THRESHOLD PRIVACY ASSESSMENT QUESTIONS

This document supports the University's Privacy Impact Assessment (PIA) Procedures.
Complete it for all new or changed projects, technology & digital systems, products, services, programs and/or initiatives ("activities").

The staff member or project manager facilitating the activity should answer the questions below. If in doubt, seek advice from the Privacy Officer privacy@westernsydney.edu.au

*"**Personal information**" means **any** information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion.*

If the answer to one or more of the questions below is "yes", you must complete a Privacy Impact Assessment.

1. Will the activity involve the collection of personal information (compulsory or otherwise)?
   "Collection" might be through any means, e.g. the University's website, by phone or text, digital chat functions, databases, surveys, interviews, membership applications, attendance lists, registrations, donations, staff recruitment, student enrolments, etc.

2. Will the activity involve a new use for personal information that is already held by the University or a third party on the University's behalf?
   Such use might be "bundled consent" and might not meet the criteria of valid consent

3. Will the activity involve any change to how personal information will be managed, shared internally, linked, matched or stored within the University or by a third party on the University's behalf?
   For example, will new or additional personal information be recorded in a Customer Relationship Management system, along with other information about that individual?

4. Will the activity involve any change to how personal information will be disclosed outside of the University or a third party acting on the University's behalf?
   'Disclosed' includes publishing on the website or releasing to third parties. This might include for research or statistics, de-identified or otherwise.

5. Will the activity involve restricting access by individuals to their own personal information?

6. Will the activity involve the creation of a new identification system?
   For example, a new way of identifying or verifying students, staff or others?

7. Will the activity involve surveillance, tracking or monitoring of individuals' movements, behaviour or communications?
   For example, using CCTV, location-tracking devices in vehicles or mobile devices, or cookies on websites.

8. Will the activity involve any other measures that may affect the privacy of an individual's personal information, body or property, behaviour or communications?

9. Will the activity involve any of the following features, which would make it an inherently 'high risk' project?

   a. Volume: High number of individuals affected

   b. Type of people: Anything involving people under 16 years of age or people of potentially vulnerable populations (e.g. prisoners, people with intellectual disabilities or who lack capacity, or otherwise disadvantaged communities)

   c. Type of information: Anything involving:
      i. evidence of identity documents (e.g. driver licence or passport)
      ii. other government-issued unique identifiers (e.g. Centrelink customer reference number, Medicare number, Individual Healthcare Identifier (IHI), Tax File Number)
      iii. biometrics
      iv. genetic information
      v. communications metadata
      vi. precise geolocation data
      vii. other types of location data the disclosure of which could put the person at risk of physical harm (e.g. the home address of a person escaping family violence)
      viii. neuro-measurement (such as emotional response analysis)
      ix. health information (including information about health, health services and disability); or
      x. 'sensitive information' (information relating to an individual's ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership or sexual activities)

   d. Type of sharing: Anything involving the sale of data (other than as part of the sale or merger of an on-going business), or data-sharing, data-linkage or data-matching across different organisations, especially if involving cross-border data flows (i.e. personal information to be disclosed outside Australia)

   e. Type of technology: Anything involving emerging technology, Internet of Things, connected or autonomous vehicles, artificial intelligence or machine learning

   f. Degree of personalisation to influence behaviour or decisions: Anything involving predictive analytics, profiling, or the promotion of personalised content, at a large scale

   g. Type of change: Any change which will:
      i. involve a particularly novel collection or use of personal information
      ii. diminish access or correction rights
      iii. reduce individuals' controls or choices over the handling of their personal information; or
      iv. lessen existing levels of data security or data quality (integrity, accuracy or confidentiality)

   h. Type of collection: Anything involving covert collection, or systematic / large-scale surveillance, monitoring, behavioural or other tracking, or the collection of publicly available data at a large scale (such as 'scraping' data from websites)

   i. Type of processor: Anything involving contracted service providers

   j. Type of function: Anything involving law enforcement or national security functions or powers

   k. Type of outcome: A project that will lead to decision-making (automated or otherwise) about individuals at a large scale (e.g. development of algorithms, use of data analytics, creation or application of risk profiles, financial/social scoring, screening applications or making behavioural predictions) with potential legal or significant effects for some individuals (e.g. if it could have an impact on an individual's: safety such as medical implants; ability to obtain or retain employment; ability to obtain or retain a right, entitlement, service or significant benefit including welfare benefits, insurance, housing or credit; access to public or critical services; physical, mental or financial well-being; or reputation)

l. Type of impact: Any change that could have:
   i. negative consequences for one or more individuals, including physical or mental wellbeing, reduced access to public or critical services, discrimination, financial loss or identity theft; or
   ii. a significant collective impact on society, such as increased surveillance and monitoring activities, or the establishment of sensitive personal information sharing arrangements between the government agencies and other entities
   iii. Type of legal authority: Any change which requires legislative amendment to support it, or which will modify the effect of the privacy principles.
   iv. Expectations: Anything likely to raise stakeholder or public concerns about dataflows or the use of personal information beyond their reasonable expectations which would affect the University's social licence for the project (e.g. if the project has already been covered in the media, if a similar project by this or another organisation raised stakeholder or public concerns or pushback, or if your organisation does not have a high level of pre-existing customer trust or community support), or
   v. On advice or recommendation from the NSW Privacy Commissioner.

If the answer to one or more of the questions above was "yes", you must complete a Privacy Impact Assessment.

privacy@westernsydney.edu.au
May 2023