**PRIVACY AND CONFIDENTIALITY IN RESEARCH SUPERVISION**

**by Simon Moss**

|  |
| --- |
| **Introduction** |

At first glance, the topic of privacy and confidentiality in supervision might not seem especially appealing or important. Nevertheless, even at CDU, research supervisors often breach the Privacy Act or violate the CDU Privacy and Confidentiality Policy. These breaches can

* significantly upset other people, including candidates
* culminate in accusations of misconduct or serious misconduct, culminating in disciplinary action, dismissal, or other legal consequences

Indeed, the federal Privacy Commissioner can seek fines of up to $1.8 million against an organisation in response to serious or repeated breaches.

**Examples**

You might assume that you never breach privacy laws and policies. Nevertheless, the following table illustrates some practices—practices that are common at CDU—that may violate privacy laws and policies. In particular

* the first column specifies a common practice.
* the second column specifies a possible risk or consequence of this practice
* the third column specifies measures that researchers should implement to prevent these risks

|  |  |  |
| --- | --- | --- |
| Practice | Risk or consequence | Measures to prevent risk |
| **Computer screens.** During a meeting, the research candidate can view the computer screen of the supervisor | The research candidate might read personal information about another person. For example   * the candidate might see an email from a colleague with the title “my anxiety” | * Conceal the computer screen from other people during a meeting * If you need to use the computer with someone else, close or conceal programs that might display personal information, such as Outlook |
| **Documents on a desk.** During a meeting, a colleague can see a document on the desk of a lecturer | The colleague might read personal information about another person, such as a candidate. | * Tidy your desk to avoid inadvertent disclosure of personal information |
| **Forwarded emails**. A research supervisor forwards an email from another colleague to a research candidate | The email might include personal information about the colleague, violating the Privacy Act. Even the opinions of this colleague are deemed as personal information | * When you forward emails, or add someone to an email exchange, check the previous emails in this thread do not contain personal information including opinions * In general, do not forward emails but write a new message—unless you are merely forwarding factual information or have received consent to forward this email |
| **Publicly seeking support for an anonymous research candidate**. In a public forum, such as a college meeting, a research supervisor might request assistance for some anonymous research candidate. For example, the supervisor might ask “Can we organize support for candidates with dyslexia”. | People who attended the meeting might be able to decipher the identity of this research candidate. These individuals, for example, might later discover the academic supervises only one person. Hence, the supervisor has, inadvertently, informed these people the candidate has been diagnosed with dyslexia. | * Before you attempt to help a candidate, seek consent * Discuss issues that relate to the candidate only to relevant individuals—individuals who are assigned the role to assist |
| **Using CALLISTA**. A research supervisor uses CALLISTA—or another database containing candidate information—to access the address of a research candidate. The supervisor then sends this candidate an invitation—an invitation to an event in which the supervisor is launching a business idea | The supervisor has used personal information about the research candidate, but not for the purpose in which this information was collected—a violation of the Privacy Act | * Do not use personal information about candidates, except for the the purpose in which this information was collected, unless you obtain consent to use the information for another purpose |

This document clarifies some of the laws and policies around privacy that could affect interactions with research candidates. This document, however, does not revolve around the privacy of participants, because this matter is discussed in other materials that revolve around research ethics.

|  |
| --- |
| **Privacy Laws in Australia** |

**Definition of personal information**

The main Commonwealth legislation that governs privacy and confidentiality is the Privacy Act (1988)—an act that was amended considerably in 2001 and 2014. In addition, most of the states and territories have also developed their own information privacy acts. For example, the Northern Territory introduced the Information Act in 2003. To appreciate this legislation, you need to appreciate the definition of personal information as well as sensitive information and health information. The following table defines and illustrates these terms.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Personal information | Sensitive information | Health information |
| Definition | Any information or opinions of a person who has been identified or could reasonably be identified | A subset of personal information that could be consequential and needs to be managed more carefully | A subset of sensitive information that includes information relevant to health |
| Includes | * Name * Contact details * Demographic details, such as age or race * Numbers, such as tax file number * Photographs; CCTV * Academic record * Opinions | * Ethnicity or race * Political beliefs or associations * Religious beliefs or associations * Criminal record * Sexual practices * Membership of a profession, trade, or union * Health information | * Physical or mental health status—such as reports, tests, and prescriptions * Bodily donations, such as blood * Genetic information * Health services used |
| Excludes | * Anonymous information * Aggregated information * Information that is not intended to be recorded, such as an informal conversation |  |  |

Most organizations that collect personal information need to comply with privacy acts. Some exceptions have been identified. For example

* sporting organizations that collect the names and addresses of members, but earns a revenue of less than $120 000, are exempted
* journalists that adopt other media privacy standards are exempted.

**The Australian Privacy Principles**.

The Privacy Act entails 13 legally binding principles that organizations must adopt, called the Australian Privacy Principles. The webpage <https://www.oaic.gov.au/privacy/australian-privacy-principles/> enumerates these principles. The following recommendations summarize these principles:

* organizations should typically, inform individuals they are collecting personal, sensitive, or health information about them
* when collecting this information, organizations should typically clarify the purpose for which they are collecting this information and, for example, to whom they might share this information
* organizations should typically seek consent whenever they collect, use, or disclose sensitive information
* organizations should typically grant individuals the right to access the personal information you have collected about them and to correct or modify this information if applicable

The following table presents some more information about the underlying principles. The first column summarizes some principles. The second column presents some more details or illustrations. The numbers specify which of the 13 principles correspond to this guideline.

|  |  |
| --- | --- |
| Summary | Details or illustrations |
| **Collection of personal information.** The personal information that organizations collect should be   * necessary for the functions or activities of this organization [3] * collected lawfully and fairly [3] * collected directly from the person whenever possible [3] * stored anonymously or with a pseudonym unless impractical or unlawful [2] * collected only after individuals are informed how this information will be used [5] | * You cannot use a ruse or trick to encourage people to tell you information they did not intend to disclose * You cannot collect any sensitive information, unless the person has consented and the information is necessary to your functions—although some exceptions have been identified. * You may be able to collect health information from third parties, but only in specific circumstances; for example, during an emergency, health information could be collected from relatives. Likewise, medical specialists can seek relevant information from a referring provider. * Even in these circumstances, you need to inform the individual, as soon as possible, this information was collected |
| **Notification [5]**. After collecting information about someone, you need to communicate to this person   * the identity and contact details of your organization * the purpose for which you want to collect, use, or disclose this information—and the consequences if this information is not collected * the nations to which you might disclose this information * how this individual can access and collect the information * how this individual can complain if their privacy is breached | * To communicate this information, you can refer this person to the privacy policy of your website or send this person a short privacy notice—sometimes called a collection notice |
| **Consent [3].** You should seek consent to collect personal information—and indeed consent is essential to collect sensitive and health information, except in specific circumstances. This consent should conform to the following principles   * the individual needs to be adequately informed before they consent—and sufficiently able to understand and communicate this consent * the individual cannot feel pressure to consent | * Consent can be written or oral * Ideally, the consent should be recorded in some way, such as a written form or voice recording * Although consent can be implied, failure to opt-out does not necessarily imply consent |
| **Unsolicited information [4].** If you receive unsolicited information—personal information you received without actively seeking this information—you need to consider whether you have lawfully collected this information.   * You can retain this information only if the information is relevant to the functions or activities of the organization and was collected lawfully. * You must notify the person that you have retained this information | * If someone sends you an unsolicited CV, you can retain this CV. But, you must notify the person you will retain this information, and manage the information according to the Privacy Laws. |
| **Storing personal information [11]**. To store personal information appropriately—and to prevent misuse, interference, or loss—you should consider several possible measures:   * conceal computer screens from people who should not be able to see relevant information * do not leave personal information about people on a desk that other individuals might see; store information in locked drawers or inaccessible cloud folders * limit the use of portable storage devices, such as USBs or laptops * encrypt documents that contain personal information before emailing * in group emails, consider BCC instead of CC to obscure email addresses when relevant * in agreements with volunteers or other third parties, include clauses around privacy and confidentiality * arrange individuals to return personal information they can access if they leave the organization | * If you outsource data services to a third party—such as a cloud server in another country—you need to ensure this third party does not breach the Australian Privacy Principles. * Indeed, you could organize this provider to sign a contract that they will not breach the Australian Privacy Principles. * You need to include measures to update the information when necessary to guarantee the accuracy of this information [10] * You must delete or discard personal information that is no longer needed—unless this information needs to be retained for legal reasons or is contained in a Commonwealth record * If you retain electronic health information, you must also comply with the Personally Controlled Electronic Health Records Act 2012. |
| **Using or disclosing personal information**. You cannot use or disclose personal information beyond the primary purpose you collected this information [6] unless   * the individual consented to the use of this information for other purposes * the information is used for a goal that is closely related to the primary purpose and the individual would most likely have consented, or * some legal obligation demands otherwise | * You cannot use sensitive information to guide direct marketing—such as communicating information about your products or services—unless the individual consented to this marketing * You can use personal information that is not sensitive to guide direct marketing, but only if you collected the information from the person, the person would reasonably expect you to use this information for direct marketing, and the person can opt-out but had not opted-out   Individuals should be able to access their personal information you collected [12] within a reasonable time. You can refuse this request only if   * access could threaten the safety of this person, or * access would be unlawful, and * you have informed the person how they can complain if they disagree with this decision   You must correct inaccuracies [13]—including notifying third parties if applicable. |

|  |
| --- |
| **CDU Privacy and Confidentiality Policy** |

If you understand these Australian Privacy Principles, you are likely to comply with the CDU Privacy and Confidentiality Policy. Nevertheless, this policy includes some additional details of which you should be mindful

* Questions or complaints about privacy should be directed to the University Privacy Officer by emailing [privacy@cdu.edu.au](mailto:privacy@cdu.edu.au)

**Obligations of staff**

Staff need to fulfil several obligations around privacy. In particular, staff need to be aware that

* even after their employment ends, they can never use, divulge, copy, or communicate confidential information without appropriate consent—except when this behavior is integral to the duties of these staff members
* if staff become aware that personal information has been accessed without authorization, they must contact the University Privacy Officer by emailing [privacy@cdu.edu.au](mailto:privacy@cdu.edu.au)
* material that staff write or record is subject to Freedom of Information, subpoena, or other authorized access.

**Use and disclosure of personal information**

Consistent with the Privacy Act, the university can only use or disclose personal information in particular circumstances—such as if the individual consents of if this use and disclosure is consistent with the purpose this information was collected and the individual would expect the university to use or disclose this information. However, in addition, the university can use or disclose personal information

* when this use or disclosure is vital for research or compilation of statistics in the public interest—and the individuals will not be identified in publications
* when this use or disclosure could diminish threats to the wellbeing of someone
* if needed or authorized for legal or security reasons. See the policy for more details

**Access to personal information and correction of this information**

Individuals can access the personal information the university compiles and retains about them. This access is sometimes limited when

* this access could threaten the health of someone
* this access could interfere with the privacy of another person
* the request is vexatious or frivolous
* the information relates to legal proceedings between the university and this individual
* access could prejudice legal activities, law enforcement, security, defense, or measures that protect the public

In these circumstances, the university must justify to the individuals this decision to limit access. If individuals believe their personal information is inaccurate, the university will attempt to correct the inaccuracy—and, in general, must notify other third parties that had been misinformed as well. Sometimes, however, the university may disagree the information was inaccurate. In these instances, the university will attach a caveat to this information, indicating the individuals believe this information is inaccurate.

**Sensitive information**

Consistent with the Privacy Act, the university will not collect sensitive information unless the individuals consent or the University is legally authorized or obliged to collect these data. However, the university might also collect sensitive information when

* the information is needed to diminish a serious, imminent threat to someone or is necessary to defend a legal claim—and the person is physically unable to provide or communicate consent
* the information is relevant to targeted welfare or educational services—and again the organization cannot readily arrange consent