University of South Australia

# Changes to the Privacy Act 1988:

## WHAT DO I NEED TO KNOW?

At the University, we collect, use, share and maintain personal information for a variety of reasons.

The Privacy Act 1988 (**Act**) defines *personal information* as:

*information or an opinion, whether or not it is true, about an individual that has been identified or who is reasonably identifiable.*

Much of this data is held in central repositories and includes student information, staff information, alumni information and other university contacts.

Please ensure that you read and are familiar with the University's Privacy Policy when collecting, handling or using *personal information*.

We are also aware that individuals or groups within the University hold their own databases which contain *personal information*.

If you create, manage or have access to *personal information* on a database that is not a centrally managed repository please note the following additional obligations:

## General

» Follow the University's Privacy Policy at all times. All employees must read, review and comply with the Privacy Policy as a principal policy of their employment with the University.

» You must keep *personal information* secure (ie restrict access). Be sure to lock your screen when you are away from your desk. If you have hard copies of personal information, lock them in a cabinet when you are not using them and always collect printing promptly from the copier.

» The degree of security that you need to provide will increase with highly sensitive information (eg. information relating to an individual's health, race, sexual orientation, religion, political/ other memberships etc. **(Sensitive Information)**). That type of information should not be exchanged between staff members by e-mail or text message, as those are unsecured forms of communication. Whenever possible, you must collect *personal information* directly from the individual to whom the information relates.

» When information is collected from an individual, a privacy statement should be provided, referring them to the University's Privacy Policy. If information is collected online, the statement must be available before the information is collected.

» You must ensure that *personal information* is up to date and correct. Any updated information provided by an individual must be immediately updated.

» If the information is not relevant or is no longer required, it must be deleted and/or destroyed. Unfortunately it is hard to say what is irrelevant or no longer required and this is a judgment call. If the same information is stored centrally, you don't need it

» Where there is an obligation at law to keep *personal information*, but the personal information is no longer relevant to you (or is not up to date), then contact Records Management for archiving (as necessary).

» The Act requires *personal information* to be up-to-date and correct, accordingly it is good practice for records to be updated or checked at least annually (and individuals contacted to confirm their details).

» If you use *personal information* to create reports, it should be de-identified where possible.

» If you collect *personal information*, you must have the consent of the relevant individual as to its use. For example, if you receive a business card and you intend placing that individual's *personal information* in a University database, then they must have given you that express consent. One way of doing this manually is to send the individual an email seeking their consent to be added to the mailing list of A, B and/or C publications. The individual must then reply to that email giving their consent. If no response is received, their *personal information* must be deleted and destroyed.

» An individual is entitled to know what information is held about them. Any such requests must be directed immediately to the Privacy Officer at privacy.officer@unisa.edu.au.

» Under no circumstances should a member of staff disclose an individual's *personal information* to a third party. Any such request must be sent to the Privacy Officer at privacy.officer@unisa.edu.au (even if the request is received from the police or the subject of a court order).

» Notice must be given wherever, and at the time that, *personal information* is being collected, ie:

- Where CCTV is being used for security purposes around campus.
- Where lectures are being recorded.

## Marketing

» If you are using *personal information* for direct marketing, have you received express consent from the individual to use their information for those purposes? If not, you cannot use the information for such purposes (unless you obtain that consent).

» Any marketing material that you send out (eg ezines, updates) **MUST** include an unsubscribe option (even if it is sent in hard copy or by text message). It is a requirement of the law that a person must be able to unsubscribe.

- If the correspondence is by email, the email should include a link to an email/webpage to unsubscribe or instructions on how to do so.
- If the correspondence is by post, please include instructions on how to unsubscribe in a prominent or natural place.

» As set out above, *personal information* must be up to date and correct. Accordingly any 'unsubscribe' instructions should also include the opportunity to update details, but if not, recipients should receive notice at least annually to check their details or to provide updated details.

» If engaging a third party provider to issue marketing material, the University's contract with such party must include privacy obligations at least as strict as those set out in the University's Privacy Policy.

» *Personal information* should not be shared or stored on any social media. If *personal information* is received in this manner, the comment/post must be deleted by the page administrator.

## HR

» The Act provides some exceptions in relation to employee records, but it must be noted that such exemptions only apply to employees **not** contractors or unsuccessful job applicants.

» If you intend to collect any Sensitive Information from job applicants during the application process, obtain their consent to do so (particularly as many will be unsuccessful job applicants).

» *Personal information* about contractors and job applicants must be destroyed or deleted once it is no longer relevant.

» If it is reasonably necessary to retain *personal information* to defend any claim made by an unsuccessful job applicant, that information must be stored in accordance with the Privacy Policy and any relevant HR policy.

» If you intend keeping an applicant's CV or application documentation on file, please notify them that you are doing this.

» Any applicant CVs should be reviewed frequently and anything that is out of date must be reviewed and updated OR destroyed.

## Contractors and other third parties

» Staff who engage service providers or other contractors must ensure that the provider/contractor complies with the Act, or at least complies with the University's Privacy Policy. The Contractor Services Agreement has been recently updated to ensure compliance with the Act.

» If the provider/contractor uses any off-shore providers, the University must be made aware of this.

## Got more questions?

» Email Chancellery Legal at legal.services@unisa.edu.au.

» Email the University's Privacy Officer at privacy.officer@unisa.edu.au.

Updated 11 August 2015