Proposed changes to Queensland's Information Privacy Framework

Comments are provided in response to the nine questions posed for agencies in the Agency Consultation Paper that was provided to QUT's Vice-Chancellor and President on 8 July 2022 by Shannon Fentiman MP (Attorney-General and Minister for Justice).

The Privacy Office in Governance, Legal and Performance have compiled this response.

A new mandatory data breach notification (DBN) scheme for Queensland

Question 1. What are the benefits of a mandatory DBN scheme to your clients?

Applying a mandatory data breach notification scheme to QUT would align with student and community expectations. Our students and community partners are aware that most health, government, and commercial services have a mandatory requirement to notify them about eligible breaches of their privacy. It would be reasonable for them to expect that the same legal obligation applies to QUT.

Question 2: What are the benefits of a mandatory DBN scheme to your agency and the public sector, or any other benefits?

QUT is subject to the mandatory data breach notification under Part IIIC of the *Privacy Act 1988* (the NDB Scheme), the *My Health Records Act 2012,* and where under contact to the Commonwealth or an Australian Privacy Principles (APP) entity that involves the handling of personal information. The University's privacy breach management protocol currently involves voluntary notification to individuals and the Office of the Information Commissioner (OIC) following an assessment of the harm to individuals caused by any reported privacy breach.

The risk assessment is based on the Notifiable Data Breaches (NDB) scheme, and the guidance issued by the OIC. The introduction of a mandatory scheme would provide a legal framework supporting the University's breach management procedures and assist with contract compliance where a third-party service provider is involved.

Question 3. Are there any disadvantages of a mandatory DBN scheme for your clients or your agency (apart from any resource impacts which are discussed below)

No significant disadvantages are foreseen, other than those that might apply to notification schemes more generally where over-reporting may lead to public indifference to the advice.

Operation Impala noted that individuals whose personal information was misused lacked awareness about what action to take and where to obtain support[1]. A mandatory DBN scheme would require QUT and other Queensland agencies to provide basic awareness and support, but it would further assist individuals if trusted third parties with privacy breach and identity theft expertise were available to provide support where a major privacy breach occurred.

Question 4. What steps would your agency need to take to prepare to implement a mandatory DBN scheme in your agency?

A mandatory scheme would require limited changes to privacy breach procedures, an update to staff training, and a review of model contracts for service providers.

[1] Crime and Corruption Commission Qld (2020). *Operation Impala: Report on misuse of confidential information in the Queensland public sector.* p. 133.

Question 5. Do you anticipate any resource impacts for your agency through implementing a mandatory DBN scheme? If you do, please outline what these would be?

The resource implication of a mandatory DBN scheme would be limited to making minor changes to QUT's existing privacy breach procedure and training materials.

A single set of privacy principles based on the APPs in Queensland (the Queensland Privacy Principles) to replace the IPPs and NPPs

Question 6. What would be the benefits for your agency of adopting a single set of privacy principles?

A single set of privacy principles would mean alignment between the privacy compliance framework that regulates the Commonwealth, a primary source of funding for QUT, and the privacy regulation that applies to the University as a Queensland state agency. Commercial dealings with service and funding providers that involve the handling of personal information would also be simplified.

Question 7. What would be the benefits to your clients of adopting a single set of privacy principles?

There would be greater simplicity for our students who are aware of the way that APPs regulate the use of their personal information in commerce, health, and federal government services.

Question 8. What steps would your agency need to take to prepare to implement the QPPs in your agency?

QUT would analyse the QPP's alignment with the current IPPs and, considering any advice from the Information Commissioner and the Queensland Government, amend its information privacy policy and procedures, update resources to support staff privacy awareness, and assess and where necessary revise existing information handling practices. A recommended implementation plan could be expected to include actions that address each of the QPPs.

- QPP1: QUT would expect to be compliant with QPP1, having an approved and well-understood information privacy policy, privacy procedures and information handling practices that comply with the *Information Privacy Act 2009*. Policy and procedures will require review and amendment to account for differences with the IPPs.

- QPP2: QUT only deals with students or staff anonymously or pseudonymously in rare circumstances. This is where the law permits anonymity or pseudonymity, or where the University decides that a process is enhanced by it (e.g. student or staff opinion surveys). Providing an option for individuals to deal with the University in this way would require an assessment of existing practices and an update to policy, collection notices and guidance issued to staff.

- QPP 3: Except for personal information collected in approved research involving human subjects, QUT collects sensitive information (as defined in section 6 of the *Privacy Act 1988*) only where it has a necessary, lawful, and fair purpose to use that information (IPP1). Although a notice is provided in accordance with IPP2, QUT collection practices do not require it to obtain consent or to record and manage that consent. QPP3 would require a review of existing practices and collection notices and the development of new consent management procedures and systems for the collection of sensitive information for QUT business purposes.

- QPP4: QUT's normal practice is to collect, use and store personal information only where it is required to fulfill a university function. Disposal of personal information contained in public records is managed according to the *Public Records Act 2002*. QPP4 would require an assessment of

information handling practices to evaluate the unsolicited collection of personal information and how best to deal with it.

- QPP5: Implementation would require a review of QUTs existing collection practices and notices for information collected by third parties and used by QUT. Personal information is supplied to QUT from a variety of sources in support of its functions, for example by the Queensland Tertiary Admissions Centre (QTAC), schools, industry partners, employers, and scholarship providers. In most cases QUT provides privacy notices to the individuals after receipt of their personal information, however it will be necessary to assess third-party collection and whether current notification practices comply with QPP5.

- QPP6: The removal of the exception permitting QUT to use or disclose personal information it collects for public interest research could restrict the ability of academic researchers, for example in the field of learning and teaching, to use data for research publications. QUT recommends that the public interest research exception contained in IPP10(1)(f) and IPP11(1)(f) be included in QPP6.

- QPP7: Personal information is frequently managed outside of Australia in cloud-hosted digital applications. These arrangements are subject to contracts that bind the service provider to the same privacy standards that apply to QUT. QPP7 would require a review of existing contracts, and an update to model contracts and to the advice provided to staff involved in the procurement of digital services and products.

- QPP8: Review policies, procedures, and systems. No major change expected.

- QPP9: QUT would review its of existing information security policy and procedures, including guidance and training to staff on disposal and de-identification of personal information where it is no longer required and does not form part of a public record.

- QPP10: QUT would need to review its existing administrative access schemes and where new time limits are applied, conduct an audit of the existing schemes.

- QPP11: QUT would review procedures for amendment and correction of personal information and audit compliance where new minimum time limits are applied.

Question 9. Do you anticipate any resource impacts for your agency through implementing the QPPs? If you do, please outline what these would be?

QUT would anticipate assigning resources to manage the implementation of the QPPs. The level of resources required have not been assessed in detail. At minimum, the resources would be required to:

- review existing privacy policy and procedure
- refresh existing privacy training
- assess and where necessary revise privacy collection notices
- assess and where necessary revise current process involving the collection, use and disclosure of sensitive information for compliance with the QPPs
- assess public interest research where that involves the use of personal information that has been collected for a QUT business purpose
- assess compliance risk in existing ICT contracts, and review model service provider contracts, seeking legal advice where necessary.