## Key Privacy Principles for Staff

<table>
<thead>
<tr>
<th>Principle</th>
<th>Your Responsibility</th>
<th>Things to remember</th>
</tr>
</thead>
</table>
| **Collect** | • Collect personal information for a lawful purpose that is directly related to the University's functions and activities.  
• Collect personal information from the person concerned unless authorised by that person or permitted by law.  
• Ensure a collection notice is provided telling the person:  
  o why their information is being collected,  
  o what it will be used for and to whom it will be disclosed  
  o how they can access and amend their personal information and  
  o any possible consequences if they decide not to give their personal information.  
• Ensure that the personal information is relevant, accurate and not excessive. The collection should not unreasonably intrude into the personal affairs of the person. |
|           | Check that your collection fits into one of the University's functions. See *Personal Information collected by the University* for more information.  
Consider why you need each piece of person information that you are collecting. Is your collection reasonable? Don't just collect information because you might need it at some point in the future.  
Where, possible link to an existing collection statement that the University has prepared. If you think you need a separate statement, use this template and contact the University's Privacy Officers for more assistance. |
| **Store** | • Store personal information securely. Do not keep it any longer than necessary and destroy it appropriately.  
• Protect personal information from unauthorised access, use or disclosure. |
|           | Make a reasonable effort to secure personal information that you hold. Options to consider include:  
  o User access controls and monitoring of access  
  o Audit trails and logs;  
  o Encryption (at rest; in transit)  
• If you engage an external service provider who will use personal information, must make sure that the contract clearly states:  
  o what information they will use and;  
  o how the information is to be returned, or destroyed in a secure manner, where the contract is either completed or terminated.  
• Consider using University's recordkeeping system to store personal information. The system ensures security by offering version and access controls, unique IDs and an audit log, amongst other features. Contact the University’s Records Management Services for more information.  
• What are our recordkeeping obligations. Not sure? Contact University’s Records Management Services for more information. |
### Key Privacy Principles for Staff

<table>
<thead>
<tr>
<th>Access &amp; Accuracy</th>
<th>Use and Disclosure</th>
<th>Restrictions on Transborder Disclosures</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Be transparent about the personal information the University stores, why the University uses the information and the right to access and amend it.</td>
<td>- Only use personal information for the purpose for which it was collected unless the person consents to it being used for an unrelated purpose.</td>
<td>- You cannot transfer personal or health information outside of NSW, or to a Commonwealth agency, unless it is covered by an exception found in the privacy legislation.</td>
</tr>
<tr>
<td>- If you are responsible for providing access to people’s own personal information, do so without unreasonable delay or expense.</td>
<td>- Only disclose personal information with people’s consent unless they were already informed of the disclosure when the personal information was collected.</td>
<td>- The exceptions for personal information are found in section 19(2) of the PPIP Act.</td>
</tr>
<tr>
<td>- If you are responsible for updating or correcting personal information, provide assistance to people wishing to do so wherever possible.</td>
<td>- Do not disclose sensitive personal information without consent. Sensitive personal information is information about ethnicity or racial origin, political opinions, religious or philosophical beliefs, health or sexual activities or trade union membership.</td>
<td>- The exceptions for health information are found in Clause 14 of Schedule 1 of the HRIP Act.</td>
</tr>
<tr>
<td>- Before you use personal information ensure that it is relevant and accurate before using it.</td>
<td></td>
<td>- The exceptions include the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- The person has consent to the transfer;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- The party to whom you are transferring the information is subject to a law, scheme or contract that upholds principles substantially similar to the privacy principles;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- The transfer is necessary for the performance of a contract to which the University is a party.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If you are considering transferring personal or health information outside of NSW, contact one of the University’s Privacy Officers for advice.</td>
</tr>
</tbody>
</table>

- If you handle student or staff file requests, be clear about the process and timeframes.
**Key Privacy Principles for Staff**

| Health information only – anonymity in certain cases | • Only assign an identifier to an individual where it is necessary for the University to carry out its functions efficiently.  
  • Where it is lawful and practical to do so, give a person the opportunity to stay anonymous when receiving a health service or otherwise providing health information. |
|-----------------------------------------------|--------------------------------------------------------------------------------|
| Health information only – linkage             | • You cannot include health information about an individual in a health records linkage system unless the person consents to the inclusion or it is covered by one of the exceptions at Clause 15 of Schedule 1 of the *Health Records and Information Privacy Act 2002* (NSW). If you’re considering an exception, contact one of the University’s privacy officer’s for assistance.  
  • If you are considering transferring personal or health information outside of NSW, contact one of the University’s Privacy Officers for advice. |

Need more information? [ARMS staff](#) are here to help.