As an institutional manager considering the introduction of an ePortfolio system, you may be faced with some new management issues such as student generated content potentially viewable on the web or by individuals outside your institution.
What is privacy?
Privacy is about people being in control of personal information about them. It is not an absolute right. Students have the right to know how personal information about them will be handled and protected. They should be able to make informed decisions about what personal information they will provide and, where possible, about how personal information is used; how much is shared about them and with whom it is shared.

Why protect student privacy?
Many institutions have legal obligations to protect learner privacy.

By early planning an institution can manage the risks to learners and avoid privacy complaints or the need for costly system changes due to compliance issues.

Take-up of an ePortfolio system is partly dependant upon trust and confidence in that system. Learners with effective controls of their personal information, who understand that this information will remain secure and confidential, are more likely to use your ePortfolio system.

Importantly, poor privacy practices could also lead to security breaches or inadvertent publishing of personal information where there could be considerable repercussions for learners, such as embarrassment, harm to reputation, impact on current or future employment, and increased possibly of identity theft.

Giving learners training on how to use their ePortfolio within your institution’s established policies and guidelines will help them understand how to protect their own privacy, to understand the actionable consequences of any illegal or inappropriate content stored in their ePortfolio and to avoid breaching other learners’ privacy. Such training will also help your institution manage its mandated responsibilities in relation to privacy, intellectual property and copyright.

Which privacy laws are applicable (if any)?
Many but not all ePortfolio providers will be subject to an Australian or state or territory privacy law. Which law applies will depend on organisation type, and other factors such as their annual turnover and whether they are contractors to a state or territory government. In summary:

• The Privacy Act applies to Australian government agencies and to the majority of the private sector including community and not-for-profit organisations. Private education providers, including universities, may be subject to the Privacy Act.
• State and territory agencies (including state education providers and universities established under state laws) will be subject to the relevant state or territory law.

Privacy laws work by establishing information handling rules, or privacy principles. It is important to know the specific privacy principles that will apply to your institution. The basic rules of these laws are, in summary:

• Collect personal information only if it is necessary Tell people why their information is needed and to whom it might be disclosed
• Use and disclose personal information only as could be reasonably expected, for example because you have told users, unless you have consent or there is a legitimate basis such as an emergency or another law
• Safeguard personal information taking account of risks and how sensitive it is
• Give people access to their own information, or correct it if they ask
• Have a privacy policy setting out how personal information will be managed.
The principles will often require organisations to take steps that are reasonable in the circumstances. In other words the steps needed to comply will be a matter of judgment for the ePortfolio provider taking account of the circumstances and good privacy practices.

If your institution is not hosting the ePortfolio you may still need to consider how the law applies to the ePortfolio host, particularly if it stores personal information in another country. The ePortfolio host may then have a different privacy legal framework or be subject to other legal obligations or commitments which may have an impact on learner privacy and which may, for example, need to be reflected in your institution’s terms and conditions for the ePortfolio.

Who owns and controls the contents of ePortfolio?
The question of ownership of and control over the content of an ePortfolio will affect how it is managed. The learner’s privacy as well other rights may be affected.

How the ePortfolio is established will affect, for example, how much control the learner has over what they put into the ePortfolio, who has access to it and whether the content of the ePortfolio goes with them at the end of the course.

For example, if the ePortfolio is being offered in the context of a partnership between a university and an employer to meet requirements for a particular qualification, then the employer may own certain material, or there may be questions of commercial confidentiality. The ePortfolio provider may also need to retain some or all of the ePortfolio content at the end of a course to meet its audit or funding body obligations. Another example may be that the ePortfolio provider may decide that the learner is the owner of the ePortfolio content but may nevertheless specify some limits on the use of the ePortfolio system.

From a privacy perspective, it is important to be clear about the issues related to ePortfolio use and communicate these to the learner as part of the process of establishing the system. It is usually a good idea to talk to learners about their perspectives on privacy of personal information within an ePortfolio environment as policy and approaches are developed.

How can privacy risks be managed?
The best way to manage privacy risks is to think about them upfront and plan the system to protect and promote privacy. This starts with understanding what personal information will be held in the system and what privacy risks could arise. Institutions can then think about the system design, education and training, policies and procedures needed to manage the risks.

Your institution may already have some privacy or other relevant policies and procedures. The ePortfolio plan would then build on these filling in any identified gaps.

The key areas to consider are:
- How can the system be made secure for example from accidental disclosure, hacking or other online security risks
- How to tell learners about the rules of the system and privacy risks and help them learn to protect themselves
- How to manage access and learner controls for the ePortfolio so that system support staff, educators, assessors and employers can see only the sections of the ePortfolio that are relevant to their role.

Planning for Privacy – What are the purposes and objectives of your ePortfolio system?
In thinking about privacy, it is important that your institution has an understanding of the ePortfolio system’s purpose and objectives. These are likely to determine matters such as the content of the ePortfolio, who will need access and in which circumstances.

Clearly stating the purpose and objectives in a privacy plan will make it easier for your institution to decide on steps required to protect individual users’ privacy. It will also make it easier to decide important matters such as the terms and conditions of use of the system.
Planning for Privacy – What will the ePortfolio contain?

An understanding of the ePortfolio’s objectives will also help your institution plan for privacy around potential content. What personal information is likely to be stored in the ePortfolio and how will this information be collected, used and disclosed? Questions to ask include:

- What types of personal information might be stored in system? Could this include student profile information or sensitive material for example, personal reflections including on health or other issues?
- Will there be specific rules or limits on content? For example, can the learner include extraneous material such as their CVs or other material not related to your institution’s activities?
- Who, including the learner, institutional staff and third parties, will be able to access the ePortfolio and under what circumstances (eg. public ‘views’ available to anyone or sharing information with auditors)?

In planning the development of ePortfolio systems and services, and in deciding what tools will be needed to manage privacy, an important prior consideration will be which parties will need access to which information in which circumstances. The following matrix (which has been populated purely as an example to show how it might be completed) suggests one approach to undertaking this analysis.

Table 1: Example Access Matrix showing what information and with whom a learner may share

<table>
<thead>
<tr>
<th>Content</th>
<th>Roles</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Learner</td>
</tr>
<tr>
<td>Qualifications</td>
<td>✓</td>
</tr>
<tr>
<td>Assessment results</td>
<td>✓</td>
</tr>
<tr>
<td>Assignments</td>
<td>✓</td>
</tr>
<tr>
<td>Work samples</td>
<td>✓</td>
</tr>
<tr>
<td>Works in progress</td>
<td>✓</td>
</tr>
<tr>
<td>Personal details</td>
<td>✓</td>
</tr>
<tr>
<td>CVs</td>
<td>✓</td>
</tr>
<tr>
<td>Reflections</td>
<td>✓</td>
</tr>
<tr>
<td>References</td>
<td>✓</td>
</tr>
</tbody>
</table>


Planning for Privacy – What will the plan contain?

Developing a privacy plan is a good way to systematically build privacy protection into an ePortfolio system. The content of a privacy plan will depend on an institution’s circumstances. Smaller organisations may not need to do very much and steps can be implemented over time, for example when forms are reprinted, or a new program is set up.

The privacy plan should include specific actions, timeframes and nominate people responsible. It should address:

- The selection and/or design of the ePortfolio system to ensure it includes security features, tools and settings to protect privacy
- Everyday good practice, including policies and procedures, security arrangements and communication and education about how staff can protect an individual’s privacy, and the actions that an individual needs to take to protect themselves
- Governance arrangements including naming those responsible for privacy, audit and assurance processes to ensure policies and procedures are implemented and effective
- Safety-net mechanisms for learners when failure or mistakes occur including easily available information sources and accessible dispute resolution processes.
For more information about privacy and ePortfolios:
Visit www.eportfoliopractice.qut.edu.au to access these other concept guides about privacy and ePortfolios
- ePortfolios and managing privacy for learners
- ePortfolios and managing privacy for academic staff

Need more information about ePortfolios?
Visit www.eportfoliopractice.qut.edu.au
- ePortfolio concepts for learners
- ePortfolio concepts for academic staff
- ePortfolio concepts for information technology and teaching and learning support services
- ePortfolio concepts for institutional managers
- ePortfolio concepts for employers, professional bodies and career services
- ePortfolio concepts for employees

Further reading

Acknowledgment
This brochure has been developed in collaboration with the Australian Flexible Learning Framework’s EPortfolios business activity www.flexiblelearning.net.au/ePortfolios and draws its contents from VET Eportfolios Privacy Guidelines (Australian Flexible Learning Network, 2010).

Contact Details:
Dept of eLearning Services
Kelvin Grove Campus
Queensland University of Technology
www.eportfoliopractice.qut.edu.au

CC - Creative Commons – Non-commercial attribute license. This work is licensed under the Creative Commons Attribution 3.0 Unported License. To view a copy of this license, visit http://creativecommons.org/licenses/by/3.0/ or send a letter to Creative Commons, 171 Second Street, Suite 300, San Francisco, California, 94105, USA.