XYZ University is a medium-sized tertiary education provider in the state of Queensland, Australia. In undertaking its normal business of teaching, learning, and research, the university collects, stores, and uses “personal information,” that is, anything that identifies a person’s identity.

With respect to students, this information may include, among other things, records relating to admission, enrollment, course attendance, assessment, and grades; medical records; details of student fees, fines, levies, and payments, including bank details; tax file numbers and declaration forms; student personal history files; qualifications information; completed questionnaire and survey forms; records relating to personal welfare, health, equity, counseling, student and graduate employment, or other support matters; records relating to academic references; and records relating to discipline matters.

The bulk of this information is retained in the student management information systems and in the file registry. Academic and administrative staff, at various levels, have access to these records only as required to carry out their duties. Portions of the information held in university student records are disclosed outside the university to various agencies, such as the Australian Taxation Office; the Department of Education, Employment and Workplace Relations; other universities; consultant student services providers; the Department of Immigration and Citizenship; and overseas sponsorship agencies.

The university has a well-documented information privacy policy in accordance with the community standard for the collection, storage, use, and disclosure of personal information by public agencies in Queensland. The policy relies on the 11 principles developed in the Commonwealth Privacy Act of 1988. These principles broadly state the following:

Personal information is collected and used only for a lawful purpose that is directly related to the collector’s function.

Before the information is collected, the individual concerned should be made aware of the purpose, whether it is required by law, and to whom the information will be passed on.

Files containing personal information should be held securely and protected against loss; unauthorized access, use, modification, or disclosure; or any other misuse.

Personal information can only be disclosed to another person or agency if the person concerned is aware of it and has consented and the disclosure is authorized or required by law.

Personal information should not be used without taking reasonable steps to ensure that it is accurate, up to date, and complete.