# Guidance note: *Information Management*

 (June 2025)

|  |
| --- |
| Providers should note that Guidance Notes are intended to provide guidance only. The definitive instruments for regulatory purposes remain the TEQSA Act and the Higher Education Standards Framework as amended from time to time. |

## What does Information Management encompass?

In the context of the [*Higher Education Standards Framework (Threshold Standards) 2021*](https://www.legislation.gov.au/F2021L00488/latest/text)(Threshold Standards) information management refers to a provider’s overarching obligations to:

* make publicly available information about its operations and the courses it offers
* ensure its information management systems and records are securely maintained to prevent unauthorised access to private and sensitive information.

A provider’s primary obligations regarding information management can be found in section 7.3 of the Threshold Standards. The purpose of section 7.3 is to ensure providers:

* are transparent about their operations
* securely manage the information they hold and create
* where relevant, protect the confidentiality of information they hold and create.

While touched upon briefly in this guidance note, the following information is dealt with in greater detail through separate guidance notes:

* facilities, and infrastructure, covered by section 2.1 of the Threshold Standards. More information about information management as it relates to facilities and infrastructure is included in the [Facilities and Infrastructure Guidance note](https://www.teqsa.gov.au/guides-resources/resources/guidance-notes/guidance-note-facilities-and-infrastructure)
* information providers give prospective and current students, covered by section 7.2 of the Threshold Standards. More information is discussed in the Information for Prospective and Current Students Guidance note (for consultation).

## What TEQSA will look for

All the Threshold Standards are potentially relevant to information management. The most notable are the following:

|  |  |
| --- | --- |
| **Part A: Standards for HE Providers** | **Key considerations** |
| 2.1.2: Facilities and Infrastructure  | * students and staff have secure access to electronic and adequate communication services, with exceptions for reasonable outages and maintenance.
 |
| 6.2.1a, e: Corporate Monitoring and Accountability | * the governing body and entity comply with legislative requirements on creating, obtaining, protecting, and disclosing information. This may include the [*Privacy Act 1988*](https://www.legislation.gov.au/C2004A03712/latest/text), other privacy/data protection legislation, and freedom of information legislation.
* risks to information management systems or processes are identified, recorded, and managed.
 |
| 7.2: Information for Prospective and Current Students | * accurate, relevant, and timely information is publicly available and accessible for current and prospective students. This is to assist students in deciding whether to take up a particular course at a particular provider.
* where applicable, a provider’s CRICOS code and course code should be visible on information provided to students.
 |
| 7.3: Information Management | * there is a publicly available and accessible repository of information about a provider’s operations.
* information systems and records are maintained securely and confidentially.
* a provider’s records, including records about enrolment, progression, complaint handling, academic misconduct, course completion and award of qualifications, are accurate and up to date.
 |
| **Part B: Criteria for HE Providers** | **Key considerations** |
| B1.1.3 TEQSA Provider ID | * the TEQSA ID of a provider is included on [relevant public information](https://www.teqsa.gov.au/guides-resources/glossary-terms#r), allowing students to check a provider’s details against the [National Register](https://www.teqsa.gov.au/national-register).
 |

### Obligations of providers offering education to overseas students

Where it applies to a provider, TEQSA considers [*National Code of Practice for Providers of Education and Training to Overseas Students 2018*](https://www.legislation.gov.au/Details/F2017L01182)(National Code), and the [*Education Services for Overseas Students Act 2000*](https://www.legislation.gov.au/Details/C2022C00066)(ESOS Act). TEQSA does so in its role as the ESOS agency for registered higher education providers.

Sections of the National Code relevant to information management are:

* **2.1** – prior to accepting an overseas student or intending overseas student for enrolment a provider must make comprehensive, current, and plain English information available to students on a range of topics including, the minimum level of English proficiency, course duration, accommodation and an indication of costs for living in Australia.
* **3.6** – a provider must retain records of all written agreements as well as receipts of payments made by students under the written agreement for at least 2 years after they cease to be a student.
* **7.7** – the provider must maintain records of all requests from overseas students for a release and the assessment of, and decision regarding the request for 2 years after they cease to be an accepted student.

Sections of the [ESOS Act](https://www.legislation.gov.au/Details/C2022C00066) relevant to Information Management are **21(2B), 21(2C)** and **21(3).** These require a provider to retain records for a least 2 years after the student ceases to be an ‘accepted student’.

### Diligent management of student records

TEQSA also considers the [*Tertiary*](https://www.legislation.gov.au/Details/C2022C00066) *Education* [*Quality*](https://www.legislation.gov.au/Details/C2022C00004) *and Standards Agency Act 2011* (TEQSA Act).

TEQSA may request provider student records under Section 197AA of the TEQSA Act if the provider ceases to operate or its registration is cancelled.

Considering this, TEQSA expects providers to maintain accurate and up to date records of students’ enrolments, progression, and completion of qualifications. This ensures:

* students’ achievements are tracked
* students have greater certainty about the recognition of their qualifications
* if provider records are sent to TEQSA because it ceases to operate, TEQSA will hold the information it needs to issue a student record to impacted students.

### Making operational information publicly available

As noted above, under sections 7.2 and 7.3 of the Threshold Standards providers must make certain information about their operations publicly available. Providers are expected to maintain this information as part of a ‘repository of publicly-available current information’.

While the meaning of ‘repository’ is not defined in the Threshold Standards, it is expected this information will be in an easily accessible place, which can be accessed by members of the public. In most cases, the appropriate place for this information will be on a provider’s website.

One key purpose of including this information is to support current and prospective students in understanding:

* which provider may best suit their individual needs
* how they can contact the provider for more information or to raise concerns
* the provider’s registration status (so the student knows if there are any risks of not being awarded a legitimate qualification).

This information should be made available for students and other members of the public engaging with the provider to help them assess or understand:

* the scale and structure, including the governance structure, of the provider’s operations
* what establishing instrument applies to the provider and any obligations this imposes
* whether the provider’s operations appear sustainable
* which courses the provider delivers in partnership or under arrangement with other parties
* the financial standing of a provider
* how they should contact the provider
* how to make a complaint
* the accreditation status of the provider, which can be searched on the national register through their TEQSA ID number.

### Course information should help students make informed decisions

The Threshold Standards set out the minimum amount of information a provider must provide in its repository about its courses. This is to allow students to have the information needed to compare different educational offerings and make an informed choice about which, if any, to take up.

The course information a provider should make available includes:

* **general information** – details of the qualification, including if it is offered to international students, duration of the course, and if the course is accredited.
* **technical information** – is the course recognised by a professional accreditation body, information about course credits, and recognition of prior learning.

Information about enrolment numbers should give prospective students an indication of the scale of the provider and learning environment. The information should be based on recent actual enrolments in the case of an existing course, or realistic projections in the case of a new course (a range can be used, e.g. ‘we expect to enrol between x and y students’). In the case of nested courses, the numbers should be for the course with the highest AQF level.

### Record keeping requirements in the *TEQSA Act* and the *Tuition Protection Guidelines*

The TEQSA Act, section 30, sets expectations on providers to keep adequate records relevant to their compliance with the TEQSA Act. This is so providers, upon request, can produce information to demonstrate that they are complying with their other obligations under the TEQSA Act.

The [Tuition Protection Guidelines](https://www.legislation.gov.au/Details/F2022C00103), section 11 (linked to section 26A of the TEQSA Act), obliges providers to retain records for the purpose of tuition protection.

### Protecting and securing information

Protecting staff and student information, as well as the intellectual information contained in research outputs (where applicable) and other sensitive information, should be a key priority for a provider’s corporate governing body. This is particularly important because of the constantly evolving threats to information management, including unauthorised access, data breaches and malware.

Providers are also subject to the [*Privacy Act 1988*](https://www.legislation.gov.au/C2004A03712/latest/text)(Privacy Act), which sets out a range of obligations to promote and protect the privacy of individuals. Notably, the Privacy Act sets out the [13 Australian Privacy Principles (APPs)](https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines) that apply to many organisations receiving, recording, using, and disclosing [personal information](https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/handling-personal-information/what-is-personal-information).

A corporate governing body should also carefully consider and oversee arrangements to manage cyber security risks. This includes compliance with the [Notifiable Data Breaches scheme](https://www.oaic.gov.au/privacy/notifiable-data-breaches/about-the-notifiable-data-breaches-scheme) and [*Security of Critical Infrastructure Act 2018 (SOCI).*](https://www.legislation.gov.au/C2018A00029/latest/versions)

The NDB requires an organisation subject to the Privacy Act to notify affected individuals and the Office of the Australian Information Commissioner (OAIC), when a data breach is likely to result in serious harm to the individual whose personal information is involved. The SOCI places enhanced cyber security obligations on operators of critical infrastructure deemed as a system of national significance. This includes providers of higher education and research to:

* develop cybersecurity incident response plans to prepare for a cyber security incident
* undertake cyber security exercises to build cyber preparedness
* undertake vulnerability assessment to identify vulnerabilities for remediation
* provide system information to develop and maintain a near real-time threat picture.[[1]](#footnote-2)

Providers should consider joining the Australian Signals Directorate’s Partnership Program, or its Business Partnership, to access the most current cyber security information and share information and resources. Relevant resources are also available from:

* The Australian Government’s Department of Home Affairs, which administers [the Cyber and Infrastructure Security Centre](https://www.cyber.gov.au/).
* The [Department of Education](https://www.education.gov.au/guidelines-counter-foreign-interference-australian-university-sector/cybersecurity), which provides advice and guidance on cyber security issues as part of its Guidelines to Counter Foreign Interference.

## Identified issues

Within the context of the Threshold Standards, TEQSA has identified a range of issues that are indicative of risks regarding information management, including:

* Quality and availability of information
	+ providers’ storage of personal information is not subjected to robust quality assurance to ensure it remains accurate and up to date
	+ no information or limited information about a provider’s operations is available to the public, making it difficult for students to make informed decisions about engaging with the provider
	+ course information is incomplete and does not disclose enough information to allow students to make an informed decision about whether to take up a particular course
	+ limited publicly available information available about a provider’s third-party arrangements
	+ published information is outdated and does not reflect changes to a provider’s operations.
* Storage and maintenance of information
	+ due to inadequate systems or lack of knowledge amongst key staff, student data is not collected, stored, used, disclosed, and disposed of in line with the requirements of the provider’s policies. This may result in the provider being in breach of relevant local, state, Commonwealth and international legislation
	+ providers are unable to ensure information collected and stored by third-parties about its students is adequately stored and maintained
	+ there is inadequate security on the provider’s electronic information/communication services leaving students and staff vulnerable to cyberattacks.

## Related resources

* [Guidance note: Facilities and Infrastructure](https://www.teqsa.gov.au/guides-resources/resources/guidance-notes/guidance-note-facilities-and-infrastructure)
* Guidance Note: Information for Current and Prospective Students (for consultation)
* Guidance Note: Corporate Monitoring and Accountability (in development)
* [Tuition Protection (Up-front Payments Guidelines) 2020](https://www.legislation.gov.au/Details/F2022C00103)
* [Office of the Australian Information Commission – information about the *Privacy Act 1988* (Cth)](https://www.oaic.gov.au/privacy/the-privacy-act)
* [Enhancing Cyber Security Across Australia’s University Sector: Final Report - Department of Education, Australian Government](https://www.education.gov.au/guidelines-counter-foreign-interference-australian-university-sector/resources/enhancing-cyber-security-across-australias-university-sector-final-report)
* [About the Notifiable Data Breaches scheme | OAIC](https://www.oaic.gov.au/privacy/notifiable-data-breaches/about-the-notifiable-data-breaches-scheme)
* [Essential Eight Explained | Cyber.gov.au](https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-explained)

| **Version #** | **Date** | **Key changes** |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

1. [Security of Critical Infrastructure Act 2018 (SOCI) (cisc.gov.au)](https://www.cisc.gov.au/legislation-regulation-and-compliance/soci-act-2018#:~:text=The%20SOCI%20Act%20protects%20information,complies%20with%20the%20SOCI%20Act.) [↑](#footnote-ref-2)