out there first and evaluated against the acceptance criteria prior to being installed in live systems. Changes will be scheduled with the user base to ensure minimum disruption to operational business.

System management will ensure any changes to system documentation resulting from change will be put in place.

Operating system changes

When it is necessary to change or update an underlying operating system, applications will be reviewed and tested to ensure that integrity has not been compromised. The IT department (and suppliers) will lead changes to operating systems ensuring the relevant other departments are brought in and that sufficient time is allowed for testing.

Restrictions to changing software

Both in-house and vendor supplied software will be controlled by restricting responsibility to authorise changes to system management and system owners.

Changes to vendor-supplied software will be governed by contractual agreement with the supplier.

Covert channels and Trojan code

The organisation will protect itself from covert channels and Trojan code that allow unauthorised access to information by applying the following controls:

In-house developed software – Application developers will be bound by contract terms of employment and job description responsibilities from inserting covert channels and Trojan code

Vendor supplied software – Contractual arrangements will ensure that the vendor does not insert covert access channels or Trojan code. Should these be found to be present in any vendor supplied software, contracts will contain appropriate penalty or termination clauses.

4. MAINTENANCE AND OPERATIONS

A. Operational procedures and responsibilities

Procedures will be documented as follows:

Data Collection & Training materials – For procedures carried out by general users of the systems documentation within detailed training materials and user manuals will suffice

System administration & operations – Each system/area will draw up detailed information on procedures required to ensure the smooth running of the system.

These will typically be both regular operational tasks and irregular system maintenance/change elements.

Technical operations – Areas to be considered include: routine maintenance, start up/shut down procedures, housekeeping, capacity monitoring etc.

Helpdesk (fault logging) - As part of IT helpdesk operations, all reported or encountered faults with systems should be logged. Procedures should be in place to review fault/helpdesk logs for resolution.

Change control documents – (see 5.3.3)

The following items should be included in documentation (where appropriate):

- Contact details (for support, queries etc)
- Instruction for handling errors, including known impacts
- Effective document management
- All operating procedures will be subject to regular review.

Operational change control

Poor change control is one of the major factors relating to system failure. By default the 'system management' role for each area/system is responsible for the application of change control procedures for their system/area.

The following elements must be considered when developing change control procedures:

- Identification and recording of significant changes
- Assessment of the potential impact of such changes
- Formal approval procedure for proposed changes
- Communication of changes to all relevant personnel
- Formal acceptance or revocation procedures for changes

Change control procedures must be applied in the following circumstances:

- Changes to datasets collected
- Changes to standard report provision
- Changes to user procedure (& documentation)
- Changes to operational system provision procedures (backups etc)

B. Housekeeping, backups, logs

Information back-up is one part of Business Continuity. All systems should have some sort of backup facility. For large specific applications this will typically be arrangements such as mirrored discs and backup servers to provide additional resilience in the event of component or power failure. They may also have a removable media backup device.

For smaller applications (such as access databases) and data folders, the regular backup of shared network storage drives should suffice.

Each system/area will determine the appropriate backup procedure using the following guides, with advice from the IT lead:

- Regularity of backup.
- Timing of routine backup – where a system is required on a continual basis at all hours, appropriate timeslots for backups should be determined between the users and the system management/technical staff
- Size of backup – In conjunction with 'regularity', the amount of data backed up should be determined. It is not always possible to backup the entirety of data on a system due to time and capacity constraints. Therefore procedures that take backups of 'data entered on that day', which combined with less regular 'full backups' can be implemented, so that complete recovery can be achieved (up to the last 'daily backup') via a combination of backup media.

- Storage and protection of backup media – Storage should be in a location remote from the main system, but subject to at least the same environmental and physical protection as the main system.
- As part of backup procedures regular testing and full restoration of backups to a separate system should be implemented.

When determining the backup requirements of a system, the organisation will calculate the cost of system failure to the organisation, in terms of reduced efficiency (loss of staff productivity), damage and distress. This combined with the likelihood of failure if sufficient backup is not implemented can give a rough cost of failure to the organisation in a given period. This can then be used in determining the prioritisation of resource allocated to information backup. The server will maintain an activity log for each system. This will include:

- System start/finish times
- System error reports

Paper based information entered on to computer, such as data collection sheets or scanned documents should not be destroyed until at least 2 full backup copies have been taken. Ideally destruction should wait until a full backup containing the information has been validated.

C. Security of system files & documentation

Operating documentation for systems, both paper and electronic will, as a default, be considered 'organisational sensitive' information, as they contain information that could be used to cause damage to systems. It will therefore be stored securely and only available to those with a justified need to access it. System documentation includes data structures, network structures, authorisation processes.

D. Software licensing and intellectual property

The organisation will comply with legal restrictions on the use of material subject to intellectual property rights such as copyright, design rights and trademarks as follows

- Staff will not be allowed to load software onto the organisations computers without authorisation. This will include a check on the intellectual property rights applicable to the software
- Capacity requirements in terms of licences for multi-user systems will be monitored to ensure that licences are not used inappropriately.
- The organisation will actively participate in shared licensing with associated institutions.
- Copies of software will only be made under the authorisation of the IT department who will check on licensing requirements.

E. Technical system audit

Any required/planned audit will take account of risk to business operations and be planned around required timing. Factors to be included are, the removal of key staff to meet with auditors, the scope of checks and the requirement for production of audit reports from the system. Access to any software tools or reports that form part of audit of a system will be restricted to specific individuals

F. Forensic readiness

Forensic readiness is defined as 'the capability of an organisation to use digital evidence in a forensic investigation'. For digital evidence to be used in an investigation it must be recovered and analysed in a systematic, standardised and legal manner in order to ensure its admissibility in legal or disciplinary terms.

The scenarios that may require digital evidence include:

- Alleged breaches of the use of personal data and confidentiality
- Unauthorised access to, or use of IT systems
- Fraud, deception.
- Disciplinary issues such as accidents, negligence, abuse of privileges.

The sources of evidence include:

- Electronic student & staff records
- Access control
- Internet monitoring tools
- Firewall logs
- Software functionality
- Network logs

With regard to investigation processes Sheridan may determine as necessary to call in a third party support organisation to carry out a forensic investigation.

Identification of need for investigation:

Potential incidents will be reported either to the IT helpdesk or the Principal.

Regardless of initial reporting these areas will consider and engage the others as required. This is most likely in the case of information governance and risk management.

Initial investigation will include consideration as to whether digital evidence is required and if so how quickly and securely it needs to be gathered. This decision will be based on the likelihood of degradation of the evidence or potential tampering.

If it is determined as necessary the external expert support will be engaged and will guide on the process for gathering, extracting and storing evidence.

Responsibility for investigation:

The Board's Audit and Risk Committee will lead any investigation under the authority of and reporting to the Board of Directors.

Preservation of evidence:

It is possible that evidence will need to be gathered swiftly to ensure its robustness and at the time of investigation specific expert advice will be taken. It may be advisable to temporarily remove the use of the system that is the source of evidence from users in order to preserve the evidence until it is extracted. However it is noted that this in some cases may have impact on operational business. The Principal will determine if access to a system should be withdrawn temporarily to allow evidence to be extracted, basing the decision on the business impact of removing all access against the seriousness of the matter under investigation.

5. APPENDIX: DOCUMENT HISTORY AND VERSION CONTROL

Document Title: Security of Information Policy

Source Documents: In the formation of this policy, Sheridan directly sourced ideas and phrasing from the publications listed below:

- *Australian College of Theology, Handbook for Registrars, Teachers, Moderators and Examiners*, 9th ed., 2010.
- *Curtin University Record-keeping Plan* 2008. Retrieved 31st January 2011 from http://uim/local/docs/secure/curtin_recordkeepingplan.pdf
- *George Washington University, Records Management Policy* 2004. Retrieved 5th May 2011 from http://my.gwu.edu/files/policies/RecordRetentionINTERIM.pdf
- *Government of South Australia, Records Management Disaster Planning Toolkit*. Retrieved 5th May 2011 from http://www.archives.sa.gov.au/files/management_guidelines_ARM_disastertoolkit.pdf
- N*HS South Gloucestershire Information Governance Management System*, March 2010. Retrieved 5th May 2011 from http://www.sglos-pct.nhs.uk/informationgovernance/Information%20Governance%20Policies%20_IGMS_%20v3%201%20final%20nov%202009%20s%20glos.pdf
- *UTS Records Management Plan Template*, University Records, Governance Support. Retrieved 5th May 2011 from
- www.**records**.**uts**.edu.au/forms/**records**-**management**-plan.docx

Associated Internal Documents:

Associated External Documents

Authorised Officer: Chairperson, Board of Directors

Approved by: Mr Michael Smith

Date of Approval: 10 Feb Mar 2021

Date of Next Review: Before Dec 2024

Version Number	Version Date	Authorised Officer	Amendment Details
1.00	30 May 2011	N/A	Draft prepared by Darren Smith for Sheridan College and Vose College of Higher Education

2.00	30 May 2011	N/A	Revised by Justin Hearn and Darren Smith for Sheridan College
2.00	02 Mar 2013	Chairperson, Board of Directors	Submitted to TEQSA for Sheridan College HEP registration: Attachment 7.5a
3.00	10 Feb 2021	Chairperson, Board of Directors	Revisions

[PAGE LEFT BLANK
INTENTIONALLY]

SHERIDAN
INSTITUTE OF HIGHER EDUCATION

Organisational Records Management Policy

Policy Area: Information Management

Approval: Chairperson, Board of Directors

Signature: Date:

ORGANISATIONAL RECORDS MANAGEMENT POLICY

1. CREATION OF ORGANISATIONAL RECORDS

Sheridan will ensure core principles and processes are applied to the creation of an organisational record. These will ensure that documents are given meaningful titles and stored in clear and searchable filing systems. This will ensure that full and timely responses are given to requests for information and that the organisation operates as effectively and efficiently as possible. For any document that will go through a lifecycle of development and review, a system of version numbering will be implemented. A core scheme will be developed and used in all areas, unless there is substantive documented reason why another system should be used.

Document naming conventions:

Documents should be titled with reference to:

- Their subject
- The type of document they are
- A reference date, only where necessary (such as the date of a meeting)
- A version number where applicable
- Document status (draft, current, final etc).

2. STORAGE AND SAFEGUARDING ORGANISATIONAL RECORDS

Each business area of Sheridan is responsible for determining how they will file their records based on a set of core principles:

- Electronic information will be stored on networked storage facilities and not on individual hard drives of PCs, unless otherwise approved by the Director of Information and Communications Technology and the Principal.
- Structure folders around projects, initiatives or similar groupings of work.
- The team should determine who should have access to a folder and sub folders.

Whilst much of the information in a folder can be disclosed, this does not mean the majority of staff in Sheridan need access to it. Access controls do not just prevent people seeing information they shouldn't see; they also prevent accidental or malicious alteration or deletion of information. Access controls can be set to 'read only' and this should be the default. The relevant manager will be responsible for ensuring that staff only have the access they require.

3. Archiving and Disposal

All trust records will be managed in line with the relevant code of practice. Where a situation is encountered that is not covered by any code, the Principal will facilitate with appropriate staff and committees a decision about the archiving and disposal of records.

4. Ensuring Storage Capacity

It is very easy in electronic systems to have multiple copies of documents, especially across a network storage and multi-user email system. This uses up storage space unnecessarily.

Each department should periodically review their electronic storage and remove duplicate documents.

5. Document Management Systems (DMS)

Sheridan will periodically review the need and cost/benefit of document management systems, recognising that the core principles of this policy must be part of the operational culture before full benefits from any DMS are realised. Individual departments wishing to look at DMS solutions may do so but provided they engage with the corporate and information governance leads to ensure that an appropriate strategic approach is taken.

6. Audit of Corporate Records

The Registrar will carry out audits of corporate records and filing on a regular basis to identify and address any of the following issues:

- Duplication and lack of version control
- Unused documentation for archiving
- Retention of documents past required period
- Unstructured and inefficient filing
- Poor access control

7. Paper Corporate Records

All records will be created electronically according to the creating and managing electronic record guidelines, including:

- Policies and procedures
- Strategies and action plans
- Minutes and agendas
- Reports (e.g. annual, Board)
- Financial standing orders

None of the above are created as 'paper' based corporate records within Sheridan. A small number are retained on paper for 'permanent' preservation as per the record retention policy. Whilst there is no creation of formal paper records by Sheridan, there are a number of documents handled on paper that Sheridan will ensure there is appropriate processes for:

Incoming mail: The correspondence will be logged by the receiving department and any replies created electronically, even if issued on paper.

When the document is received and logged it will be given a reference number either automatically by the recording system or manually. Any documents created in response to

incoming mail need to be linked to the paper document by this tracing/tracking reference number.

Paper documents will be filed according to the requirements of the receiving department in a manner that will facilitate easy retrieval such as subject, date or numerical order, or detail about the subject (issue) or the person. Any paper documents will be held for the required retention period and disposed of appropriately, using confidential waste or shredding when required.

When filing paper documents consideration must be made of their content, any document containing service user, staff or organisationally sensitive information must be held in secure or lockable filing systems. Other documents created on paper include the following, although this list is not exhaustive. However the fundamental principles are that these items require an 'authorisation' on the data collection form and will be held by the relevant department in the most appropriate filing system:

Invoices: Invoices should be passed to the payment system for processing. Whilst these are received on paper, they are handled via an electronic system.

Sickness certificates: Received on paper and stored in HR in the appropriate personnel file for the period of time required to be retained. Data is entered as required onto the Electronic Staff Record and Payroll systems.

Incident Forms: These include personal statements and staff signatures and are stored by the Principal for the required period.

6. Appendix: Document History and Version Control

Document Title:	Organisational Records Management Policy
Source Documents:	In the formation of this policy, Sheridan directly sourced ideas and phrasing from the publications listed below:

- *Australian College of Theology, Handbook for Registrars, Teachers, Moderators and Examiners*, 9th ed., 2010.
- *Curtin University Record-keeping Plan* 2008. Retrieved 31st January 2011 from http://uim/local/docs/secure/curtin_recordkeepingplan.pdf
- *George Washington University, Records Management Policy* 2004. Retrieved 5th May 2011 from http://my.gwu.edu/files/policies/RecordRetentionINTERIM.pdf
- *Government of South Australia, Records Management Disaster Planning Toolkit*. Retrieved 5th May 2011 from http://www.archives.sa.gov.au/files/management_guidelines_ARM_disastertoolkit.pdf
- N*HS South Gloucestershire Information Governance Management System*, March 2010. Retrieved 5th May 2011

from http://www.sglos-pct.nhs.uk/informationgovernance/Information%20Governance%20Policies%20_IGMS_%20v3%201%20final%20nov%202009%20s%20glos.pdf

- *UTS Records Management Plan Template*, University Records, Governance Support. Retrieved 5th May 2011 from
- www.**records**.**uts**.edu.au/forms/**records-management**-plan.docx

Associated Internal Documents:

Associated External Documents

Authorised Officer: Chairperson, Board of Directors

Approved by: Mr Michael Smith

Date of Approval: 11 Mar 2020

Date of Next Review: Mar 2021

Version Number	Version Date	Authorised Officer	Amendment Details
1.00	30 May 2011	N/A	Draft prepared for Sheridan College and Vose College of Higher Education
2.00	30 May 2011	N/A	Revised for Sheridan College
2.10	02 Mar 2013	Chairperson, Board of Directors	Submitted to TEQSA for Sheridan College HEP registration: Attachment 7.5a
3.00	18 Mar 2020	Chairperson, Board of Directors`	Policy update for Board of Directors

SHERIDAN COLLEGE
PERTH | WESTERN AUSTRALIA

Acceptable Use of ICT Policy [NOT REVIEWED: REVIEW IN 2022]

Ensuring effective and appropriate use of fax, phone, email, skype, instant messaging, social media, electronic office, mobile computing and removable media

Policy Area: Information Management

Approval: Chairperson, Board of Directors

Signature: Date:

ACCEPTABLE USE OF INFORMATION & COMMUNICATION TECHNOLOGIES POLICY

1. INFORMATION HANDLING PROCESSES

All departments will have procedures for handling information. As a default, the policy for handling information, in line with its classification is as follows:

Personal sensitive information & Organisational sensitive information:

- Accessed only by staff with a 'need to know' and a 'justified purpose'
- Only minimum information accessed, used and shared
- Only distributed to named individuals where possible (in conjunction with first bullet point)
- Stored and filed appropriately in a timely manner

Specific policy elements around handling information communication via email, fax and phone are covered under section 3

2. INFORMATION EXCHANGE AGREEMENTS

Information exchange operates on two levels. There is routine sharing of information between organisations for general operational activity and also strategic sharing of data for planning and development purposes, which may be both regular and ad-hoc.

Routine sharing – The organisation will participate in common, high-level principle agreements set out across the community(ies) of which it is part. It is recognised that the boundaries change periodically and it is part of the Information Governance role to maintain the organisation's participation.

Where routine sharing requires either the exchange of a set of data on a regular basis, or is achieved by providing access to an information system there will be formally agreed documentation, such as an exchange agreement or access agreement. Routine communication (via secure methods) between professional staff about the direct care of an individual do not require specific formal agreement, however each agency must ensure all staff are aware of their responsibilities to share data appropriately.

Strategic/development sharing - New or existing strategic partnerships require information from across organisations to develop. Where such an arrangement exists or is proposed, the organisation will ensure that it evaluates and agrees to appropriate formal procedures for extracting and sharing information. Procedures should refer to relevant sections of this policy.

3. Use of Faxes, Emails, Phone and Post

As there are many varied situations specific policy is difficult to set in relation to these areas, however the following minimum standards will be applied:

Faxes

- Mark all pages confidential if appropriate
- Confidential information should only be faxed if urgent
- Don't include names in information unless you need to
- Where possible send the fax to a named individual using a coversheet
- Double check the fax number, with the recipient
- For important/confidential faxes, tell the recipient it is being sent and check they receive it.

E-mails

- Emails may be disclosed to the public – be professional.
- Check you have the correct email address.
- Don't include names in your message unless you need to
- Do not send person/service user identifiable information unless you have to and only by approved methods
- Don't send emails that could be offensive
- Do not make personal use of email/internet when you should be working.
- Don't keep emails about arrangements that have passed.
- Do keep emails where you give opinions, advice or professional comment

Telephone

- Be sure you know who you are talking to
- To confirm someone's identity ring them back through a switchboard.
- Ask them what they want to know and why they need it
- Do not make confidential calls where you can be overheard.
- If phoning student, ask them to confirm details to you to check they are the student.
- Always ask to speak to the student, without revealing where you are calling from.
- Only leave an answering phone message (of limited detail) if it is urgent and you can't try calling again

Post

- Don't include names in information unless you need to
- Confirm the name and address of the recipient when addressing the envelope.
- If you only want the recipient to open it, mark it 'addressee only'
- If it contains confidential information, mark it 'private and confidential'
- Always seal the information in a robust envelope
- If it is critical check it has been received.

- Use recorded delivery for sending important (but not original) documents
- Use special delivery if proof of posting, tracking and receipt on delivery is important

4. Acceptable use of Email, Internet and Electronic Office (inc Monitoring)

The following are the core policy statements that relate to the use of email, internet and electronic office facilities in the organisation. These are backed up by operational guidance set methods of working compliant with the core policy statements. Staff are informed of acceptable use via education sessions and awareness products.

A form of agreement will be used when staff are initially set up on the system that details what use is acceptable and where they can find more information

Users can -

- Send identifiable student data or sensitive data on staff to other users with the same organisational email address, provided it is to a named individual and is necessary to do so.
- Send identifiable student data or sensitive data on staff to other recipients provided they get confirmation of the appropriate method from the Principal.
- Make limited personal use.

Users must NOT -

- Share personal usernames and passwords or leave computers logged in and unattended.
- Cause offence to any other user or damage the organisation's reputation by creating, accessing, storing or sending any images, files or data that could be said to be abusive, sexist, racist, defamatory, obscene or otherwise offensive or inappropriate.
- Use College facilities for advertising/fund raising not directly connected with the College, other than the use of social notice board facilities.
- Deliberately delete or alter information the College needs to keep and maintain, or overload systems with the effect of denying access or wasting resources.
- Use data that identifies individuals unless absolutely necessary.
- Store student identifiable, staff/organisationally sensitive data on equipment not owned by the College.
- Put student identifiable or staff/organisationally sensitive data on CD/DVD, memory stick unless the files or devices are encrypted.
- Leave College equipment unattended unless it has been secured in a locked office, room or house.
- Remove equipment or information without sufficient authorisation.
- Connect College equipment to other networks without permission, nor connect non-College equipment to the network without permission of the IT department.
- Download or install software without the approval of the IT department.
- Delete emails about discussion or decisions/agreements before the period for which they should be retained has expired (see section 6)

The College will –

- Routinely monitor system capacity (including connectivity and storage)
- Investigate breaches of policy in conjunction with relevant HR policies

- Implement and maintain restricted access technologies
- Educate users in appropriate use and monitoring that is undertaken
- Routinely record every aspect of computer use, including keystrokes, screenshots, login, file access logs and web access logs

The College may –

- Implement monitoring/blocking software that automatically checks content of email and websites for inappropriate items, such as images, software etc
- Provide access to a user's email account to their line manager where there is documented and justified need (i.e. period of leave)

The College will not –

- Monitor the activity of individuals without consent, unless there is a justified reason identified either by routine monitoring or concerns raised by others.

Where an investigation is deemed necessary, justification for the level of 'intrusion' must be documented. For example if a user is suspected of misusing email facilities an investigation can be carried out, but this should not include investigating their use of other systems, unless there is also cause for concern about those.

The College reserves the right to suspend, limit or remove access from users suspected or convicted of misuse.

5. Mobile Computing and Home Working

Authorisation processes for the off-site use of equipment, either as a one-off or regular occurrence are implemented, which will ensure a record of all staff undertaking such activity is kept. The authorisation process includes detail of technical security requirements required to be in place for electronic access to information. The following controls are applied:

- Equipment and media taken off premises should not be left unattended. During transportation equipment must be adequately protected from breakage and locked out of sight in a car.
- No College equipment will be connected to another network without authorisation from the IT department.
- Student identifiable data, or staff identifiable data, of a sensitive nature (such as appraisal, complaint or disciplinary information) must only be used on equipment supplied by the organisation and protected by restricted access technologies.
- Staff may use their own computers for work purposes but only non sensitive information can be used and this must not be permanently stored on the equipment unless approved by the IT Department.
- Home-working controls should be determined by a risk assessment in relation to the activities undertaken and suitable controls applied.
- Staff are responsible for the security of any information in their own home and must not allow other members of the family access to it.
- Any media containing personally identifiable data or organisationally sensitive data must be returned to the office and disposed of appropriately.
- Adequate insurance cover should be in place to protect equipment off-site.

Formal records (e.g. student records) will be subject to a tracking system that incorporates logging out and back.

Spot checks will be undertaken to detect unauthorised removal of property. Staff will be informed that these take place, although not when and how.

6. Management of Media, Encryption tools and Port Control & Secure File Transfer

The media on which information is stored is a key element to the appropriate handling and use of information. The following controls will be applied to the management of media.

- Procedures for the tracking of paper-based information will be used. Due to the nature of 'original' paper information being in one place at one time, it is important that critical records are tracked. This will apply to paper Student Records and any other paper record that by its nature requires formal control.
- Staff who are required to remove information via any media will be made aware of the procedures governing the use of laptops, electronic media and remote access and any subsequent revisions. Careless use of media could result in breaches of confidentiality or risk to the integrity of the organisation, therefore the following controls form the policy for use of media:
    - Paper media (including carbon copies, computer printouts) containing information that is classified as *'Personally Identifiable'* or *'Organisationally sensitive'* (see section 3 classification guidelines) will be disposed of via secure methods such as incineration or shredding. Collection of media for controlled disposal will be via 'confidential' waste sacks or bins. Contracts with external waste contractors will contain confidentiality clauses and indemnities. Confidential paper waste maybe recycled by external contractors as long as an agreement with appropriate security controls is in place.
    - Magnetic media (hard discs & tapes) will be erased prior to disposal via secure means, such as incineration by external contractor working to appropriate security controls (confidentiality clauses, indemnities).
    - Any PC holding personal data (due to lack of fileservers in some locations) will be encrypted.
- Staff needing to carry personal/sensitive information on portable devices are required to apply, detailing the data held, the purposes and the uses. Applications will be processed by the line manager who will advise on use as required.
- All staff needing portable devices are to be issued with College-owned devices upon request, whilst issued with reminder that information should only be put on such devices if necessary.

7. Intranets and Public Websites

Publication of material to the College's official public website will be controlled by the College's communications function. By instructing the IT function to provide web editing software and access to websites for updating, they will approve who can manage content.

Department managers will have responsibility for content published on the intranet and can delegate publication to team members via requesting the installation and set up of publishing tools (as above).

For both Internet and Intranet publication, content shall be routinely monitored and removed when out of date.

The key issues that must be addressed by specific policy/procedure for an 'electronic' system are:

- Authentication – proof the user or data source is who they claim to be
- Authorisation – proof the user or data source is authorised to undertake what they are attempting or have done.
- Liability – who is responsible for reducing risk/failure within the system(s)
- Security – all systems will employ appropriate restricted access technologies

The development of such systems is really the replacement of existing paper based arrangements, so any formal documentation must be amended at the appropriate time to reflect any change.

8. Business Continuity for the Use of Systems and Information

The organisation has a process for management of continuity across the organisation comprising of:

- Risk assessment and management, to identify critical business processes and information assets, threats to these, vulnerabilities and probability of failure
- System resilience requirements to reduce probability of failure
- Communication responsibilities to initiate manage and restore from continuity plans.
- Plan management, development and testing responsibilities

Departmental co-ordination and collaboration is key to the development and maintenance of effective and efficient continuity planning.

Senior management will set the high level priorities for continuity of systems based on the business objectives and priorities of the College. This will aid prioritisation of resource available to build system resilience and effective disaster recovery for systems identified as 'mission critical'. This will aid the continuity planning for these systems, however policy is that all systems will be covered by continuity plans.

Impact analysis

Continuity requirements will be determined by identifying events that can cause disruption to business processes. These will include, but are not limited to:

- Fire, flood, impact damage
- Equipment & component failure, severe capacity restriction
- Power supply withdrawal
- Malicious attack including physical and network/system intrusion
- Theft of information and media (including paper) resulting in unavailability of information.
- Loss of resources such as staff and information assets (reference materials etc)

Writing & implementing continuity plans

The Principal will co-ordinate analysis of impact of disruptions to information availability. This will identify impact, fallback activity, required recovery periods and local preventative measures.

Each department is then required to link plans around continuity with regard to their information assets to their overall continuity plans.

The following will be included in all information related 'business' continuity plans:

- Identification of key information assets, key responsible staff, the impact of loss over specific periods of time elapsed and procedures, including when impact becomes a concern, remedial action, recovery and restoration to normal activity
- Education programmes for staff in agreed continuity procedures
- Follow up action to learn from incident and ensure further risk is reduced if possible (see 2.6)

Identification of restoration priorities will also be included, if there is a requirement to restore operations to specific key areas in an ordered manner, or partial restoration can be achieved effectively prior to full restoration.

Planning framework

System focussed business continuity planning will be incorporated with wider organisational continuity plans where available, so that should there be a requirement for the organisation to move essential business operations to alternative (temporary) locations, essential information for operation at temporary locations is available.

Testing (review) of plans

Each individual plan will be reviewed and updated annually. It is expected that a facilitated review will be undertaken every two years, with department heads required to review in between these and update when there is significant change.

The department head is required to take the plan(s) to team/departmental meetings both to raise awareness and 'test' the fallback activities and impacts with the rest of their department.

9. Appendix: Document History and Version Control

Document Title: Acceptable Use of ICT Policy

Source Documents: In the formation of this policy, Sheridan College directly sourced ideas and phrasing from the publications listed below:

- *Australian College of Theology, Handbook for Registrars, Teachers, Moderators and Examiners*, 9th ed., 2010.
- *Curtin University Record-keeping Plan* 2008. Retrieved 31st January 2011 from http://uim/local/docs/secure/curtin_recordkeepingplan.pdf
- *George Washington University, Records Management Policy* 2004. Retrieved 5th May 2011 from

http://my.gwu.edu/files/policies/RecordRetentionINTERIM.pdf

- *Government of South Australia, Records Management Disaster Planning Toolkit*. Retrieved 5th May 2011 from http://www.archives.sa.gov.au/files/management_guidelines_ARM_disastertoolkit.pdf
- N*HS South Gloucestershire Information Governance Management System*, March 2010. Retrieved 5th May 2011 from http://www.sglos-pct.nhs.uk/informationgovernance/Information%20Governance%20Policies%20_IGMS_%20v3%201%20final%20nov%202009%20s%20glos.pdf
- *UTS Records Management Plan Template*, University Records, Governance Support. Retrieved 5th May 2011 from
- www.**records.uts**.edu.au/forms/**records-management**-plan.docx

Associated Internal Documents:

Associated External Documents

Authorised Officer: Chairperson, Board of Directors

Approved by: Mr Michael Smith

Date of Approval: 02 Mar 2013

Date of Next Review: Before Dec 2022

Version Number	Version Date	Authorised Officer	Amendment Details
1.00	30 May 2011	N/A	Draft prepared by Darren Smith for Sheridan College and Vose College of Higher Education
2.00	30 May 2011	N/A	Revised by Justin Hearn and Darren Smith for Sheridan College
2.00	02 Mar 2013	Chairperson, Board of Directors	Submitted to TEQSA for Sheridan College HEP registration: Attachment 7.5a

SHERIDAN COLLEGE
PERTH | WESTERN AUSTRALIA

Electronic Learning Management System Policy

Policy Area: Information Management

Approval: Executive Principal

Signature: Date:

ELECTRONIC LEARNING MANAGEMENT SYSTEM POLICY

1. POLICY

Sheridan College will support learning with an Electronic Learning Management System.

2. BACKGROUND

Sheridan College utilises appropriate electronic technologies to support student learning including an Electronic Learning Management System. Such systems provide online access to study materials (e.g. lectures), communications, marks, and provide for assessment submissions, online discussions etc. There are several providers of Electronic Learning Management Systems (e.g. Canvas, Blackboard etc.)

3. CONSIDERATIONS

In implementing this policy Sheridan College will:

- Ensure the selected Electronic Learning Management System is well constructed and user friendly
- Provide continuous secure online access to the Electronic Learning Management System for students and staff (allowing for reasonable maintenance outages).
- Ensure all teaching staff and students receive training in the use of the relevant Electronic Learning Management System.

4. APPENDIX: DOCUMENT HISTORY AND VERSION CONTROL RECORD

Document Title:	Electronic Learning Management System Policy
Source Documents:	
Associated Internal Documents:	Information Management Policy Handbook
Associated External Documents	
Authorised Officer:	Executive Principal
Approved by:	Mr Darren Smith
Date of Approval:	26 May 2017
Next Review Before:	Dec 2022

Version Number	Version Date	Authorised Officer	Amendment Details

0.01	April 2017	N/A	Draft prepared by Matthew Bambach for Sheridan College
1.00	26 May 2017	Executive Principal	Inclusion of proposed "Electronic Learning Management System Policy" in Information Management Policy Handbook
2.00	18 Mar 2020	Chairperson, Board of Directors	Policy update for Board of Directors