Privacy Obligations and Requirements Guideline

Section 1 - Introduction

(1) This is a guide to the obligations and requirements of the Privacy Act 1988 (Cth) (Privacy Act) and the application of the Privacy Policy which sets out the manner in which ACU complies with and implements the requirements of the Privacy Act.

(2) This Guide is based on the Australian Privacy Principles Guidelines (APPs) issued by the Office of the Australian Information Commissioner.

(3) The Guide is intended only to provide an overview of aspects of Privacy Law requirements, the specific requirements of the Privacy Policy, and to indicate where potential risk to the University may arise. It is not advice or an instruction manual. Advice should be sought on specific matters from the Privacy Coordinator or, if legal advice is required, the Office of General Counsel (OGC).

Section 2 - What is Privacy?

(4) The Privacy Act 1988 (Cth) protects personal information.

(5) Personal information is information or an opinion about an identified individual or an individual who is reasonably identifiable that:

a. includes academic records, assessments and contact information;
b. includes photographs;
c. includes opinions; and
d. does not include information about deceased persons.

Section 3 - What Activities Does the Privacy Act Cover?

(6) The Privacy Act covers the following:

a. collecting personal information;
b. giving out personal information;
c. using personal information; and
d. keeping personal information.

Section 4 - Employee Records

(7) Records of acts done or practices engaged in by ACU which are directly related to a current or former employment relationship between ACU and the individual are exempted from the Privacy Act. Such records however will generally be considered to be confidential and must be treated accordingly.

(8) Employment records are exempt only insofar as they relate directly to the employment relationship. Payroll or contact details for example are exempt only in relation to their use in the employment relationship. They cannot be used or disclosed for other purposes unless under the terms of the Privacy Act.

(9) The personal information of individuals who are not or do not become employees is not covered by this exemption. This includes personal information of unsuccessful job applicants (including references) or information about persons in ACU employment records who are not employees (e.g. information about an individual's family).

Section 5 - Collecting Information

What Information can ACU Collect?

(10) ACU can collect personal information only if it is reasonably necessary for, or directly related to, its functions and activities. This includes support functions, including administration, security, public relations and recruitment activities. It will not include information which is more than required, may be useful as opposed to necessary, or for other entities where the purpose is not necessary for, or directly related to an ACU function or activity. Photographs of students in a class, for example, may not be considered reasonably necessary or directly related to teaching if they are taken only for the convenience of the lecturer as opposed to confirming identity to prevent cheating or for security purposes.

What Does ACU Have to Tell the Individual?

(11) When ACU collects information about an individual it must take reasonable steps to tell the individual (where applicable):

a. ACU's name and contact details:
    i. generally this will be the contact details of the Privacy Coordinator (on behalf of the Privacy Officer) and the email address privacy@acu.edu.au;
b. the fact and circumstances of collection:
    i. this applies where ACU collects information from another entity such as another university, a Government authority or the individual may not be aware of the collection of the information (e.g. cookies on the website);
    ii. if it is impractical to refer to a specific entity, it is sufficient to indicate the kinds of entities from whom the information is collected (e.g. other educational institutions or work placements);
    iii. where information is collected by, for example, cookies or electronic tags, the method of collection should be explained;
c. whether it is required or authorised by law:
    i. It is not necessary to identify any law and usually no law requires or authorises the collection of the information. If there is a legal requirement or authorisation however, the applicable law(s) or type of laws should be identified. This can be done generically where applicable (e.g. as required by taxation laws or immigration laws).
d. the purpose of collection:

i. This can include a number of purposes.
ii. It is not necessary to specify purposes which are part of internal normal business practice e.g. billing or managing a student record.
iii. Stating the general purposes of collection will be sufficient. It is not necessary to outline all specific purposes.

e. the consequences if the information is not collected:
    i. applicable in cases where there are significant consequences of not providing information (e.g. the enrolment will not be processed; a placement cannot be allocated; a concession cannot be granted; or not providing the information will result in slower delivery of a service); it is not necessary to state consequences which are obvious;

f. the usual disclosures of personal information of the type collected:
    i. if it is not practicable to list specific entities to whom disclosure may be made it is sufficient to refer to the type of entities (e.g. other universities; Government agencies administering Higher Education funding or Immigration laws);

g. information about:
    i. the right to access and correction of personal information; and
    ii. the right to complain and how complaints are dealt with.

(12) This can be done by reference to the Privacy Policy (e.g. by a link to the Policy on the ACU webpage or a reference to it).

(13) Other entities or types of entities to which that kind of personal information is usually disclosed (e.g. immigration authorities; placement providers; other educational institutions).

(14) Whether ACU is likely to disclose personal information to overseas recipients and if practicable, where those recipients are located. This does not include routing information overseas or use by ACU of the information overseas (e.g. for operation of the Rome Centre).

When Should Notification Occur?

(15) This information should be provided before, or at the time of collection or, if this is not practicable, as soon as practicable after collection of the information. It may be considered impracticable to provide information before collection if, for example, there is an urgent situation or collection of the information is by telephone.

Does the Individual Have to be Notified of Everything, Every Time?

(16) It may not be reasonable to notify the individual of all or some of the required information. In which case, ACU may not have to give the information. ACU must be able to justify this clearly.

(17) Reasons for not notifying of some or all of the required information may include:

a. the information is collected from the individual on a recurring basis for the same purpose;
b. it is impracticable (e.g. details of an emergency contact received from a student or staff member);
c. there is a legal obligation of confidentiality; and
d. the circumstances are such that some or all of the matters required to be notified are obvious and clear from the context of obtaining the information.

How can the Individual be Notified of Collection of Information?

(18) Options for providing notice of the information required to be given on collection of personal information include:

a. in paper form which is provided at the time of, or prior to, collection;
b. a readily accessible and prominent link to a pro-forma notice online;
c. by a telephone script if the information is collected in this way or, if this is not practicable, in any subsequent electronic or paper communication, or directing the individual to a notice on the ACU website;
d. a reference to the Privacy Policy or relevant sections of it (such as overseas disclosures) may be sufficient but this will depend upon the nature and purpose of the collection of the information; and
e. if the information is collected by a third party, the contract with that third party should include a requirement to provide the required notifications.

How Must Collecting be Done?

(19) Collection of personal information must be done:

a. lawfully and fairly. Lawful collection excludes information obtained by, for example, unlawful surveillance, hacking or theft. Fairly means that there should not be intimidation or deception or taking unfair advantage. Individuals should not be misled as to the circumstances purpose and nature of the collection of the information (e.g. representing that there is a requirement to provide the information when there is not. Cultural differences or the particular circumstances of a person may need to be taken into account in considering whether this requirement is complied with.
b. from the individual unless it is unreasonable or impracticable. This requirement covers not only collecting information about an individual from other persons, but also collecting information by e.g. aggregating data from various sources or even doing a Google search.

(20) Relevant considerations in determining whether it is unreasonable or impracticable may be:

a. whether the individual would reasonably expect the information to come directly from them or from someone else;
b. if the information is sensitive (as defined by the Privacy Act) or not. If it is sensitive, then there is a greater burden on ACU to establish that it is unreasonable or impracticable. Sensitive information includes health information and financial information;
c. if direct collection jeopardises the purpose of collection or the integrity of the information;
d. the privacy risk in collecting from another source; and
e. the time and cost in collecting information directly from the individual – the time / cost burden must be excessive in all the circumstances.

What if ACU is Provided with Information from Other Sources Which it has not Requested (Unsolicited Information)?

(21) Unsolicited information includes additional information to unrequested information (e.g. examples of work not requested for a job application).

(22) ACU must, within a reasonable period after receipt of the information, decide whether it can collect the information. If it could not collect the information and it is lawful and reasonable to do so, ACU must destroy or de-identify it as soon as practicable. The information may also be returned to the person who provided it.

(23) It will generally be lawful to destroy the information unless there is e.g. a court order in place or there is an audit requirement.

(24) If ACU keeps the information it must be treated in the same way as other personal information.

Section 6 - Using and Disclosing Personal Information

What can ACU do with Personal Information?

(25) ACU may use or disclose information only for the purpose for which it was collected e.g. enrolment information may only be used for the purposes of enrolment and administration of a student's studies unless:

a. there is consent; or
b. the individual would reasonably expect the use or disclosure and the purpose of the use or disclosure is related to the reason why it was collected; or
c. it is authorised by law or a court or tribunal; or
d. there is a permitted health situation or permitted general situation; or
e. ACU reasonably believes that the use or disclosure is reasonably necessary for an enforcement related activity conducted by or for an enforcement body (e.g. police).

What is Using Personal Information?

(26) Using personal information includes reading it; searching for it in records; making a decision on the basis of it; access to it by an employee or one part of ACU passing it to another.

What is Disclosing Personal Information?

(27) Disclosing means making it accessible outside ACU and releasing control of it. It includes accidental disclosure and unauthorised release by a member of ACU staff if they are acting in the course of their employment. It does not include an external "hack" of ACU systems or theft unless ACU has failed to take reasonable steps to protect the information.

What is Consent?

(28) In relation to consent:

a. it may be express or implied. For example, consent to use personal information for administration of a student's studies, including assessment and arranging placements required for those studies may be implied by enrolment;
b. express consent will be necessary to use this information for e.g. using enrolment information for research or marketing purposes;
c. the individual must have adequate information before giving consent;
d. the consent must be voluntary; and
e. the consent must be current and specific. Simply giving notice of a proposed collection, use or disclosure of the personal information will not normally be sufficient.

(29) The individual must have the capacity to understand and communicate the consent.

Opt Out Provisions

(30) An opt out provision can be used for the purposes of consent but it must be used appropriately and constructed carefully in order to be effective. Usually, express consent and an opt in mechanism is preferred.

(31) Use of an opt out consent is more likely to be effective if:

a. the opt out option is clear and prominent;
b. the individual is likely to receive and read relevant information;
c. there is information on the implications of not opting out;
d. the option is freely available and not bundled with other purposes;
e. it is easy for the individual to opt out – there is little or no financial cost or effort;
f. the consequences of failure to opt out are not serious;
g. opting out at a later time will not give rise to significant disadvantage.

Section 7 - The Police and the Law

Warrant, Subpoena, Notice to Produce

(32) If ACU is served with a valid warrant, a subpoena or a notice to produce information under an Act, then personal information required to be produced must be produced.

(33) The warrant, subpoena or notice and the information to be produced must however be referred to the Office of General Counsel to ensure that it is valid and that the information produced falls within the strict terms of what is required to be produced otherwise ACU may breach the Privacy Act.

(34) In some circumstances an order to provide counselling or health records may be contestable.

Requests from Police and Other Law Enforcement Agencies

(35) ACU may respond to a proper request for information that it reasonably believes is reasonably necessary for the purposes of the law enforcement agency. ACU requires a request in writing from the agency with sufficient information to enable it to decide whether it can release information and what information is reasonably necessary.

(36) ACU does not have to release the information and any request must be referred to the Office of General Counsel.

(37) A written note of the use or disclosure of the information must be kept with details of the disclosure or use, and the basis for the reasonable belief which was the basis of the disclosure. The Office of General Counsel will generally do this on its file.

Suspected Criminal Offences and Unlawful Behaviour

(38) If ACU has reason to suspect unlawful activity that relates to ACU functions or activities and reasonably believes that it needs to collect, use or disclose personal information to deal with this then it can do so. This allows reports to police or other appropriate authorities with information relating to the report or required for investigation of the report – for example in the case of a suspected fraud on ACU, ACU may provide details of relevant payments to a person and bank details. It also allows ACU to collect, use or disclose personal information to investigate suspected unlawful behaviour itself. There must be grounds on which to base the suspicion of unlawful activity by the individual concerned such as a credible complaint or a record of suspect transactions or activity on a credit card.

(39) The unlawful activity must relate to ACU and includes discrimination or harassment. Any information collected, used or disclosed must be only what is reasonably believed is necessary.

Section 8 - Misbehaviour

Suspected Serious Misconduct

(40) If ACU has reason to suspect serious misconduct by a student or employee or associate of ACU that relates to

ACU functions or activities and reasonably believes that it needs to collect, use or disclose personal information to deal with this, then it can do so. This enables ACU to e.g. investigate a suspected serious breach of the Code of Conduct for Staff such as significantly wrongful use of its internet resources.

(41) The suspected conduct must be serious and the use or disclosure of the personal information must only be what is reasonably believed is necessary to deal with it. There must be grounds on which to base the suspicion of misconduct against the individual concerned such as a credible complaint or a record of suspect transactions or activity on an internet account.

Section 9 - Complaints or Allegations

Dealing with Complaints or Allegations made to ACU

(42) If an individual makes a complaint about ACU then that individual may reasonably expect that ACU will use their personal information to deal with that complaint, including investigation of the complaint and informing persons complained of about the complaint.

(43) Only information required for dealing with the complaint should be used or disclosed. Best practice is to obtain the consent of the complainant for the use or disclosure of their personal information or, at least inform them of the intention to disclose information before doing so.

(44) Where a complaint is made under the Protected Disclosures Policy particular processes and obligations apply and no disclosure should be made without complying with the Policy.

Dealing with Complaints or Allegations about ACU

(45) If an individual makes a complaint or attack on ACU in the media then that individual may reasonably expect that ACU may respond publicly to those comments revealing personal information of the individual but only if that information is specifically relevant to the particular issues raised. For example, if a student complains to the media that international students are treated more favourably than domestic students, it would not be acceptable to make a public statement including information about that particular student's academic record. If a student complains to the media that they have been discriminated against in the way in which they were assessed, it may be acceptable to make a statement which includes information about that student's academic record where it is relevant.

Section 10 - Emergency and Threat Situations

Threat Situations

(46) If ACU reasonably believes that collecting, using or disclosing personal information is necessary to lessen or prevent a serious threat to the life, health or safety of any person or to public health or safety and it is unreasonable or impracticable to obtain the individual's consent then ACU may collect, use and disclose personal information.

(47) Relevant considerations include:

a. the nature of and potential consequences of the threat – how urgent and serious it is and how likely it is;
b. the adverse effects on individual of not obtaining consent. This will usually be a question of the possible adverse effects of disclosure of personal information;
c. whether the individual is capable of or able to give consent – the individual may not be in a proper physical or psychological state or may be non contactable within the relevant time-frame;
d. the number of persons who have to give consent – this may make it impracticable to obtain consent;

e. inconvenience, time and cost of obtaining consent; and
f. the threat must be a present threat (i.e. not a threat that has passed).

Section 11 - Collection, Use and Disclosure of Personal Information for Purposes of ACU

Normal business requirements

(48) If use of personal information is part of normal business processes then the individual will be considered to have given implied consent to its use e.g. by enrolling the student gives implied consent to use of personal information for enrolment and administration of the student's study and student experience, including the opportunity to participate as an alumnus after graduation, but not for the purposes of fund-raising.

Photographs

(49) If a photograph can identify a particular person it is personal information.

(50) Taking photographs where persons can be identified can be done without consent but the general requirements around collecting personal information apply and the taking of the photograph must be reasonably necessary for ACU's functions or activities. If, for example, photographs are expected to be taken at an event of an audience so that persons in that audience may be identifiable, if practicable, invitations or material distributed at the event should state that photographs of the event will be taken and provide the usual information such as the purpose of taking the photographs and how they will be used.

(51) If a person's racial, ethnic origin or religious belief may be identified by the photograph, then this is considered to be sensitive information.

Consent

(52) If there is explicit consent, then personal information may be used within the terms of that consent. Consent must be freely given, the individual must be adequately informed and if possible, there should be provision to opt in or out.

Section 12 - Health Information

(53) Health Information includes:

a. opinion about an individual's health or disability;
b. an individual's wishes about provision of health services to them; and
c. information collected to provide or in providing a health service.

(54) A health service includes any activity that is intended or claimed by the individual or person providing it to assess, record, maintain or improve the individual's health; diagnosis; treatment or prescription. It includes a fitness centre or gym.

Section 13 - Research

Collecting Health Information for Research

(55) ACU may collect personal health information about an individual if the research (including the compilation or

analysis of statistics):

a. is relevant to public health and safety; or
b. the management, funding or monitoring of a health service (e.g. quality assurance processes); and
c. the purpose of the research cannot be served by de-identified information; and
d. it is impracticable to obtain the individual's consent (this includes adversely affecting the integrity or validity of the research as well as practical problems such as lack of current contact details for individuals); and
e. it is either:
    i. required by or under an Australian law;
    ii. in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation; or
    iii. it is accordance with NHRMC Guidelines approved under the Privacy Act.

(56) Reasonable steps must be taken to ensure that the information is de-identified before it is disclosed or published.

Using and Disclosing Health Information for Research

(57) Researchers may use and disclose personal health information for research if:

a. it is necessary for the research; and
b. it is impracticable to obtain the individual's consent to the use or disclosure; and
c. it is done in accordance with the NHMRC Guidelines approved under the Privacy Act; and
d. ACU (the researcher) reasonably believes that the recipient of the information will not disclose the information.

(58) Disclosure of health information should be in de-identified form if reasonably possible.

(59) Normally, if personal health information is being provided to a person or entity outside of ACU because it is necessary for the research, a confidentiality deed will be required before this can occur. If the person or entity is an investigator on the grant, then a deed of confidentiality will not usually be required.

(60) Without specific consent of the individual and approval of the Human Research Ethics Committee (HREC), no personal health information may be published.

HREC and Obligations of Researchers

(61) All research involving collection of personal health information will normally require the approval of the HREC and, in that case, the HREC will consider and apply the privacy obligations so that the HREC application and approval processes will cover the Privacy Act requirements to enable collection of the information.

(62) Researchers will be responsible for ensuring that the information is collected, used, stored and disclosed in accordance with the HREC approval and the Privacy Act.

Section 14 - Providing a Health Service

Collecting, Using and Disclosing Personal Health Information in the Course of Providing a Health Service

(63) Where ACU is providing a health service it may collect, use and disclose personal health information if:

(64) Providing the health service:

a. the information is necessary to provide a health service to the individual and:
    i. either the collection is required or authorised by an Australian law; or
    ii. it is collected in accordance with rules established by a competent health or medical body that deals with obligations of professional confidentiality which bind ACU (i.e. there is a sanction or adverse consequence if the rules are breached). This would apply to the Counselling Service or a medical clinic operated by ACU.

(65) Management and administration of the health service:

a. For the purposes of management and administration of the health service; and
    i. the purpose cannot be served by de-identified information;
    ii. it is impracticable to obtain the individual's consent; or
    iii. it is collected in accordance with rules established by a competent health or medical body that deals with obligations of professional confidentiality which bind ACU i.e. there is a sanction or adverse consequence if the rules are breached. This would apply to the Counselling Service or a medical clinic operated by ACU.

(66) Any disclosure of health information should be de-identified.

Disclosure Without Consent

(67) Disclosure without consent is permissible if ACU is providing a health service and is satisfied that either:

a. disclosure is necessary to provide appropriate care or treatment of the individual; or
b. the disclosure is for compassionate reasons; and
c. the individual is physically or legally incapable of giving consent; or
d. physically cannot communicate consent; and
e. the recipient of the disclosure is a responsible person for the individual; and
f. the disclosure is not contrary to any prior wish expressed by the individual of which ACU could reasonably be expected to be aware; and
g. the disclosure is limited to the extent reasonable and necessary for the purpose.

Genetic Information

(68) There is provision in the Privacy Act for disclosure of genetic information obtained in the course of providing a health service where there is a risk to a genetic relative of the individual.

Sensitive Information about Race, Ethnicity, Religion, Political Opinions, Sexual Orientation or Practices, Criminal Record and Health

(69) Information about a person's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, professional or trade association / trade union membership, sexual orientation or practices or criminal record, health information, genetic or biometric information is considered sensitive information and there are additional restrictions which apply to how this information is collected, used and disclosed.

Other Times when Collection, Use and Disclosure of Personal Information is Permitted

(70) The Privacy Act allows the collection, use and disclosure of personal information in various circumstances and under specific situations including:

a. locating missing persons;

b. defending legal claims; and
c. participating in alternative dispute process.

(71) Matters relating to these matters should be referred to the Privacy Coordinator.

Section 15 - Direct Marketing

What is Direct Marketing?

(72) Direct marketing is the use or disclosure of personal information to communicate directly with an individual to promote goods and services. It would not include invitations to public lectures, but would include invitations to post-graduate courses.

When can Personal Information be used for Direct Marketing?

(73) ACU can use personal information for direct marketing when:

a. the individual has the opportunity to opt out; and
b. the information has been collected directly from the individual and the individual would reasonably expect it to be used for direct marketing or the individual has consented to the use of personal information. This can be done by notifying the individual of ACU's intention to use the personal information in this way. The consent must remain current and be specific, or the individual has the opportunity to opt out; and
c. information has been collected directly from the individual but the individual would not reasonably expect it to be used for direct marketing or it is obtained from a third party; and
d. the individual has consented or it is impracticable to obtain that consent.

Opting Out

(74) The opt out must be:

a. clear and visible;
b. not complicated and easy to use.

Requests to Identify Source of Personal Information

(75) An individual may ask ACU to identify the source of the personal information it uses for direct marketing. This must be given within a reasonable period – generally 30 days unless it is impracticable or unreasonable to provide the information.

Spam Act and Do Not Call Register Act

(76) The Spam Act 2003 (Cth), Do Not Call Register Act 2006 (Cth), and the Privacy Act, all apply to direct marketing.

Section 16 - Disclosing Personal Information Overseas

What is Disclosing Personal Information Overseas?

(77) Disclosing personal information overseas includes:

a. information delivered or exchanged at a conference overseas;
b. publication on the internet –intentionally or otherwise – which is accessible to a person located overseas; and
c. sharing personal information with a person overseas by any means.

Can ACU Disclose Personal Information Overseas for Operational Purposes?

(78) Advice should be sought from the OGC before personal information is disclosed to an overseas recipient.

(79) In general terms, there are provisions allowing disclosure to overseas recipients in circumstances which should be assessed carefully. ACU can:

a. send personal information overseas if it is to a unit or staff member of ACU located overseas e.g. to the Rome Centre. The general rules regarding privacy apply to the use, disclosure and handling of personal information as in Australia;
b. send personal information to an overseas recipient if the individual is expressly informed of this and consents to it. The information provided to the recipient prior to any consent should include a statement that ACU will not be accountable under the Privacy Act and will not be able to seek redress under the Privacy Act. If the information is particularly sensitive, then more information may be required to be given in order to establish that the consent was sufficient;
c. use servers located overseas for the purposes of routing information to a recipient. This is not considered a disclosure;
d. use overseas located services (cloud service provider) for purposes of storing and accessing data provided that the contract with the cloud service provider:
    i. provides that ACU owns the data;
    ii. ensures that the provider and any contractors handle the information only for the purposes of ACU storing and accessing the data;
    iii. gives ACU on-going control of how the data is managed and accessed (including retrieval or disposal); and
    iv. has appropriate provisions for security of the data.
e. engage an overseas based contractor to perform services for it such as marketing or data analysis on the basis that ACU still holds the information and there are measures in place to ensure that the data receives the protections and management required by the Privacy Act. ACU will be liable for any mishandling of the information by its contractor. As a result:
    i. The contract for the services must include specific privacy provisions.
    ii. There may be a requirement for auditing compliance with privacy requirements.

(80) If the overseas recipient is subject to a privacy law or some form of regulation which is equivalent to the Australian law and which has mechanisms which enable a complainant to use that law, then the burden on ACU is much less.

(81) Arrangements which involve personal information being sent overseas to be used by a third party must be reviewed by OGC.

Can ACU disclose personal information overseas in emergencies, cases of wrong doing or for law enforcement purposes?

(82) ACU may disclose personal information where:

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

individual's consent;

b. it has reason to suspect that unlawful activity or misconduct of a serious nature that relates to ACU functions or activities has been, is being or may be engaged in, and ACU reasonably believes that the disclosure is necessary for it to take appropriate action in relation to the matter;
c. it reasonably believes that the disclosure is reasonably necessary to assist an entity subject to the Privacy Act to locate a person reported as missing and it the disclosure complies with rules made by the Information Commissioner.

(83) These provisions are similar to those which apply to disclosure of personal information within Australia and more information on how they are applied is set out above. Where practicable the advice of OGC should be sought before disclosing personal information to an overseas recipient.

How responsible is ACU for what an overseas recipient does with personal information received from ACU?

(84) ACU may be liable for the actions or practices of an overseas entity in relation to personal information disclosed by it to that entity. This may be the case even where the entity has taken reasonable steps to comply with Australian requirements, the fault lies with the overseas entity's sub-contractor or the breach of the Australian requirements is inadvertent.

(85) It is important to ensure that the circumstances around the disclosure minimise the risk that ACU will be exposed to penalties for the failures of an overseas entity to whom it has disclosed personal information. OGC should be consulted on all potential arrangements involving disclosure of personal information to overseas recipients to prevent or minimise this risk.

What if foreign law requires disclosure by an overseas recipient of personal information provided by ACU?

(86) If ACU discloses personal information to an overseas recipient and that recipient is required by a law of that jurisdiction to disclose the personal information then this will not be a breach of the Privacy Law. A contract with the overseas recipient should deal with this possibility and provide for notification to ACU in the event of disclosure under compulsion of law and consideration should be given as to whether individuals should be notified that disclosure of this type may be required. The USA Patriot Act, for example, gives the US Government extensive powers to obtain personal information.

Section 17 - Keeping and Maintaining Personal Information

Data Quality

(87) ACU must take reasonable steps to ensure that the personal information it holds and discloses is accurate, up-to-date and complete. This is an on-gong and positive obligation.

(88) Practices which assist in demonstrating that ACU has met its obligations with respect to data quality include:

a. auditing, monitoring and correction of data quality;
b. use of a consistent format for collecting and recording information;
c. ensuring that updated or new information is promptly added;
d. providing means for individuals to review and update their information;
e. getting rid of personal information which is no longer needed and which is old information;

f. where personal information is received from a third party, checking to ensure that there are appropriate quality processes and procedures in place; and
g. not using data without first considering its quality.

Data security obligations

(89) ACU must take reasonable steps to protect personal information from misuse, interference and loss, unauthorised access, modification or disclosure.

(90) Where the information is no longer needed it must be destroyed or de-identified.

How can ACU meet its obligations for data security?

(91) Practices and procedures which can help to show that ACU is meeting its obligations to keep data secure are:

a. local policies, procedures and awareness about data security;
b. training and instruction;
c. access restrictions – both physical and system access restrictions;
d. contracts with third parties which address issues of data security;
e. regular audits and reviews;
f. incorporating destruction and de-identification into management of data; and
g. written and promulgated standards for maintaining security of data.

(92) While data security may be managed principally by IT systems, breaches of data security can occur by inadequate local policies, procedures and practices such as:

a. staff copying or downloading data and losing it in a public place;
b. failure to keep back-ups of information;
c. circumvention of or failure to comply with IT security processes; and
d. failure to destroy or de-identify information appropriately.

Section 18 - What Rights Has the Individual Whose Personal Information ACU Holds?

Access to information

(93) ACU must give an individual access to their personal information unless specific exceptions apply (see below).

(94) There are time periods for responding to requests and other procedural requirements which are set out in the Privacy Inquiry and Complaints Procedure. The information required to be provided includes not only information but also may include opinions.

(95) The request for access must be made by the individual concerned or a person properly authorised by that individual and ACU must satisfy itself that the request is from the appropriate person.

Can ACU refuse to give an individual access to their personal information?

(96) ACU can refuse access by an individual to their personal information if:

a. ACU reasonably believes that giving access would pose a serious threat to the life, health or safety of any

individual or to public health or safety;

b. giving access would have an unreasonable impact on the privacy of other individuals;
c. the request is frivolous or vexatious;
d. the information relates to existing or anticipated legal proceedings between ACU and the individual and the information would not be accessible by legal discovery processes in the proceedings (e.g. information covered by legal professional privilege);
e. the information would reveal ACU's intentions in relation to negotiations with the individual so as to prejudice those negotiations;
f. giving access would be unlawful;
g. ACU has reason to suspect that there is, has been or may be unlawful activity or misconduct of serious nature relating to its functions or activities and giving access to the material is likely to prejudice taking appropriate action in relation to that activity or misconduct;
h. giving access would be likely to prejudice an enforcement related activity conducted by or on behalf of an enforcement body; or
i. giving access would reveal evaluative information generated within ACU in connection with a commercially sensitive decision-making process.

(97) Consideration must be given to whether material can be produced in an alternative form if applying one of these exceptions. It may be possible for example, to redact the information of other persons, or provide a summary of the information, or deleting the information or facilitating access by providing the material for inspection but not providing it in hard copy or electronic form or using an intermediary to provide the information (e.g. providing it through a suitably qualified medical professional where the material may be sufficiently distressing to the individual to lead to a concern about self-harm by that individual).

(98) ACU must provide the individual with reasons for a refusal to respond to a request for access to information and the individual must be provided with certain information such as the way in which the individual can complain about the refusal.

Can ACU charge for responding to a request for personal information?

(99) ACU can charge for costs in finding and producing requested information, including costs of deciding which information to provide and copying costs and the like. The costs must not be excessive and do not include costs of legal advice or of consulting with the individual about how access is provided. If it is proposed to make a charge (which would be only in exceptional circumstances), a record must be kept of all expenditure and time and the costs charged must be on a reasonable basis. Costs must be communicated and explained before access is given.

Other means of accessing information

(100) Unlike many other Universities, ACU is not bound by Freedom of Information legislation. This applies only to government entities.

(101) Information however may be subject to production in Court proceedings.

Right to correction of information

(102) ACU must take reasonable steps to correct personal information if requested by the individual.

(103) ACU must respond to a request for correction of personal information within 30 calendar days and deal with it within a reasonable period (generally 30 days).

(104) If ACU receives a request for correction of information it must assure itself that the information is incorrect.

(105) The Privacy Inquiry and Complaints Procedure sets out how requests for correction of information are made and dealt with however requests for correction of information can be made informally and it is not necessary to state the request is made under the Privacy Act.

(106) ACU must, if requested take reasonable steps to notify any third party which comes under the Privacy Act or the correction to the personal information if requested and it is not impracticable or unlawful to do so. If a third party has been informed of incorrect information and it is not impracticable or unlawful, ACU should take steps to correct the information held by the third party whether or not there is a request and / or prompt a request.

(107) If ACU refuses a request to correct personal information it must give the individual reasons for that refusal (unless this is unreasonable or unlawful) and advise the individual of matters such as available complaint mechanisms.

(108) If a request for correction of personal information is refused, the individual may request ACU to have an associated statement of the individual's belief that the information is inaccurate, out-of-date, incomplete, irrelevant or misleading. If it is reasonable and practicable ACU must comply with the request. This can be done by attaching the statement to a physical record or by an electronic link to a digital record or, if this is not practicable, a note on the record which references where the statement can be found. ACU is not obliged to accept overly long, irrelevant, defamatory, offensive, abusive or unlawful statements (e.g. a statement which breaches another individual's privacy) but if such objections are made, then ACU should attempt to negotiate with the individual on the form and substance of the statement.

(109) ACU cannot charge for a request for correcting personal information, correcting information or for associating a statement with the personal information.

Section 19 - Review

(110) Unless otherwise indicated, this Guideline will still apply beyond the review date.

Status and Details

Status	Current
Effective Date	17th March 2024
Review Date	29th April 2024
Approval Authority	Director, Governance
Approval Date	17th March 2024
Expiry Date	Not Applicable
Responsible Executive	Diane Barker Director, Legal, Assurance and Governance
Responsible Manager	Matthew Charet National Manager, Governance
Enquiries Contact	Legal, Assurance and Governance Directorate