Information Privacy Guide - Policy Guideline

1 Intent

a) The intention of the Information Privacy Guide - Policy Guideline (this Guideline) is to —

i. provide context to those individuals engaging the University in relation to Personal information;
ii. provide more detailed definitions and information in support of the policy;
iii. provide contact details for individuals seeking to lodge a Privacy Request in relation to their Personal Information or the University's management of Personal Information;
iv. provide a general awareness on the University's processes for assessing and managing data breaches.

b) In this Guideline:

2 Applicability of legislation and policy

a) The University is not subject to the Privacy Act 1988 (Commonwealth), except in certain circumstances in relation to a specific type of information (i.e. Tax File Numbers) or information obtained in respect of a specific purpose (i.e. under Part 3 and 4 of the Higher Education Support Act 2003 (Commonwealth)).
b) The University's Information Privacy Policy however uphold the University's aim to apply the Australian Privacy Principles to its management of Personal Information.
c) The University must maintain records in accordance with the State Records Act 2000 (WA) and the relevant published Disposal Authorities. This may require the University to retain personal information longer than is required for the purposes it was collected as it forms part of a required university record.
d) The University will review and consider the applicability of other jurisdictions' privacy laws, as part of the University's engagements with individuals, organisations or service providers.

3 Definitions of Personal and Sensitive Information

a) The University aligns its definitions of personal and sensitive information with that of the Privacy Act 1988 (Commonwealth).
b) Personal information may include, but is not limited to —

i. name;
ii. address (residential, postal and email);
iii. phone number;
iv. date of birth;
v. gender;
vi. ethnic origin;
vii. passport number;
viii. banking and credit card details;
ix. tax file number;
x. health or impairment information;
xi. emergency contact details;
xii. photographs or video recordings (including CCTV footage);
xiii. criminal history;
xiv. academic record;
xv. IT access logs;
xvi. records of donations or transactions;
xvii. employment details;
xviii. geospatial /location details; and
xix. telecommunications metadata.

c) Sensitive information means information that is personal, that is also information or an opinion about an individual's —

i. racial or ethnic origin;
ii. political opinions;
iii. membership of a political association;
iv. religious beliefs or affiliations;
v. philosophical beliefs;

vi. membership of a professional or trade association;
vii. membership of a trade union;
viii. sexual orientation or practices; or
ix. criminal record;
x. health information about an individual; or
xi. genetic information about an individual that is not otherwise health information; or
xii. biometric information that is to be used for automated biometric verification or biometric identification; or
xiii. biometric templates.

4 Disclosure of Personal Information in Emergencies

a) The University may disclose Personal Information to police, medical or hospital personnel, civil emergency services, or other person assessed as necessary to respond in the case of an emergency where —

i. it is unreasonable or impracticable to obtain consent; and
ii. the University reasonably believes that disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of an individual, or to public health or safety.

5 Disclosure to third party service providers

a) The University discloses Personal Information to third party service providers, including providers of cloud services and website hosts, which may be located overseas. In these cases such disclosure will only be for the purposes of providing services to the University, or University Community, and limited to only such Personal Information that is necessary to provide such services on behalf of the University. Providers will be required to collect, store and disclose Personal Information only as authorised by the University and only in direct relation to the primary purpose the Personal Information was collected.

b) In this case, the University will ensure it has a contract that requires that the third party complies with the Australian Privacy Principles and with the State Records Commission Standard 6: Outsourced Functions as articulated in the University's Recordkeeping Plan.

6 Management of Personal Information – reasonable steps

a) The University will take reasonable steps to ensure the protection of Personal Information in accordance with the University's Information Privacy Policy. Personal Information will be protected proactively and by design.

b) The University will take reasonable steps to —

a. destroy or de-identify Personal Information which is no longer needed for University processes or required to be retained under any law, regulation or code applicable to the University;
b. ensure that the Personal Information it collects, uses or discloses (having regard to the purpose of the use or disclosure) is relevant, adequate but not excessive, is accurate, up to date and complete;
c. ensure that the systems, tools and methods of capturing, transmitting and holding information are protected from misuse, interference, loss and from unauthorised access, modification or disclosure; and

d. ensure Personal Information is protected with integrity, confidentiality and with appropriate security.

c) However, the University cannot be held responsible for the theft of data by a third party, or the loss of data through technical or technological malfunction, tampering by a third party, or any event that is beyond the reasonable control of the University

6.1 University Employees

a) Guidance for all employees on the implementation and management of Personal Information in accordance with the Framework, the Information Privacy Policy and these Guidelines can be obtained from the Information Governance Team, Office of Strategy, Planning and Performance.
b) The University assigns specific Information Governance roles to employees, who are accountable and responsible for the implementation and management of this Policy. These Information Stewards and Information Custodians provide localised direction and support to employees handling Personal Information in context of their business function.
c) Employees will be educated around the policies and procedures for handling Personal Information and identifying and reporting a data breach. Employees will be made aware of circumstances that might give rise to a data breach, such as:
    i. lost or stolen employee equipment;
    ii. employees accessing information where they were unauthorised to do so, whether intentionally or by accident;
    iii. records being stolen from storage or disposal units; or
    iv. employees mistakenly granting access to information to unauthorised third parties.

7 Privacy Collection Notices

a) A Privacy Collection Notice must advise the individual of the primary purpose for which the information is being collected, the type of organisations to which the information may be disclosed, the relevant rights of the individual, who to contact and any other salient information which demonstrates the University's transparency and integrity when collecting, using and disclosing Personal Information.
b) The privacy collection notice is not exhaustive and provides a practical summary at the point of data collection.
c) The University's standard privacy collection notices can be found at –
    i. UWA Student Personal Information Privacy Collection Notice;
    ii. UWA Staff Personal Information Privacy Collection Notice; and
    iii. UWA Medical Health Records Privacy Collection Notice.

8 Website Privacy

a) The University uses digital cookies to deliver you a personalised experience on its websites. The University uses Google Analytics and other analytics services for the purpose of evaluating online activity and improving your personalised experience online.
b) Analytics services use cookies which transmit information on your use of the website to a cloud service that may not be within Australia. This information may transfer to third parties where required by law, or where such third parties process the information on the service's behalf.
c) The University website may also employ Facebook Insights. This provides aggregated, non-personally identifiable information to page owners and platform developers.

d) The University may use re-targeting advertising to deliver to content, including advertisements to those who have previously visited one of its websites. Google, Facebook and other advertising companies may serve you advertisements from the University. Contact UWA Marketing if you have any concerns about the University's advertisements through re-targeting.
e) By using UWA websites or other University digital channels, you consent to the processing of data about you by Google in the manner and for the purposes set out above. You may refuse the use of cookies by selecting the appropriate settings on your browser; however, please note if you do this you may not be able to use the full functionality of certain UWA website or receive a personalised experience.

9 Breach of Policy

a) The University accepts that breaches of this policy may occur, and individuals whether employees or members of the University community should be able to report these, so they may be investigated. Breaches of the policy may include –

i. where an individual feels the University has failed to collect, use, or manage their or others' Personal Information in accordance with the policy; or
ii. where an individual believes or suspects that Personal Information has been disclosed in an eligible data breach.

9.1 Definition of an eligible data breach

a) An eligible breach is –

i. when there is an unauthorised access or disclosure of Personal Information and a reasonable person would conclude that the disclosure or access is likely to result in serious harm to those individuals affected; or
ii. when information is lost in circumstances where unauthorised access or disclosure is likely to occur and assuming that unauthorised access or disclosure were to occur, a reasonable person would conclude that the disclosure or access is likely to result in serious harm to the affected individuals; and
iii. would qualify as a statutory eligible data breach under the Privacy Act 1988 (Cth).

b) An eligible data breach may also be as prescribed by other laws such as the General Data Protection Regulation, where it has applicability to the University and the Personal Information it holds.

9.2 Summary of provisions relating to data breaches

a) All suspected data breaches, whether detected by internal controls, or reported by employees or other persons will be investigated in accordance its Information Privacy Incident Response Plan, to determine if a data breach has occurred, if it involved Personal Information and whether it is an 'eligible data breach'.
b) Where notified of a suspected breach the University will investigate to determine whether a breach has occurred, and whether it is an eligible data breach. The University will take all steps to do this in a timely manner and where possible within 30 days of becoming aware of the breach.
c) When assessing whether serious harm is likely to result from the Breach, consideration is given to the information's sensitivity, the types of people who have obtained the information, if the information is protected by security and whether these measures can be circumvented.
d) Only data breaches which can be categorised as an 'eligible data breach' require notification.

e) The University will, where it has reasonable grounds to believe an eligible data breach has occurred, act as follows:

   i. prepare a statement providing details of the breach including the information concerned, steps that can be taken by individuals to protect or mitigate any harm and how to contact the University; and
   ii. provide the statement, directly where possible, to those individuals affected or at risk; and
   iii. provide the statement where appropriate to the Office of the Australian Information Commissioner (Cth) or other required Authority.

f) The University may, where such a breach is not an eligible data breach, take such discretionary actions as it believes are commensurate with the nature of the breach and the likelihood of harm to those impacted.

10 Personal Information Requests

a) Please contact with full details the UWA Privacy Office at privacy@uwa.edu.au

   i. If you wish to make an access request to understand and inspect your Personal Information or wish to correct your Personal Information where you believe the University has not corrected or updated your Personal Information as requested.

   ii. If you are eligible and wish to exercise any of the rights conferred by the General Data Protection Regulation (GDPR).

11 Reporting potential Breaches

b) Please contact with full details the UWA Privacy Office at privacy@uwa.edu.au

   i. If you believe that there has been a breach of this policy by the University, or a member of its staff in the collection, handling or disclosure of your or another person or persons' Personal Information.

   ii. If you believe there has been a data breach, that is unauthorised access to or disclosure of data, involving Personal Information.