Kenvale
COLLEGE OF HOSPITALITY
COOKERY & EVENTS

Information Technology (IT) Cybersecurity Policy

Policy Summary	
Department Responsible for Policy	IT Department
Contact Person for Policy	Chief Operations Officer
Approving Authority	Finance and Audit Risk Committee
Date Last Approved	4/08/2020
Next Review Date (Evaluation)	Every three years from date of release
Related Documents	**Guidelines** • *The National Code 2018* • *Australian Skills Quality Authority (ASQA) Standards for NVR Registered Training Organisations 2015* • *Australian Qualifications Framework (AQF)* • *The Tertiary Education Quality Standards Agency (TEQSA) Higher Education Standards Framework 2015* • *Privacy Act 1988* • *Privacy Amendment (Notifiable Data Breaches) Act 2017* • *ISO 31000:2018,* Risk management – Guidelines **Policies** • *7-01-001 Use of Information Technology (IT) Policy* • *10-01-002 Records Management Policy* **Manuals** • *7-02-001 Use of IT Manual* • *7-02-002 IT Administrator Manual* • *7-02-007 Data Breach Response Plan* • *10-01-001 Document Management Policy* • 10-02-013 Records Management Manual • *10-02-005 Document Management Manual*
Document Number	7-01-002

Policy History		
Policy version	**Main changes made**	**Date Amended**
1.0	New Policy	17/11/2013
2.0	Updated to align with changes to the Privacy Act and to comply with Higher Education Standards	13/12/2016
3.0	Updated to include post internal audit recommendations, the updated National Code indications and the introduction of *Privacy Amendment (Notifiable Data Breaches) Act 2017*	6/11/2018
4.0	Routine internal quality review of document and update to cyber security and change name to reflect a more broader content	4/08/2020

1. Preamble

1.1 This document sets out College policy on Information Technology and the corresponding Cyber Security.

1.2 Cyber Security is about defending IT Facilities and Services and stored data from unauthorised access, use, disclosure, disruption, modification and destruction. It is concerned with ensuring integrity, availability, confidentiality and safety of data and services; and ensures controls are proportionate to risk.

1.3 Information is an asset and is crucial to the effective management of a business or entity.

1.4 Information can be sensitive and such information must be protected in line with statutory and compliance requirements. Personal information falls within this category.

1.5 Information can also be commercially sensitive in that it relates to the College's operations and activities, as well as to College business partners and associated arrangements, which contribute to the College being a competitive and financially viable business.

1.6 Where information is not effectively secured, the College is exposed to a number of intolerable risks. In addition, College staff, students and other stakeholders are also exposed to intolerable risk.

1.7 The College is committed to the appropriate use of Information Technology and Services to support its learning, teaching, administrative, and service functions. *7-01-001 Use of Information Technology (IT) Policy* defines acceptable behaviour expected of Users of the College IT Facilities and Services. The College requires users to comply with the IT policies and associated requirements governing the Use of IT

Facilities and Services as a condition of their use.

2. Definitions

Account Any computing or electronic communication resource allocated to a user by the College and protected from general usage by a security system (e.g. password).

The Australian Skills Quality Authority (ASQA) is the national regulator for Australia's vocational education and training sector. ASQA regulates courses and training providers to ensure nationally approved quality standards are met.

Australian Qualifications Framework (AQF) First introduced in 1995, it is the national policy for regulated qualifications in Australian education and training. It incorporates the qualifications from each education and training sector into a single comprehensive national qualifications framework.

Australian Quality Training Framework (AQTF) The national set of standards which assures nationally consistent, high-quality training and assessment services for the clients of Australia's vocational education and training (VET) system. Initially established in 2001 for implementation in 2002, it is approved by the Ministerial Council for Tertiary Education and Employment (MCTEE), which includes all Ministers for VET in Australia.

The components of AQTF are: AQTF Essential Conditions and Standards for Initial and Continuing Registration; The Quality Indicators; AQTF Standards for State and Territory Registering Bodies; AQTF Excellence Criteria; AQTF Standards for Accredited Courses; AQTF Standards for State and Territory Course Accrediting Bodies. (AQTF, 2010, 6)

Backup: A means of making a duplicate copy of a system and / or data for the purpose of being able to restore a system should a failure or corruption occur.

Bluetooth**:** A short range (10 meters) personal wireless connection of compliant devices.

The College Kenvale College of Hospitality, Cookery and Events.

College IT Resources All networks, hardware, software and communication services and devices which are owned, leased or used under license by the College. It includes technologies such as desktop and laptop computers, software, peripherals, telephone equipment and connections to the Internet that are intended to fulfil information processing and communications functions.

College Network Kenvale College's IT cable and wireless network. Personally-owned devices which are connected to the College network for the purposes of this policy will be considered to be part of the College network.

Cyber Security The practice of defending computing devices, networks and stored data from unauthorised access, use, disclosure, disruption, modification or destruction

The Education Services for Overseas Students Act 2000, (ESOS Act), establishes legislative requirements and standards for the quality assurance of education and training institutions offering courses to international students who are in Australia on a student visa. ESOS also provides tuition fee protection for international students.

Foundation for Education and Training (FFET) The College is a project of the Foundation For Education and Training Limited (FFET), a non-profit company limited by guarantee.

Higher Education (HE) Provider A body that is established or recognised by the Commonwealth or a state or territory government to issue qualifications in the HE sector.

LAN: Local Area Network.

The National Code of Practice for Providers of Education and Training to Overseas Students 2018 (National Code 2018) sets nationally consistent standards for the delivery of courses to overseas students. The National Code 2018 commenced on 1 January 2018.

Registered Training Organisation (RTO) A vocational education and training organisation registered by a state or territory registering body in accordance with ASQA.

Strategic Boards All boards, committees and advisory panels set up by the FFET Board for the purpose of managing the affairs of the College. Refer to *8-01-002 Delegations Register* for more detailed information.

The Tertiary Education Quality Standards Agency **(*TEQSA)*** registers and evaluates the performance of higher education providers against the Higher Education Standards Framework - specifically, the Threshold Standards, which all providers must meet in order to enter and remain within Australia’s higher education system.

Unit of Competency (UoC) A single component of a qualification, or a stand-alone unit, that has been accredited by the same process as for a whole AQF qualification. (AQF, 2013).

Unit of Study (UoS) A unit of study is a term used by our student management system to refer to subjects offered in our course curriculum. These subjects can comprise of one or a number of competency units, selected from a training package. Competencies are grouped together according to similar or complementary content material, creating subjects with the correct amount of content achievable in the designated hours allocated.

Unique Student Identifier (USI) The USI is a reference number that will link to the National Vocational Education and Training (VET) Data Collection allowing an individual to view all of their training results from all providers including all completed training units and qualifications.

User Means and includes all staff, students and other users who are authorised by the College to access its systems and/or network.

Virus: A program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes.

Vocational Education and Training (VET) A type of tertiary education under the Australian Qualifications Framework (AQF), which enables students to gain qualifications for all types of employment, and specific skills to help them in the workplace.

Wireless: Computer devices that connect using radio signals rather than cables.

3. Scope

Aim

3.1 This policy aims to:

3.1.1 Prevent unauthorised disclosure of information stored or processed on Kenvale College systems

3.1.2 Prevent the accidental or unauthorised corruption, deletion or alteration of information important to the College

3.1.3 Ensure the ongoing availability of all necessary information to authorised staff who require such information, and

3.1.4 Provide assurance as to the security and privacy of information stored by the College, whether that information is stored onsite or offsite (i.e. CLOUD).

Scope

3.2 This policy applies to all information prepared, processed, stored, viewed or distributed in electronic form by systems and services on the College network or via systems/networks used by the College for information storage and/or transfer purposes.

3.3 This policy does not detail the procedures associated with IT security. For all procedural information, please refer to the *7-02-001 Use of IT Manual* and *10-02-005 Document Management Manual.*

3.4 This policy should be used in conjunction with the *7-02-001 Use of IT Manual*, *10-02-013 Records Management Manual* and *10-02-005 Document Management Manual.* Data breaches are dealt with separately in *7-01-006 Data Breach Policy.*

4. Staff and Student Access

4.1 The College provides students and staff with access to computing and communications services in support of its teaching, learning, research and administrative activities. These facilities include access to email, Internet, file and print services, an integrated data network.

4.2 Users are responsible for maintaining the use and security of their assigned User IDs and all activity associated with that ID. Knowingly disclosing passwords to others will be deemed a breach of policy and could be referred to disciplinary procedures.

4.3 The College expects its staff, students and associates to take all reasonable steps to ensure the integrity and security of the College systems and data.

5. Human Resources Responsibilities

5.1 It is the responsibility of the Human Resources Department to ensure correct termination dates are entered into the HR system for staff terminations. After a fixed number of days from the date of termination, the staff account will be disabled. Following a further pre-determined number of days, the account will be deleted.

5.2 There are however, situations where an account may need to be disabled immediately and this can only be performed with the authorisation from the Chief Operations Officer.

6. Contract/Temporary Access

6.1 Where temporary access is required for a specific purpose such as, but not restricted to, contract workers and 'test' accounts, a user expiry date based on the completion date of the required tasks must be used to ensure the temporary account is not accessible after that date.

6.2 In the case of ongoing maintenance and support from 3 rd party companies, access must only be granted to the relevant facilities within the system and be restricted to only the systems for which they provide support.

7. Network Usage

7.1 The College provides students and staff with access to computing and communications services in support of its teaching, learning, research and administrative activities.

7.2 By signing the appropriate forms for obtaining access to the College computing facilities, users agree to abide by all policies that relate specifically to the use of these facilities. Any breach of these policies will be deemed an infringement and dealt with accordingly which could result in suspension of access privileges or in severe cases, legal authorities will be involved.

7.3 Interfering, in any way, with the College network or associated equipment, be it intentional or accidental, is not permitted.

8. IT Access

Introduction

As most of the College’s information and business processes are electronically based, it is essential that access is restricted to the College’s IT resources and networks.

Access privileges are only given to staff, students and other necessary users of College IT resources and networks such as IT specialists contracted to Kenvale College.

The Chief Operations Officer is responsible for managing access privileges for users.

8.1 User Logins

Individual user logins are created for access to the following resources:

8.1.1 The College Network

8.1.2 The College’s Wireless Network

8.1.3 College web-based e-mail,

8.1.4 Student Management System; and

8.1.5 Student Learning Platform.

8.2 Hardware User Codes

There are user codes for the all the photocopiers on the College Network.

The process for creating these logins and codes can be found in *7-02-002 IT Administration Manual*.

8.3 Mobile Devices

Mobile devices including, but not limited to, laptop and netbook computers, mobile phones, smart phones and tablet devices, are all subject to the same policies and procedures as for other computing and communication devices.

In addition, College supplied mobile devices must be configured with a password or pin code in order to access the device. Preferably, a password or phrase should be used, but at a minimum, a four (4) digit PIN code is acceptable. This becomes essential if College data and/or email is held or accessed from the device.

8.4 Passwords

Passwords provide the first line of defence to the College computers and electronic devices. Passwords are not to be shared with, or used by, any other individual and failing to comply will be treated as a serious breach of system security which may result in disciplinary action.

It is important to use strong passwords. If passwords are too simple, hackers can easily guess or gather them, giving cybercriminals free access to the system. The stronger and more complex your passwords, the safer your network will be from a cyber-attack.

Passwords should:

- be at least 10 characters long
- not contain a complete word which easily links to you including your name, company name, family member or pet
- include a mix of upper-and lower-case letters, numbers and symbols
- be different from each other and from previous passwords
- change regularly
- be kept private
- be unique and hard to guess

8.5 Tips to create a strong password

It can help if you:

- make your passwords have meaning
- use the letters of a song, musical or movie title and change some of the characters to make a strong password. For example: Casino Royal 007 = C@s!n0r0y@Le7 or Les Miserable= L3$m!s3r@bLe
- use a password manager – this will create and securely store unique passwords for you
- don’t write passwords down on paper or store a list in a word document – they can be stolen and used to access your accounts
- select no when a computer offers to automatically remember your password when logging onto a website.

9. Applying a Risk Based Approach to Cyber Security

9.1 Using a risk management framework

The risk management framework has the following six steps:

9.1.1 Define the system

When embarking upon the design of a system, the type, value and security objectives for the system, based on confidentiality, integrity and availability requirements, should be determined. This will ultimately guide activities such as selecting and tailoring security controls to meet those security objectives and determining the level of residual risk that will be accepted before the system is authorised to operate.

9.1.2 Select security controls

Each cyber security guideline discusses security risks associated with the topic it covers. Paired with these discussions are security controls that the ACSC considers to provide efficient and effective mitigations based on the security objectives for a system.

While security risks and security controls are discussed in the cyber security guidelines, and act as a security control baseline, these should not be considered an exhaustive list for a specific activity or technology. As such, the cyber security guidelines provide an important input into each organisation’s risk identification and risk treatment activities however do not represent the full extent of such activities.

While the cyber security guidelines can assist with risk identification and risk treatment activities, organisations will still need to undertake their own risk analysis and risk evaluation activities due to the unique nature of each system, its operating environment and the organisation’s risk tolerances.

Following the selection and tailoring of security controls for a system, they should be recorded along with the details of their planned implementation in the system’s system security plan annex. In addition, and as appropriate, security controls should also be recorded in both the system’s incident response plan and continuous monitoring plan.

9.1.3 Implement security controls

Once suitable security controls have been identified and agreed upon for a system, they should be implemented.

9.1.4 Assess security controls

Assess security controls for the system and its operating environment to determine if they have been implemented correctly and are operating as intended.

9.1.5 Authorise the system

Authorise the system to operate based on the acceptance of the security risks associated with its operation.

Before a system can be granted authorisation to operate, sufficient information should be provided to the authorising officer in order for them to make an informed risk-based decision as to whether the security risks associated with its operation are acceptable or not. This information should take the form of an authorisation package that includes the system’s system security plan, incident response plan, continuous monitoring plan, security assessment report, and plan of action and milestones.

The authorising officer at Kenvale College is the Chief Operations Officer who has an appropriate level of seniority and understanding of security risks they are accepting on behalf of the College.

9.1.6 Monitor the system

Regular monitoring of cyber threats, security risks and security controls associated with a system and its operating environment, as outlined in a continuous monitoring plan, is essential to maintaining its security posture. In doing so, specific events may necessitate additional risk management activities. Such events may include:

- changes in security policies relating to the system
- detection of new or emerging cyber threats to the system or its operating environment
- the discovery that security controls for the system are not as effective as planned
- a major cyber security incident involving the system
- major architectural changes to the system.

10. Safeguarding Information

To ensure the confidentiality and security of staff and student personal information contained on the College's IT facilities, it is essential that only those authorised to access such data are permitted to do so.

Anyone, staff or student, who gains access to such personal information through methods other than those granted by the Chief Operations Officer shall be deemed as unauthorised and subject to disciplinary action.

Staff should be aware of their legal and corporate responsibilities in relation to appropriate use, sharing or releasing of information to another party. Any other party receiving restricted information must be authorised to do so and that the receivers of the data also adopt information security measures to ensure the safety and integrity of the data.

10.1 Electronic Document Storage

All information prepared, stored and distributed using the College network is a valuable asset to the College and requires safeguarding.

The College systems have safeguards that provide an appropriate level of security to store, process and distribute sensitive or valuable information. For more information regarding the management of electronic records, please refer to *10-01-002 Records Management Policy*.

10.2 Web-based Electronic Information Storage

In order to provide adequate assurance against risks relating to web-based electronic information storage and transfer, the Chief Operations Officer must take into consideration the arrangements for transfer of personal information to a relevant location out of Australia from a risk and compliance perspective, including CLOUD services and back-up servers hosted in other countries.

The Chief Operations Officer must review and maintain all standard agreements used for the acquisition of goods and services where personal information is provided to or obtained from the service provider located outside of Australia, to confirm;

10.2.1 How College information will be handled,

10.2.2 Whether College information is likely to be sent overseas and where, and

10.2.3 What processes and mechanisms are available to the College should there be a breach of privacy.

For more detailed information regarding the College's obligations with regards to information storage and transfer overseas, please refer to the *Privacy Act 1988*.

10.3 Protection of IT Assets

Damage to, or loss of, IT assets puts the College at risk. The Chief Operations Officer is responsible for ensuring that procedures and guidelines in place provide adequate assurance for the protection of all IT assets from damage or loss.

For more information regarding the College's procedures and guidelines for the protection of IT assets, please refer to *7-02-001 Use of IT Manual* and *7-02-002 IT Administration Manual*.

10.4 Data Breach Notifications

In the event that personal information is lost or subjected to unauthorised access, modification, disclosure or other misuse or interference, *the Privacy Amendment (Notifiable Data Breaches) Act 2017* requires a response to minimise risk and/or harm that can be caused by the compromised data.

The College's data breach response plan can be found in *7-02-007 Data Breach Response Plan*.

10.5 Cloud Storage

Administration of cloud-based infrastructure, systems and applications brings different challenges and may require a different approach. As such, not all security controls within this document may be directly applicable to the administration of cloud assets and may require assessment and adjustment before being applied to infrastructure used for cloud administration.

10.6 End-Point Security and Antivirus Software

All College PCs and laptops have end-point security software installed which has an automatic pattern update feature enabled. This is to ensure that the software is kept updated for the latest threats. There are also antivirus systems in place checking all incoming email into the organisation and also on internally circulating emails.

It is expected that any non College PCs and / or laptops also have current updated antivirus software installed, and it is the owners / users responsibility to ensure this. Not having current updated antivirus software installed exposes the College systems and infrastructure to potentially significant disruption and damage due to virus infected computers. All non-college PC’s and laptops that require connection to the college server will need to be registered with the Chief Operations Officer.

10.7 Removal of Equipment

No computer equipment can be removed from the College premises unless specific authorisation has been received by the Chief Operations Officer. This does not apply to laptop or notebook computers where one of their primary purposes is to allow the custodian to work while away from their normal working location.

Any equipment taken from the College without appropriate authorisation will be in direct violation of this policy and appropriate misconduct and / or legal action will be taken.

10.8 Allowing Access

Any non-College issued laptop or portable device connected to the College network is the responsibility of the owner. Kenvale College will take no responsibility for virus or other damage that may be caused by being connected to the network.

Since portable and hand held devices are more and more common, it is necessary that to allow for their use on the network. The College will not be obliged to enter into any other support arrangements for non-College owned devices.

10.9 Reporting Security Problems

Any suspected inappropriate or illegal usage of the College Information services network and equipment should be reported to the Chief Operations Officer for investigation.

10.10 Monitoring and Reporting

Jam Cyber are contracted to monitor all aspects of the College network and associated infrastructure. They are also able to report any suspected inappropriate and / or illegal activity to the Chief Operations Officer for further investigation.

It is also the role of Jam Cyber to actively monitor and analyse all network related activity included, but not restricted to, Internet Usage, email and dissemination and use of programs and data across the College network infrastructure.

This monitoring will be done for the sole purpose of identifying and responding to any suspected inappropriate activity.

All information reported to the Chief Operations Officer shall be treated in the strictest confidence.

10.11 Backup Requirements

All major systems within the College computing infrastructure are backed up on a regular basis by Jam Cyber. Jam Cyber have a Backup Strategy which details the frequency of backups. It is also strongly advised that all users save their work to the College share drive as this is backed up and any loss or damage to files can often be rectified by the restoration of the files from an existing backup.

10.12 Change Control

To ensure that the IT facilities and services running within the College infrastructure are maintained and kept running at maximum performance and functionality, it is often a requirement to perform maintenance and upgrades to equipment. To ensure that there is minimal disruption to essential services, appropriate Change Control procedures are to be followed. This is to ensure that the disruption is kept to a minimum and appropriate roll back procedures exist should there be issues during the system changes.

10.13 Business Continuity Plan

In the event of a disaster that impacts the IT infrastructure and / or services, the implementation of 8-02-009 Business Continuity Plan is essential. The Plan provides step by step procedures and processes required to ensure that services are returned to normal operation in the shortest possible time.

11. Application

11.1 This policy covers all users of the College network and IT resources including all staff, temporary staff, students, consultants and contractors as well as other third parties.

11.2 For further procedural information, please refer to the *7-02-001 Use of IT Manual*.

11.3 In line with AQF (2013), this policy will be applied consistently and fairly.

12. Responsibilities

12.1 The College's IT Department is responsible for the management of this policy.

12.2 The College's Chief Operations Officer is responsible for the application of this policy, where applicable.

13. Quality and Compliance

13.1 This policy will be reviewed and updated every three years or whenever there are changes applicable by the IT Department to ensure the quality and relevance of its content, and to maximise the effectiveness of its application to both the students and the needs of industry.

13.2 This policy has been developed in full consideration of the *Privacy Act 1988* and the obligations it imposes on the College.

13.3 The following legislation and compliance regulations apply to this policy:

Standards for Registered Training Organisations (RTOs) 2015	
Standard 4	Accurate and accessible information about an RTO, its services and performance is available to inform prospective and current learners and clients. Clause 4.1 Information, whether disseminated directly by the RTO or on its behalf, is both accurate and factual, and: • accurately represents the services it provides and the training products on its scope of registration • includes its RTO Code • refers to another person or organisation in its marketing material only if the consent of that person or organisation has been obtained • uses the NRT Logo only in accordance with the conditions of use specified in Schedule 4 • makes clear where a third party is recruiting prospective learners for the RTO on its behalf • distinguishes where it is delivering training and assessment on behalf of another RTO or where training and assessment is being delivered on its behalf by a third party • distinguishes between nationally recognised training and assessment leading to the issuance of AQF certification documentation from any other training or assessment delivered by the RTO • includes the title and code of any training product, as published on the National Register, referred to in that information • only advertises or markets a non-current training product while it remains on the RTO's scope of registration • only advertises or markets that a training product it delivers will enable learners to obtain a licensed or regulated outcome where this has been confirmed by the industry regulator in the jurisdiction in which it is being advertised • includes details about any VET FEE-HELP, government funded subsidy or other financial support arrangements associated with the RTO's provision of training and assessment, and

	• does not guarantee that: ○ a learner will successfully complete a training product on its scope of registration, or ○ a training product can be completed in a manner which does not meet the requirements of Clause 1.1 and 1.2, or a learner will obtain a particular employment outcome where this is outside the control of the RTO.
Standard 8	8.5.The RTO complies with Commonwealth, State and Territory legislation and regulatory requirements relevant to its operations. 8.6. The RTO ensures its staff and clients are informed of any changes to legislative and regulatory requirements that affect the services delivered..

Higher Education Standards Framework 2015	
Standard 2	2 Learning Environment 2.1 Facilities and Infrastructure 1. Facilities, including facilities where external placements are undertaken, are fit for their educational and research purposes and accommodate the numbers and educational and research activities of the students and staff who use them. 2. Secure access to electronic information and adequate electronic communication services is available continuously (allowing for reasonable outages for maintenance) to students and staff during periods of authorised access, except for locations and circumstances that are not under the direct control of the provider. 3. The learning environment, whether physical, virtual or blended, and associated learning activities support academic interactions among students outside of formal teaching.
Standard 6	6.2 Corporate Monitoring and Accountability 1. The provider is able to demonstrate, and the corporate governing body assures itself, that the provider is operating effectively and sustainably, including: e. risks to higher education operations have been identified and material risks are being managed and mitigated effectively f. mechanisms for competent academic governance and leadership of higher education provision and other academic activities have been implemented and these are operating according to an institutional academic governance policy framework and are effective in maintaining the quality of higher education offered i. there are credible business continuity plans and adequately resourced financial and tuition safeguards to mitigate disadvantage to students who are unable to progress in a course of study due to unexpected changes to the higher education provider's operations, including if the provider is unable to provide a course of study, ceases to operate as a provider, loses professional accreditation for a course of study or is otherwise not able to offer a course of study k. lapses in compliance with the Higher Education Standards Framework are identified and monitored, and prompt corrective action is taken.

	6.3 Academic Governance 1. Processes and structures are established and responsibilities are assigned that collectively: a. achieve effective academic oversight of the quality of teaching, learning, research and research training b. set and monitor institutional benchmarks for academic quality and outcomes c. provide competent advice to the corporate governing body and management on academic matters, including advice on academic outcomes, policies and practices.
Standard 7	7 Representation, Information and Information Management 7.2 Information for Prospective and Current Students 1. Accurate, relevant and timely information for students is publicly available and accessible, including access for students with special needs, to enable informed decision making about educational offerings and experiences. 2. Information for students is available prior to acceptance of an offer, written in plain English where practicable, accompanied by an explanation of any technical or specialised terms, and includes: b. information to assist in planning for and participation in educational and other activities, including contact points, advice about orientation and induction, delivery arrangements, technical requirements for access to IT systems for online activities, timetables, access to learning resources, avenues to participate in decision making and opportunities to participate in student representative bodies e. information to facilitate access to services and support including the types of services available such as educational resources including English language support, personal support services, cultural support and ancillary services, hours of availability, how to access services and emergency contact details where applicable. 7.3 Information Management 1. There is a repository of publicly-available current information about the higher education provider’s operations that includes: h. an overview of teaching campuses, facilities, learning resources and services provided for students 3. Information systems and records are maintained, securely and confidentially as necessary to: a. maintain accurate and up-to-date records of enrolments, progression, completions and award of qualifications b. prevent unauthorised or fraudulent access to private or sensitive information, including information where unauthorised access may compromise academic or research integrity c. document and record responses to formal complaints, allegations of misconduct, breaches of academic or research integrity and critical incidents, and c. demonstrate compliance with the Higher Education Standards Framework.

The National Code 2018	
6.1	The registered provider must support the overseas student in adjusting to study and life in Australia by giving the overseas student information on or access to an age and culturally appropriate orientation program that provides information about: 6.1.5 the registered provider's facilities and resources
6.4	The registered provider must facilitate access to learning support services consistent with the requirements of the course, mode of study and the learning needs of overseas student cohorts, including having and implementing documented processes for supporting and maintaining contact with overseas students undertaking online or distance units of study.

1. References

1.1 Australian Skills Quality Authority (ASQA). (2012). *Standards for VET Accredited Courses 2011*. Australia.

1.2 Australian Skills Quality Authority (ASQA). (2013). *Australian Quality Training Framework (AQTF): User's Guide to the Essential Conditions and Standards for Initial Registration.* Australia.

1.3 Australian Qualifications Framework Council, 2013, *Australian Qualifications Framework (AQF)*, second ed., South Australia.

1.4 Australian Skills Quality Authority (ASQA), 2015, *Standards for Registered Training Organisations (RTOs) 2015*.

1.5 Australian Skills Quality Authority (ASQA), Standards for Registered Training Organisations (RTOs) 2015 – *Financial Viability Risk Assessment Requirements.*

1.6 Australian Skills Quality Authority (ASQA), Standards for Registered Training Organisations (RTOs) 2015 – *Fit and Proper Person Requirements*.

1.7 Department of Education and Training (DET), 2007, *National Code of Practice for Registration Authorities and Providers of Education and Training to Overseas Students* (The National Code).

1.8 *Education Services for Overseas Students Regulations 2001 (Statutory Rules)* made under the *Education Services for Overseas Students Act 2000* and the *Education Services for Overseas Students (Consequential and Transitional) Act 2000*.

1.9 The Tertiary Education Quality Standards Agency (TEQSA) (2015). *Higher Education Standards Framework 2015*. Australia.

1.10 Australian Cyber Security Centre- Secure Administration 2020