

# VET E-portfolio Privacy Draft Guidelines

Considerations for managers of learner information and  
e-portfolio service providers

March 2010



## Acknowledgement

These guidelines were written by Information Integrity Solutions Pty Ltd on behalf of the Australian Flexible Learning Framework.

The authors, Christine Cowper and Malcolm Crompton, worked in collaboration with the E-portfolios Business Manager, Allison Miller, in the consultation, research and writing of this document.

The views expressed herein do not necessarily represent the views of the Commonwealth of Australia.

© Commonwealth of Australia 2010. Licenced under AShareNet Free For Education licence.

This work is copyright and licensed under the AShareNet Free For Education Licence (AShareNet–FfE Licence). The onus rests with you to ensure compliance with the AShareNet-FfE Licence and the following is merely a summary of the scope of the Licence.

You may use and copy any material covered by an AShareNet-FfE licence, for educational purposes only, and only within or for the services of your organisation.

Conditions for the licence can be found at <http://www.aesharenet.com.au/FfE2/>. Queries regarding the standard AShareNet-FfE Licence conditions should be directed to the AShareNet website at <http://www.aesharenet.com.au/help/support/>.

In addition to the standard AShareNet-FfE Licence conditions, the following special condition applies: The licence territory is limited to Australia and New Zealand.

Requests and inquiries concerning other reproduction and rights should be directed in the first instance to the Director, VET Technology Policy and Projects, Department of Education, Employment and Workplace Relations, GPO Box 9880, Canberra, ACT, 2601.

# Table of contents

<b>1. Introduction and overview</b> .....	<b>2</b>
1.1 About privacy .....	2
1.2 E-portfolios and privacy risks .....	3
<b>2. About these guidelines</b> .....	<b>4</b>
2.1 General approach .....	4
2.2 Guidelines based on Unified Privacy Principles .....	4
2.3 Guidelines assume e-portfolios are ‘personal information’ .....	5
2.4 Ownership and control – impact on compliance obligations .....	5
2.5 Learner generated content – impact on compliance obligations .....	5
2.6 Glossary and key terms .....	<b>Error! Bookmark not defined.</b>
<b>3. Steps in setting up a privacy protective e-portfolio system</b> .....	<b>6</b>
3.1 Establishing an e-portfolio system – privacy checklist .....	7
3.2 Steps to assist service providers complete the privacy checklist .....	8
<b>4. Privacy principles and e-portfolios – tips for compliance</b> .....	<b>16</b>
4.1 Important information about this guidance material .....	16
4.2 Planned approach to privacy compliance .....	17
4.3 UPP summary and tips for compliance .....	18
<b>5. E-portfolios – Terms and Conditions of use relating to privacy</b> .....	<b>24</b>
5.1 Service provider obligations or commitments .....	24
5.2 Learner responsibilities and obligations .....	25
<b>6. For more information</b> .....	<b>25</b>
<b>Appendix 1: E-portfolio software and system assessment checklist</b> .....	<b>26</b>
<b>Appendix 2: E-portfolio use cases and privacy compliance issues</b> .....	<b>29</b>
1. Using an e-portfolio to enter accredited training .....	29
2. Using an e-portfolio to support workplace training and assessment .....	29
3. Using an e-portfolio to gain employment .....	30
4. Providing an e-portfolio service .....	31
<b>Appendix 3: List of Australian privacy laws</b> .....	<b>32</b>
<b>Appendix 4: Resources</b> .....	<b>34</b>

## 1. Introduction and overview

These draft guidelines have been developed for e-portfolio service providers (service providers)<sup>1</sup> and managers of learner information (MLI)<sup>2</sup> in the vocational education and training (VET) sector.

They are intended to offer practical guidance and some tools to assist service providers to:

---

<sup>1</sup> An e-portfolio service provider is an organisation which hosts an e-portfolio system.

<sup>2</sup> People within a RTO who are responsible for the information held about learners – for example, ICT and administrative support personnel, ICT and educational managers.

- comply with obligations under applicable privacy law and avoid compliance problems which could lead to the need for costly changes or for e-portfolio systems to be under-utilised and
- assure learners that they are in control of the personal information held in an e-portfolio system and that this information will remain secure and confidential, thereby building trust and confidence, and therefore take-up, amongst learners.

These guidelines focus on privacy compliance and good practice for service providers. They are intended to complement, not replace, service providers' existing privacy policies and procedures.

The advice in these draft guidelines is not legal advice and should not be relied upon as such. Rather, it is general advice about good privacy practice. If there were any conflict between these draft guidelines and relevant law or existing service provider guidelines the latter would take precedence.

These draft guidelines contain:

- a checklist of matters of privacy to consider when establishing an e-portfolio system, with some explanatory notes and tools
- an overview of privacy principles and some tips for compliance
- sample e-portfolio use cases, identifying key privacy compliance issues
- issues to consider in developing terms and conditions for e-portfolio system use.

These draft guidelines are a result of a Privacy Impact Assessment (PIA) of the use of e-portfolios in VET in 2009. The PIA was undertaken by Information Integrity Solutions (IIS) on behalf of the Australian Flexible Learning Framework's (Framework<sup>3</sup>) E-portfolios business activity<sup>4</sup>, as outlined in the *VET E-portfolio Roadmap* (Roadmap<sup>5</sup>). The *VET E-portfolio Privacy Impact Assessment Report*<sup>6</sup> details the outcomes of this PIA.

## **1.1 About privacy**

Broadly speaking, the concept of privacy includes information, bodily, territorial and communications privacy<sup>7</sup>. Put another way, privacy is "...the right to control access to one's person and information about one's self. The right to privacy means that

---

<sup>3</sup> The Framework is the national training system's e-learning strategy:  
<http://flexiblelearning.net.au>

<sup>4</sup> The E-portfolios business activity supports the development of national e-portfolio standards to improve the portability of learner-collected evidence of learning:  
<http://flexiblelearning.net.au/e-portfolios>

<sup>5</sup> The *VET E-portfolio Roadmap* is a national strategic plan designed to support the diverse requirements for e-portfolios in VET, and aims to assist in the development of a standards-based framework: <http://www.flexiblelearning.net.au/content/e-portfolios-resources>

<sup>6</sup> *VET E-portfolio Privacy Impact Assessment Report* :  
<http://www.flexiblelearning.net.au/content/e-portfolios-resources>

<sup>7</sup> For a detailed discussion of the concept of privacy see the Australian Law Reform Commission's Report 108 *For Your Information: Australian Privacy Law and Practice*:  
[www.alrc.gov.au](http://www.alrc.gov.au)

individuals get to decide what and how much information to give up, to whom it is given, and for what uses<sup>8</sup>.

Australia's sets of privacy laws focus on protecting personal information (called data protection in some international jurisdictions). They operate by setting information handling rules called privacy principles. The rules follow the information life cycle (the flow of information through an organisation), and aim to balance and take account of the interests of individuals, organisations and wider society.

Generally, privacy principles set limits and expectations about the handling of personal information. For example:

- Personal information should only be collected if necessary, and only for a specified purpose.
- Individuals should be told about matters affecting their personal information, such as to who the information might be passed on to and, in some laws, asked for consent to the collection of sensitive information. Where possible and appropriate, the anonymity of the information should be maintained.
- Personal information should be used or disclosed only in ways consistent with the stated purpose of collection, unless exceptions apply including where consent is given or law enforcement or health or safety needs apply.
- Appropriate steps must be implemented to ensure personal information is held and managed safely, as well as be accurate, up-to-date and complete.
- Individuals' rights of access to the information held about them, and the need for corrections to be made to any inaccurate information must be explained.

## **1.2 E-portfolios and privacy risks**

E-portfolios are becoming increasingly popular in the VET sector. They are exciting and potentially powerful tools for learners:

- undertaking course work
- collating evidence of skills and achievements
- to assist in the recognition of prior learning (RPL), or
- when seeking employment.

However, e-portfolios can hold a variety of information, including personal information about learners, some of which may be quite sensitive.

While service providers often will be providing access to an e-portfolio for learning or assessment activities, learners will largely generate the content to be stored in the e-portfolio. Learners may also be primarily responsible for mediating access to their e-portfolio by service provider staff, employers or the wider world.

This combination of factors means there is considerable potential for learners' personal information to be inappropriately disclosed or otherwise misused (including by learners themselves). For learners, privacy risks include:

- the potential for the learner to inadvertently disclose inappropriate information, for example about a health issue or a poor assignment results, to an employer or the world at large

---

<sup>8</sup> Privacy Commissioner of Canada Speech at Freedom of Information and Protection of Privacy Conference, 13 June 2002.

- that the use of an e-portfolio exposes them to online security risks such as hacking or identity fraud or theft
- that the contents of an e-portfolio are used or disclosed in ways they did not expect or welcome, either by service providers or other parties and either intentionally or unintentionally.

The consequences for learners could be severe. There is potential for embarrassment, harm to reputation, impact on current or future employment, and possibly an increased risk of identity theft. The risk increases where the e-portfolio is not confined to the 'walled garden' of an organisation but rather is used to actively engage in the online environment.

For service providers, failure to set up procedures to govern access, use, or disclosure of personal information in an e-portfolio system, or to support learners to use e-portfolios safely, may lead to privacy complaints, risk to reputation or under utilisation of the e-portfolio system.

## 2. About these draft guidelines

### 2.1 General approach

The e-portfolio environment is complex and service providers' obligations under privacy principles could vary considerably depending on the nature of their organisation, where they are located and how the e-portfolio service is being provided. Brief guidelines such as these will not be able to tell service providers what to do in the full range of possible circumstances.

In addition, as privacy principles generally set minimum standards, simply complying with the principles may not be all that is needed, particularly where the service provider considers it important to build learner trust and confidence in using the e-portfolio system.

In some areas, the guidelines suggest steps that are good practice and may be more than is strictly required by the privacy principles.

While service providers may draw on the information in these draft guidelines, they will need to ensure compliance with the local law nevertheless.

### 2.2 Guidelines based on Unified Privacy Principles

Australia has a complex array of privacy laws at the national and state and territory levels. This means service providers will be subject to different privacy laws, or in some cases no privacy law, depending on factors such as whether they are Australian Government agencies, state or territory agencies, or private or community based organisations. Section 3.2, step 4 of these draft guidelines explains how service providers can find out which privacy law might apply.

While there are some important variations, the key Australian privacy laws all have at their core a set of privacy principles with similar themes and obligations.

These draft guidelines use a set of privacy principles called the Unified Privacy Principles (UPP)<sup>9</sup>. These principles were drafted by the Australian Law Reform Commission as part of its review of Australia's privacy law framework.

---

<sup>9</sup> Australian Law Reform Commission Report 108, *For Your Information: Australian Privacy Law and Practice Modified Unified Privacy Principles*:  
[http://www.austlii.edu.au/au/other/alrc/publications/reports/108/\\_4.html#Heading21](http://www.austlii.edu.au/au/other/alrc/publications/reports/108/_4.html#Heading21)

The UPP are used here because they combine the Information Privacy Principles (IPP) in the *Privacy Act 1988* (the Privacy Act) which apply to Australian Government agencies, and the National Privacy Principles (NPP) in the Privacy Act that apply to many privacy sector organisations.

### **2.3 Guidelines assume e-portfolios are ‘personal information’**

Australian privacy laws protect privacy by setting rules for the handling of personal information. These draft guidelines use the Privacy Act definition of personal information, which is:

*“information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion<sup>10</sup>”.*

An e-portfolio is essentially a collection of different types of information put together by a learner and in some sense the whole e-portfolio is personal information about that learner. It is possible that some content, for example material prepared by other people or a photo of another person, would not meet strict legal definitions of personal information. However, applying different rules to different elements of the e-portfolio is likely to be complex.

As privacy principles are generally about good information management, these draft guidelines consider all the content of an e-portfolio to be personal information in terms of privacy law.

### **2.4 Ownership and control – impact on compliance obligations**

Australian privacy laws tend to place obligations on agencies or organisations that hold or are responsible for personal information whether or not they are the owners of that information under copyright or other law. In other words, a service provider might have compliance obligations under privacy law to protect personal information in an e-portfolio even where the learner owns that personal information and/or has generated the content.

It is likely to be necessary for service providers to consider ownership of the content of an e-portfolio, as well as legal obligations relating to intellectual property, copyright, obscenity and indecency.

The service provider’s obligations in these areas may have an impact on its approach to privacy. For example, there may be a need to monitor or set limits on e-portfolio content or laws may require service providers to disclose personal information in certain circumstances, ie for law enforcement or health or safety reasons.

### **2.5 Learner generated content – impact on compliance obligations**

As already noted above, the privacy principles in Australian privacy law place obligations on organisations by setting a general framework within which they must operate. The privacy principles are not detailed or specific and this means organisations are responsible (and accountable) for deciding which steps are most appropriate to take to protect privacy in their particular circumstances.

---

<sup>10</sup> Section 6, Privacy Act 1988 -

[http://www.austlii.edu.au/au/legis/cth/consol\\_act/pa1988108/s6.html](http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/s6.html)

A relevant factor in deciding on which actions best meets a service provider's privacy obligations in the provision of an e-portfolio will be the fact that learners may be generating content and may be completely or partly in control of access to the e-portfolio. However, organisations will also need to think about their overall objectives. For example, when a service provider is keen for learners to use an e-portfolio system and to do so in a safe way, the service provider may need to consider privacy actions that go beyond what might be required under minimum standards set by privacy principles.

Where the service provider is able to control, for example, of who has access to the e-portfolio system, privacy protection measures might include instituting policy and technology systems to ensure access is appropriately controlled. However, where the service provider has less control and the use of the e-portfolio system may contribute to learner privacy risk, the focus of privacy activities may be more about ensuring the technology can support learner privacy choices, than on learner education and support.

As a general rule, a 'good practice' approach would be to put in more effort where there are likely to be greater privacy risks for individuals, for example where the likelihood of inappropriate use or disclosure of personal information is high due to the functionality of the e-portfolio system or the group of learners.

E-portfolios can have quite a lot in common with other online social networking services such as Facebook and YouTube. This is a very rapidly evolving environment. Developers of e-portfolio services may find it useful to take note of privacy developments in the social networking space as these may give useful insights for the management of privacy in the use of e-portfolios.

### **3. Steps in setting up a privacy protective e-portfolio system**

This section of the draft guidelines aims to assist service providers by setting out a systematic process to consider issues that may have an impact on privacy compliance or learner privacy for a particular e-portfolio system. Identifying issues or policy questions at an early stage in the process means that responses, including written policies and procedures or education and training, can be in place before the system is implemented.

The checklist in section 3.1 is intended as a planning tool to assist MLIs identify actions needed. It suggests ten key areas that are likely to be important in implementing an e-portfolio system that meets privacy law obligations and protects learner privacy.

The steps in section 3.2 provide more detail about the matters that could be considered at each step and suggest some resources to assist service providers, where needed.

### 3.1 Establishing an e-portfolio system – privacy checklist

	Step	Service providers comments/notes (have issues been addressed, where, etc)	Action needed (Y/N)
1	Establish e-portfolio system purpose and objectives		
2	Consider and list e-portfolio parameters and list likely content		
3	Establish/decide on ownership and control of contents of e-portfolio		
4	Identify applicable privacy law, if any		
5	Assess privacy risks to service provider and to learners, taking account of learner views		
6	Review privacy compliance obligations in relevant privacy law and privacy measures currently in place including: <ul style="list-style-type: none"> <li>• privacy policies and procedures</li> <li>• access and other security controls</li> <li>• staff and management roles, training</li> <li>• monitoring and reporting</li> <li>• any privacy compliance plan (section 4.2)</li> </ul>		
7	Identify e-portfolio features needed to meet purpose and objectives and to manage privacy risks and choose or assess e-portfolio system		
8	Develop plan or strategy to meet any gaps in legal compliance arrangements for e-portfolio system and/or to manage learner privacy risks, including through education and support		
9	Implement plan including: <ul style="list-style-type: none"> <li>• developing policies and procedures</li> <li>• training and support approaches</li> </ul>		
10	Establish mechanisms for ongoing governance and evaluation		

### **3.2 Steps to assist service providers complete the privacy checklist**

#### **Step 1 - Establish e-portfolio system purpose and objectives**

An e-portfolio system may be set up to meet a very specific set of objectives – for example, to meet a course objective, build learner IT skills, or to record evidence of employment tasks completed towards a qualification – or may have broad open-ended objectives. The purpose and objectives are likely to determine matters such as the content of the e-portfolio and who will need access, and in what circumstances.

A clear understanding of the e-portfolio system's purpose and objectives will make it easier to decide on steps to protect privacy.

If the e-portfolio system's purpose and objectives have been established for other purposes, for example course design or funding applications, this is likely to be sufficient for the privacy analysis.

#### **Step 2 – Consider e-portfolio parameters and list likely content**

Compliance with privacy laws requires an understanding of the personal information to be handled and how it will be collected, used and disclosed.

Questions to consider in developing a clear picture of the personal information in an e-portfolio system and how it might be used or disclosed include:

- what types of personal information might be associated with the e-portfolio, including profile information, and the e-portfolio system logs
- what sort of material might be included in the e-portfolio to meet the purpose and objectives
- whether sensitive material – for example, personal reflections including on health or other issues – is likely to be included
- whether the system should/will be able to log use of the e-portfolio; what will be logged; how will the logs be used and how long will they be kept; who will need to access these and for what purposes; and will they be accessible by the learner
- who will need to add material to the e-portfolio:
  - the learner
  - a teacher, trainer, tutor or other service provider staff, for example assessment comments, or marks
  - other learners
  - external parties, for example employers, workplace supervisors or mentors
- should there be specific rules or limits on content
- can the learner include extraneous material, for example CVs or other material not related to the service provider's activities
- who, including the learner, service provider staff and third parties, will be able to access the e-portfolio and under what circumstances ie public 'views' to the whole world.

It would be desirable to consult with learners at this point to get their views or concerns about how the e-portfolio system might be established.

In planning the development of e-portfolio 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 exercise to show how it might be completed) suggests one approach to undertaking this analysis.

**Table 1: Example Access Matrix**

Content	Roles						
	Learner	MLI	System Admin	Tutors	Other teaching staff	Employer	Wider world
Qualifications	√	√	√	√	Where relevant	With consent	With consent
Assessment results	√	√	√	√	Where relevant	With consent	With consent
Assignments	√	√	√	√	X	With consent	With consent
Work samples	√	With consent	√	With consent	X	With consent	With consent
Works in progress	√	With consent	√	With consent	X	X	With consent
Personal details	√	Where relevant	√	Where relevant	X	X	With consent
CVs	√	Where relevant	√		X		With consent
Reflections	√	With consent	√		X	X	X

**Resources:**

Table 2: *UPP Summary and Tips for Compliance table* in section 4.3 gives a summary of privacy principles relating to collection, use and disclosure of personal information and the compliance steps that may be needed once the service provider has an idea of what personal information will be held in the e-portfolio.

**Step 3 – Decide on ownership and control of contents of e-portfolio**

Section 2.5 noted that the question of ownership of the content of an e-portfolio is not directly a privacy question.

However, ownership issues may affect how the e-portfolio is established including how much control the learner has over who has access or the nature of the content. For example, if the e-portfolio is being offered in context of a partnership between an RTO and an employer to meet requirements for a particular qualification, then there may be issues of employer ownership of certain material, or questions of commercial confidentiality. The service provider may also need to retain some or all of the e-portfolio to meet its audit or funding body obligations.

Another example may be that the service provider may decide that the learner is the owner of the e-portfolio content but may nevertheless specify some limits of the e-portfolios systems use, such as in the case of Queensland University of Technology (QUT), which prohibits the inclusion of offensive material or that the e-portfolio cannot be used for commercial purposes.

From a privacy perspective, the important thing is to be clear about the issues related to e-portfolio use and communicate them to the learner as part of the process of establishing an e-portfolio. It is likely to be helpful to obtain learner perspectives on privacy of personal information within an e-portfolio environment as policy and approaches are developed.

#### Resources:

Australian Flexible Learning Framework, *Managing Learner Information - Important Considerations for implementing e-portfolios in VET*, final report, April 2009: [http://pre2005.flexiblelearning.net.au/newsandevents/E\\_PORTFOLIOS\\_09/Managing\\_Learner-Info\\_V0-93\\_FINAL.pdf](http://pre2005.flexiblelearning.net.au/newsandevents/E_PORTFOLIOS_09/Managing_Learner-Info_V0-93_FINAL.pdf). This report contains a discussion of ownership on pages 17 and 18.

Ownership is also discussed in material prepared in the United Kingdom, for example, Charleswork A, Home A, *Legal Aspects of ePortfolio Systems: A Short FAQ*: Centre for IT & Law, University of Bristol, JISC Study [http://www.jisc.ac.uk/uploaded\\_documents/Legal\\_Aspects\\_FAQ.pdf](http://www.jisc.ac.uk/uploaded_documents/Legal_Aspects_FAQ.pdf)

The QUT approach is discussed in Kift S, Harper W, Creagh T, Hauville K, McCowan C, Emmett, D, *ePortfolios: Mediating the minefield of inherent risks and tensions*. In *Proceedings ePortfolios Australia – Imagining New Literacies*, RMIT University, Melbourne, 2007: <http://eprints.qut.edu.au/6495/>

#### Step 4 – Identify applicable privacy law (if any)

Many but not all service 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. There are exemptions where the Act does not apply, including for small businesses with an annual turnover of \$3m or less (unless they trade in personal information or handle health information or where they are contracted service providers). 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.

However, the legal situation is complex, particularly where there is health information involved, or where the organisation is a contracted service provider. In these cases legal advice may be needed.

#### Resources:

The key Australian privacy laws are listed at Section 8, Appendix 3 of these guidelines. The websites of the relevant national (<http://www.privacy.gov.au/>) or state/territory (<http://www.privacy.gov.au/law/states>) privacy regulators provide a range of useful information that may assist organisations to establish if a particular law will apply. The Office of the Privacy Commissioner's website includes a checklist to assist organisations, including small businesses or community organisations, to decide if they will need to comply with the Privacy Act. The checklist is available at: <http://www.privacy.gov.au/business/mybusiness/comply>

## Step 5 – Assess service provider and learner privacy risks

The privacy principles that form the basis of Australian privacy laws are high level and in general they set a framework rather than listing specific black and white requirements. In a number of places they 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 service provider.

Service providers will be accountable for their decisions to individuals and to privacy regulators and might, for example, be subject to an audit by a privacy regulator or an investigation where an individual complains about a possible interference with their privacy.

One way for service providers to decide how to go about meeting any privacy law obligations is to consider the nature of privacy risks that they, or learners, may face as e-portfolios are introduced.

The value of a risk management based approach is that it will assist service providers to target their actions, so making best use of resources. It is also a way to take account of the risks that learners may face, which may not otherwise be systematically considered.

The privacy risks in an e-portfolio system will depend on the e-portfolio system parameters as identified at step 2 above and other contextual factors such as:

- learners' age and experience in using ICT tools and e-portfolios in particular
- the particular e-portfolio system adopted and whether it is hosted in-house or held on an external system
- whether personal information is held in Australia or overseas.

A privacy risk assessment could be a relatively short informal process for a small organisation with few learners, or require a significant amount of effort by larger organisations.

There are three key risk factors for the handling of personal information in connections with e-portfolios<sup>11</sup>. These are:

- the extent of user-generated content
- learner control of access to e-portfolio content by third parties and
- the dynamic and online nature of e-portfolio systems.

The key areas to address in managing these risks are:

- making sure learners are aware of the potential privacy risks and are properly educated and supported to manage those privacy risks that are under their control
- scaffolding the right educative framework around the generation of e-portfolio content so that it is appropriate and does not expose learners or service providers to undue privacy risks
- managing access to the content contained with the e-portfolio, including instituting fine grained access controls, so that learners feels assured of the level of control they have over their information, and can allow other people to

---

<sup>11</sup> *VET E-portfolios Privacy Impact Assessment* report - <http://www.flexiblelearning.net.au/content/e-portfolios-resources>

access specific content with the confidence that the third party will not be able to access the whole e-portfolio

- keeping personal information in e-portfolios secure, for example from hacking or other online security risks.

An insight into risk and trust in online services can be found in research conducted through the United Kingdom Trustguide project<sup>12</sup>. This research started with the initial hypothesis that people do not engage with online services because they do not *trust* them, but found that 'What is more important to understand is that people are willing to take risks online, as long as they are informed, and it is clear how consequences will be addressed'. The data collected through Trustguide has enabled the development of a set of guidelines to inform policy making and service development for ICT mediated services. In summary the guidelines are as follows:

- **Education** – Enabling better informed risk decision making. The fundamental foundation of the guidelines lies in education. Citizens engage with services because they make a decision concerning whether it is worth the risk to engage (ie do the pros outweigh the cons). Currently education is sparse and disconnected, resulting in ill-founded beliefs hampering engagement. A more educated online society is more likely to engage with ICT mediated services based upon confidence through knowledge.
- **Experimentation** – Learning through doing. Complementary to education, people will develop trust in a service through experimentation in a 'safe' environment prior to engaging in a potentially risky transaction.
- **Restitution measures** – Provide a positive impact on personal perceived risk. Citizens believe there is no such thing as a secure service and claiming so leads to mistrust. A more effective method of engagement is to clearly state the measures that are in place in the event of something going wrong.
- **Guarantees** – Provide assurance and improve confidence in whether to enter into a transaction through guarantees of restitution. Guarantees should be open and honest, and suitable in aiding an individual in making an informed choice regarding whether to engage with a new service.
- **Control** – Increased transparency brings increased confidence. Citizens are aware of large-scale data collection through online services and mistrustful of it. They know it is their data, and they want to be able to control it.
- **Openness** – Trust is not built through unsubstantiated claims of security and protection. Being clear about the benefits and issues related to a service will engender far greater trust.

As has been suggested at other steps in this guide, it is likely to be helpful to consult learners as part of the risk assessment process.

---

<sup>12</sup> *Trustguide: final report*, Stephen Crane, Hazel Lacohee, Andy Phippen, October 2006: <http://www.trustguide.org.uk/publications.htm>

**Resources:**

Table 2: *UPP Summary and Tips for Compliance table* in Section 4.3 below gives a summary of privacy principles relating to collection, use and disclosure of personal information and the compliance steps that may be needed once the service provider has a picture of what personal information will be held in the e-portfolio.

Appendix 3 at Section 8 lists privacy laws and the relevant privacy regulator – these sites include information about privacy audits, and the privacy complaint process.

A useful framework for privacy risk assessments is the privacy impact assessment guides prepared by privacy regulators. For example, the Victorian Privacy Commissioner's guide: <http://privacy.vic.gov.au>

For larger organisations, Australian standards on risk assessment and security may be relevant. These are available for purchase at:

<http://www.saiglobal.com/shop/script/Result.asp?DegrKeyword=Risk+assessment&Db=AS&SearchType=publisheronly&Status=all&Max=15&Search=Proceed>

**Step 6 – Review privacy compliance obligations and current privacy measures**

These draft guidelines are intended to complement service providers existing privacy protection activities. Steps 1-5 are intended to identify the information needed to determine the privacy issues that will need to be addressed to protect privacy in the context of e-portfolios. This step asks service providers to decide what activities or measures would be needed to address the issues, and then to identify any gaps in current activities or measures. Where there are gaps, policies or procedures may need to be amended or developed or another action, such as staff or learner training, may need to be taken.

The suggested approach is to:

- review the requirements in the applicable set of privacy principles (or the UPP if no law applies and the service provider wishes to adopt these principles), taking account of the information gathered in steps 1-5
- assess measures currently in place (which might include privacy policies and procedures, access and security controls, staff management and training, monitoring and reporting)
- identify gaps or areas where work may be needed.

**Resources:**

If the service provider has a privacy officer or a privacy plan or strategy this step may involve consulting those resources.

Section 4.2 and 4.3 of these guidelines give an indication of the steps that could be needed.

The privacy impact assessment guides prepared by the Office of the Privacy Commissioner (<http://www.privacy.gov.au/materials/types/guidelines>) and the Office of the Victorian Privacy Commissioner (<http://www.privacy.vic.gov.au/privacy/web.nsf/content/guidelines>) include questions and suggestions that may be a helpful framework.

Australian Standard 3806 sets out a framework for compliance that would be relevant for larger organisations. These are available for purchase at:

<http://www.saiglobal.com/shop/script/Result.asp?DegrnKeyword=Risk+assessment&Db=AS&SearchType=publisheronly&Status=all&Max=15&Search=Proceed>.

**Step 7 – Identify preferred privacy features for e-portfolio system and assess systems available**

This step is related to step 5 (identifying privacy risks) and step 6 (identifying existing measures in place) but is noted separately because the e-portfolio system design and the arrangements under which it is offered (if the e-portfolio system is hosted externally) could have a significant impact on the overall privacy scorecard for the e-portfolio system.

The aim in this step is both to establish a clear picture of the privacy issues that may arise in e-portfolio software, and to use this analysis to assist in making a choice between a number of systems, should these be available. Establishing a learner consultation group could be one way of testing the feature of particular systems.

**Resources:**

Appendix 3 at section 8 provides an e-portfolio software and system assessment checklist of privacy features that would, in most cases, be needed in setting up a privacy protective e-portfolio system.

**Step 8 – Develop plan to address identified privacy risks**

The approach and effort required for this step will vary depending on how much work the service provider considers will be needed given the gaps identified.

The plan should include specific actions, timeframes and nominate people responsible. A possible framework to use to ensure that all relevant issues are addressed would be to frame the plan against the key strategies in a layered defence to protect privacy<sup>13</sup>. The layers are as follows:

- 'Business as usual' good practice, which includes considering educational, process and cultural change within an organisation regarding the expectations about the way things are done by staff to protect an individual's privacy, and the actions that an individual needs to take to protect themselves.
- Additional laws are enacted where risks are particularly high (for example specific use and disclosure limitations, criminal penalties, special measures to ensure review before critical changes are made).

<sup>13</sup> VET E-portfolios Privacy Impact Assessment report, page 10: <http://www.flexiblelearning.net.au/content/e-portfolios-resources>

- Technological solutions, including design limits on information collected, what personal information can be connected to what other information, and who can see what.
- Governance changes, including transparency and accountability.
- Safety-net mechanisms for citizens when failure or mistakes occur including easily available information sources and accessible dispute resolution processes.

**Resources:**

The privacy regulator websites, in particular of the Office of the Privacy Commissioner, ([www.privacy.gov.au](http://www.privacy.gov.au)) and the Office of the Victorian Privacy Commissioner ([www.privacy.vic.gov.au](http://www.privacy.vic.gov.au)) have a range of relevant material including information sheets that deal with developing privacy policies and considering security measures and guidelines on matters such as data breach notification. The Notes to step 2 include a sample access matrix that may assist service providers to decide on the analysis of appropriate role based access.

Section 5 of these guidelines sets out matters that could be considered in terms and conditions of use of an e-portfolio system.

QUT has a well-developed e-portfolio system and there is a range of material available about its approach: <http://www.studentportfolio.qut.edu.au/projectinfo/publications.jsp>

**Step 9 – Develop policies and procedures and implement plan**

The approach and effort required for this step will vary depending on how much work the service provider considers will be needed given the gaps identified. Possible policies and procedures that may need to be developed include:

- privacy notices and privacy policies
- terms and conditions of use of the e-portfolio system (see Appendix 4 - E-portfolios – terms and conditions of use relating to privacy)
- training plan based on the privacy risks for learners, the characteristics of the learner group, and the purpose and objectives of the system; issues that may need to be addressed include using privacy settings, setting up access to different 'views' of the e-portfolio to control who can see what, and appropriate online behaviour
- access rules – who can access the e-portfolio and when they can access it, and how do people with access to the e-portfolio, including the learner, know about these access rules
- e-portfolio content monitoring and actions that may result, including responding in emergencies (people at risk of harming themselves or others) or the reporting of inappropriate behaviour.
- security plan with particular emphasis on the tools learners will have to manage access (for example, one-off or time limited passwords)
- data breach notification plan, for example, addressing if and when learners will be told about unauthorised access to their e-portfolio

### **Step 10 - Ongoing governance and evaluation**

Finally, there needs to be a process to ensure privacy promises are kept and that privacy approaches are kept up to date. Governance arrangements essentially close the loop.

Depending upon the service provider's assessments under this checklist, ensuring appropriate governance arrangements are in place may be an important element of the privacy implementation plan in step 9.

Governance measures might include:

- nominating a person in a senior position responsibility for privacy
- developing an audit plan, with a particular focus on ensuring role based access arrangements are working
- undertaking ongoing monitoring of security arrangements including any security incidents
- developing and implementing mechanisms to review privacy complaints and for senior managers to be kept informed of any issues and
- keeping abreast of how learners are managing their e-portfolio through feedback and surveys.

## **4. Privacy principles and e-portfolios – tips for compliance**

This part of the draft guidelines is intended to give service providers and MLIs an overview of the nature of legal obligations that might arise from privacy laws and what actions may be needed to comply with the related obligations.

Where service providers are subject to the privacy law there are a number of factors that affect what steps they might need to take and the level of effort needed. These include:

- privacy laws generally only apply to information about identifiable individuals (often called personal information)
- privacy principles are often high level and general, and require organisations to make judgements about what might be reasonable in the circumstances.

Depending on the law, there may be exemptions including for information that is publicly available or for employee records.

### **4.1 Important information about this guidance material**

To assist service providers, *Table 1: UPP Summary and Tips for Compliance table* in section 4.3 below includes a brief summary of the UPP and examples of the actions that could be taken to comply with the principles.

The table is not intended as legal advice or as detailed description of a service provider's privacy law obligations. It is intended to give an indication of the steps that might be needed to establish privacy law compliant e-portfolios.

The suggestions in Table 1 in section 4.3 are based on guidance material available, for example, from the Office of the Privacy Commissioner and the Office of the Victorian Privacy Commissioner<sup>14</sup>.

## **4.2 Planned approach to privacy compliance**

A helpful approach to privacy compliance is to develop a privacy compliance plan that:

- makes a person in a senior position responsible for privacy compliance and establishing an organisation culture that respects privacy
- identifies privacy knowledge needed by the organisation; for example, the provisions of the relevant privacy law and privacy principles, and a process to obtain knowledge if needed, for example staff training or seeking legal advice
- is based on a review or stock take that identifies what personal information is held and how it is managed from the point of collection to the point of disposal, including, for example, the privacy advice on forms or websites, and the policies and procedures that apply
- identifies any gaps and develops a plan to address these, taking account of the organisation's circumstances
- ensures staff are trained, for example, if they are making decisions about system design, or will be handling sensitive personal information
- includes an appropriate complaint handling system
- includes governance measures to make sure processes are followed and commitments to privacy are met.

The content of a plan will depend on 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.

---

<sup>14</sup> The Office of the Privacy Commissioner: <http://privacy.gov.au>; the Office of the Victorian Privacy Commissioner: <http://privacy.vic.gov.au>

### 4.3 UPP summary and tips for compliance

The information in this section is in summary form to give an indication of the privacy law obligations that a service provider may have. It is not a complete description of all provisions in the UPP or other sets of privacy principles nor is it a comprehensive set of actions needed to comply. Steps similar to these are likely to be included in existing service provider privacy policies and procedures.

**Table 2: UPP Summary and Tips for Compliance table**

Summary of the UPPs		Sample compliance steps for e-portfolio service providers – meeting obligations under the UPPs	Good privacy practice tips for service providers offering e-portfolio systems
UPP 1 Anonymity and pseudonymity	Where lawful and practicable, give individuals the option of transacting with you anonymously or pseudonymously.	<ul style="list-style-type: none"> <li>Unlikely to be practicable to offer e-portfolios anonymously and learners will generally only be giving access to specified people in specified circumstances.</li> </ul>	<ul style="list-style-type: none"> <li>Unlikely to be practicable to offer e-portfolios anonymously so no additional measures suggested.</li> </ul>
UPP 2 Collection	Collect personal information only where necessary, by fair and lawful means and not in an unreasonably intrusive way.	<p>Collection of personal information into e-portfolio is a shared process.</p> <p><u>Service provider control</u></p> <ul style="list-style-type: none"> <li>Consider collection process – is it fair, not unreasonably intrusive. For example, are learners informed, aware of privacy risks before they start to include information in an e-portfolio.</li> <li>Where service provider actively collects (or adds) information including account profiles, system logs, assessment feedback or grades:                             <ul style="list-style-type: none"> <li>consider if the collection of personal information is necessary</li> <li>develop collection policy</li> <li>review periodically.</li> </ul> </li> </ul> <p><u>Learner control</u></p> <ul style="list-style-type: none"> <li>Where the service provider collects personal information passively (that is where the learner adds information to their e-portfolio) the service provider should review the need for content rules and include these in terms and conditions of use or other information for learners.</li> </ul>	<ul style="list-style-type: none"> <li>Given the potential for system logs to be used to monitor learner activity and to give insights into their behaviour, decide what logs are really needed, and how they may be used in what circumstances. Also consider potential for logs, if made available to learners, to support learner control and service provider and/or third party accountability.</li> <li>Develop approach to assist learners to use e-portfolios safely, including in relation to what material may be inappropriate to include and/or to permit other parties to view.</li> <li>UK research on encouraging citizen engagement with online services suggests this might include                             <ul style="list-style-type: none"> <li>education, particularly about the nature of risks</li> <li>the ability to ‘experiment’ safely, that is learning through doing in a safe environment</li> <li>giving realistic and honest information about risks and what organisations will do if risks eventuate.<sup>15</sup></li> </ul> </li> </ul>

<sup>15</sup> Locohee H, Crane S, Phippen A, *Trustguide: final report*, October 2006: <http://www.bristol.ac.uk/law/research/centres-themes/law-it/jisc1/kptutguid.pdf>

Summary of the UPPs		Sample compliance steps for e-portfolio service providers – meeting obligations under the UPPs	Good privacy practice tips for service providers offering e-portfolio systems
UPP 3 Notification	Take reasonable steps to make individuals aware of matters such as why your organisation needs the personal information, to whom it might be passed on, the organisation's contact details, their rights to seek access or to complain, and what happens if the information is not provided.	<ul style="list-style-type: none"> <li>Collection is an important control point where service providers share control with learners over content of an e-portfolio, who has access to the e-portfolio and management of security. There is an opportunity to make sure learners are informed and can make informed choices.</li> <li>Develop a privacy notice that would be provided to learners when first setting up an e-portfolio and which is available each time they access the service which sets out what personal information the service provider collects including: <ul style="list-style-type: none"> <li>what personal information (or profile) information is attached to the e-portfolio</li> <li>in what circumstances service provider staff will be able to access content</li> <li>the nature of system logging</li> <li>any disclosures of any content, for example to auditors, or other RTOs.</li> </ul> </li> <li>Privacy notices may be combined with a privacy policy (see UPP 4).</li> </ul>	<ul style="list-style-type: none"> <li>It would be good practice to give learners information about risks, for example, in giving wide access permissions to sensitive content.</li> <li>It would also be good practice to: <ul style="list-style-type: none"> <li>explain what will happen to the e-portfolio at the end of the course etc, what the service provider will retain, for how long, and if and how the learner may take the e-portfolio with them or access it later</li> <li>have terms and conditions of use that explain both the service provider's expectations and obligations and the learner's obligations</li> <li>provide detailed information about the use of system logs including how long logs will be kept, how used and disclosed.</li> </ul> </li> <li>Where the e-portfolio is hosted externally, the service provider should make sure the learner knows: <ul style="list-style-type: none"> <li>if the e-portfolio will be held in another state or country</li> <li>how the host will use or disclose personal information, for example to application developers.</li> </ul> </li> <li>Research is showing that individuals are more likely to understand and act on privacy notices if they are simple, clear and follow a consistent format. Measures to achieve this include: <ul style="list-style-type: none"> <li>seeking advice from plain English experts</li> <li>considering the use of a layered privacy notice for simplicity and clarity<sup>16</sup>.</li> </ul> </li> </ul>
UPP 4 Openness	Have a privacy policy that sets out how your organisation	<ul style="list-style-type: none"> <li>The service provider privacy policy may need to be amended to include information about the handling of personal information in e-portfolios.</li> </ul>	<ul style="list-style-type: none"> <li>Consider including detailed information about e-portfolio privacy risks.</li> <li>Consider including detailed information about what</li> </ul>

<sup>16</sup> See the Center for Information Policy Leadership publication *Ten steps to develop a multilayered privacy notice*: [http://www.hunton.com/files/tbl\\_s47Details/FileUpload265/1405/Ten\\_Steps\\_whitepaper.pdf](http://www.hunton.com/files/tbl_s47Details/FileUpload265/1405/Ten_Steps_whitepaper.pdf); and *Berlin Privacy Notices Memorandum*: [www.privacyconference2003.org/resolution.asp](http://www.privacyconference2003.org/resolution.asp)

Summary of the UPPs		Sample compliance steps for e-portfolio service providers – meeting obligations under the UPPs	Good privacy practice tips for service providers offering e-portfolio systems
	handles personal information including types of information and how used and how individuals can exercise rights to seek access or redress.	<ul style="list-style-type: none"> <li>If the service provider does not have a privacy policy, a basic approach is at section 4.2 above. The Office of the Privacy Commissioner website also has information: <a href="http://www.privacy.gov.au/materials/types/infosheets/view/6562">http://www.privacy.gov.au/materials/types/infosheets/view/6562</a></li> <li>Also consider referring to standards for example the Australian compliance standard AS3806: <a href="http://www.standards.org.au/cat.asp?catid=126&amp;contentid=671&amp;News=1">http://www.standards.org.au/cat.asp?catid=126&amp;contentid=671&amp;News=1</a></li> </ul>	the service provider will or won't be responsible for and how it will assist if things go wrong (for example, the learner discloses inappropriate information or gives access to someone and then wishes to withdraw access).
UPP 5 Use and disclosure	Only use or disclose personal information for the primary or main purpose for which it was collected unless exceptions include consent, public health or safety or legal authority apply.	<p><u>Service provider control</u></p> <ul style="list-style-type: none"> <li>Review/decide how the service provider will use and disclose personal information and have in place procedures to assess purpose/necessity at point of collection.</li> <li>Tell individuals of expected routine uses and disclosures at the point of collection.</li> <li>Develop policies, procedures, and technology controls to ensure decisions about role based access can be enforced and monitored.</li> <li>Develop procedures to assess proposed new uses/disclosures that learners may not be expect including seeking consent, or legal advice.</li> <li>Develop procedures for consent to new uses.</li> <li>Privacy audit to confirm use/disclosure being managed in accordance with principles.</li> <li>Given potential for use of e-portfolio, including logging of e-portfolio activity, to result in a clearer picture of learner's activities, consider impact and necessity of any proposed uses/disclosures.</li> <li>Tell learners about proposed routine uses/disclosures.</li> </ul> <p><u>Learner control</u></p> <p>Where learners have complete discretion over what they want used/disclosed, service providers will not otherwise need to consider UPP 5.</p>	<ul style="list-style-type: none"> <li>Where service providers are using another organisation's e-portfolio service, be aware of how that organisation proposes to use and disclose information about the use or content of e-portfolios and negotiate to limit and/or make sure learners are aware.</li> <li>Where learners are in control of use/disclosure it would be good practice to make sure learners: <ul style="list-style-type: none"> <li>are aware of the risks</li> <li>have tools available that are easy to use that give them good control over who can see what and</li> <li>are educated in how to use the tools.</li> </ul> </li> </ul>

Summary of the UPPs		Sample compliance steps for e-portfolio service providers – meeting obligations under the UPPs	Good privacy practice tips for service providers offering e-portfolio systems
UPP 6 Direct marketing	Use or disclose personal information for direct marketing only where individuals are over 15, would expect this and are able to opt-out of further marketing at any time.	<ul style="list-style-type: none"> <li>• Develop clear information for individuals about the service providers' direct marketing activities and easy to use processes for people to opt-out.</li> <li>• Develop systems to record and enforce learner preferences about direct marketing.</li> <li>• Monitor/audit processes to confirm systems work and are being followed.</li> </ul>	<ul style="list-style-type: none"> <li>• Recognise that use and disclosure for direct marketing is a significant source of distrust in organisations so err on the side of conservative approach and be able to justify any marketing decisions fully.</li> <li>• Recognise that if using a third party to provide e-portfolio platform or services, these organisation may intend to use e-portfolio use or content for targeted marketing and so negotiate limits in contracts and/or ensure learners are aware and able to exercise choice.</li> </ul>
UPP 7 Data quality	Take reasonable steps to ensure that personal information is accurate, complete, up-to-date and relevant.	<p><u>Service provider control</u> Where the service provider has control of personal information and the consequence of poor quality data may be significant it could take steps including:</p> <ul style="list-style-type: none"> <li>• adopting Australian or International Standards for records management eg AS ISO 15489: <a href="http://www.naa.gov.au/records-management/IM-framework/requirements/Standards/AS-ISO-15489.aspx">http://www.naa.gov.au/records-management/IM-framework/requirements/Standards/AS-ISO-15489.aspx</a></li> <li>• developing and implementing quality control processes including when and how often personal information is reviewed and updated</li> <li>• extending possible collection of personal information directly from the learner concerned and encouraging them to review/update information.</li> </ul> <p><u>Learner control</u> Where the learner has complete or significant discretion over the e-portfolio content the service provider would not generally need to take steps in relation to UPP 7.</p>	<ul style="list-style-type: none"> <li>• If the service provider has data quality measures in place no additional steps needed.</li> </ul>
UPP 8 Data security	Take reasonable steps to protect personal information from misuse, loss, unauthorised access, modification or disclosure.	<p>This will be an area where, depending on the e-portfolio system responsibility will be shared:</p> <ul style="list-style-type: none"> <li>• learners' responsibilities would include having a safe computer (eg installed up to date anti-virus and spy-ware software) and protecting their passwords</li> <li>• service providers' responsibilities would include</li> </ul>	<p>Issues likely to be addressed by a combination of technology measures, governance arrangements, policy development, legal compliance and education as well as information for learners.</p> <p>Recognise that using a third party e-portfolio platform or services may introduce particular security risks that may need to be addressed in contracts or by making learners</p>

Summary of the UPPs		Sample compliance steps for e-portfolio service providers – meeting obligations under the UPPs	Good privacy practice tips for service providers offering e-portfolio systems
		<p>developing and implementing approaches to data encryption, identity management, role based access and hacking prevention.</p> <p>Service providers could consider steps that include:</p> <ul style="list-style-type: none"> <li>• identifying relevant security standards</li> <li>• security risk assessment</li> <li>• develop policies, procedures or institute technological measures, including role based access controls</li> <li>• establish governance framework</li> <li>• consider data breach security notification plan.</li> </ul>	are aware and able to exercise choice.
UPP 9 Access and correction	Give individuals access to personal information held about them without charge, or with reasonable charge, unless an exception applies and take reasonable steps to correct information if requested.	<ul style="list-style-type: none"> <li>• Establish policies and procedures in relation to matters such as: <ul style="list-style-type: none"> <li>○ whether fees will be charged for access and if so at what rate</li> <li>○ how learners request access</li> <li>○ steps to verify identity before providing access</li> <li>○ circumstances in which access might be denied.</li> </ul> </li> <li>• Review regularly in light of feedback or any complaints.</li> </ul>	<p>Decide what will happen to e-portfolios at the end of the learner's relationship with service provider and make this known to learners, in particular:</p> <ul style="list-style-type: none"> <li>• will the service provider need to retain any/all content of the e-portfolio and for what purposes and for how long will the information be retained</li> <li>• will the learner be able to access content held by the service provider and in what circumstances</li> <li>• will the learner be able to 'pack' and take any or all of the content of the e-portfolio when they leave.</li> </ul>
UPP 10 Government identifiers	Unless authorised by law do not adopt government identifiers as the organisation's identifier for an individual <sup>17</sup> .	<ul style="list-style-type: none"> <li>• Be familiar with the concept of government identifiers and ensure not adopted.</li> </ul>	<ul style="list-style-type: none"> <li>• No additional steps needed.</li> </ul>
UPP 11 Cross-border data flows	The organisation remains accountable for personal information transferred across	<ul style="list-style-type: none"> <li>• Ensure the service provider control of the data by understanding data flows, including third party service providers.</li> <li>• If personal information is transferred across borders:</li> </ul>	<ul style="list-style-type: none"> <li>• This principle may be very significant where an e-portfolio system is hosted in a state other than the one in which the service provider operates (if the service provider is a state agency) or if it is hosted outside Australia.</li> </ul>

<sup>17</sup> Government identifiers are defined at clause 7, Schedule 3 of the Privacy Act and include numbers assigned by federal or state or territory agencies to uniquely identify an individual such as tax file numbers, Medicare numbers or drivers' licence numbers.

Summary of the UPPs		Sample compliance steps for e-portfolio service providers – meeting obligations under the UPPs	Good privacy practice tips for service providers offering e-portfolio systems
	borders except in certain circumstances including that the transfer is required or authorised by law.	<ul style="list-style-type: none"> <li>○ undertake risk assessment and have contractual arrangements with data recipients to ensure privacy protections maintained</li> <li>○ advise individuals before data is transferred.</li> </ul>	<ul style="list-style-type: none"> <li>● The service provider needs to make sure it knows where personal information will be held and handled and under what conditions and that it then takes appropriate management steps in contracts and/or in advice to learners.</li> </ul>
Other issues	Privacy compliance will usually be best managed in the context of a systematic and planned approach to handling personal information.	<ul style="list-style-type: none"> <li>● Overall privacy compliance plan needed – see section 4.2.</li> <li>● Complaint handling and other ‘Safety net’ arrangements are an expected part of privacy protection systems.</li> </ul>	<ul style="list-style-type: none"> <li>● Additional measures could include:                             <ul style="list-style-type: none"> <li>○ data breach notification plan to advise learners if their e-portfolio has been the subject of unauthorised use or disclosure or other security breach</li> <li>○ privacy impact or risk assessments when setting up or changing an e-portfolio system.</li> </ul> </li> </ul>

## 5. E-portfolios – Terms and Conditions of use relating to privacy

This section suggests matters that may be included in Terms and Conditions of use of an e-portfolio system, where a service provider decides to use Terms and Conditions for its e-portfolio service.

There may be some overlap between the items that might be included in the Terms and Conditions, the separate obligations that a service provider may have under privacy principles to provide certain information, and the content of education or support material for learners. This is not necessarily a problem. However, service provider may want to consider how best to ensure learners have the information they need at the point where it is relevant and that there is consistency in approach at all levels.

This guidance is not an exhaustive list of matters and takes the form of issues to address in e-portfolio system Terms and Conditions of use and offers possible approaches rather than providing actual clauses. The actual clauses would be a matter for the service provider to develop taking account of its own circumstances and legal advice if needed. Also, this section will only address privacy issues and will not, for example, address copyright or intellectual property issues.

Organisations offering online services sometimes seek to manage their potential privacy liabilities by adopting a ‘buyer beware’ approach, effectively aiming to leave as much risk as possible with the user.

These draft guidelines aim for a fair approach where the obligations of both parties are made clear and where, when there are risks for individuals, assistance is offered if possible and appropriate. The overall approach suggested for service providers is to:

- make open realistic statements about assurances or risks
- consider which party is in the best position to manage risks
- set out service provider obligations and commitments as well those applying to learners
- ensure that learners have sufficient information and support to meet their obligations and manage the risks that they need to manage.

### **5.1 Service provider obligations or commitments**

Service provider obligations or commitments to consider for inclusion in e-portfolio terms and conditions of use:

- realistic assurance about the operations, for example about security or about stability of content and whether or not the service provider will back up the e-portfolio content
- provide a safe environment, including by investigating and removing inappropriate material
- explain who has access, including IT staff, in what circumstances
- explain what will be logged and how the learner may gain access to this information
- explain retention/deletion of e-portfolio.

## **5.2 Learner responsibilities and obligations**

Learner obligations or commitments to consider for inclusion in e-portfolio terms and conditions of use:

- what material may or may not be included
- system etiquette including limits on feedback or comments to others
- system security requirements
- acceptable use including what is personal use
- look after passwords, protecting computer with up-to-date firewall and anti-virus, back up contents (even if the service provider does do this)
- complying with specified legal requirements.

## **6. For more information**

**For more information about the E-portfolios Business Activity:**

Phone: (08) 8348 4075

Website: <http://flexiblelearning.net.au/e-portfolios>

Blog: <http://www.flexiblelearning.net.au/e-portfoliosblog>

**For more information on the Australian Flexible Learning Framework:**

Phone: (07) 3307 4700

Email: [enquiries@flexiblelearning.net.au](mailto:enquiries@flexiblelearning.net.au)

Website: [flexiblelearning.net.au](http://flexiblelearning.net.au)

## Appendix 1: Glossary and key terms

Term	Description
ACE	Adult and community education
ALRC	Australian Law Reform Commission
Framework	Australian Flexible Learning Framework
IPP	Information privacy principles
LMS	Learning management system
Learners	Learners, or other users of e-portfolios
MLI	Managers of learner information (MLIs) are the people within RTOs responsible for establishing and managing such systems
NPP	National privacy principle
Personal Information	Information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion <sup>18</sup>
PIA	Privacy impact assessment
Privacy Act	Privacy Act 1988 (Commonwealth)
RPL	Recognition of prior learning
RTO	Registered training organisation
Service provider	An organisation providing an e-portfolio service
UPP	Unified Privacy Principles
VET	Vocational education and training

---

<sup>18</sup> Section 6, *Privacy Act 1988*:  
[http://www.austlii.edu.au/au/legis/cth/consol\\_act/pa1988108/s6.html](http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/s6.html)

## Appendix 2: E-portfolio software and system assessment checklist

The factors set out in steps 1-5 in section 3 of the draft guidelines will assist service providers to decide on the privacy risks associated with their e-portfolio system and therefore the extent to which privacy protective features will be critical or desirable.

The following checklist lists features that are likely to be needed in establishing a privacy protective e-portfolio system.

E-PORTFOLIO SOFTWARE AND SYSTEM ASSESSMENT CHECK LIST		
Privacy principle	E-portfolio design – privacy features	Yes/No
UPP 2.3 - fair, not unreasonably intrusive collection	Provides privacy preference settings that are easy to use, with the default setting being for maximum privacy protection	
UPP 3 - Collection	Provides for flexibility and transparency in what personal information (including learner profiles) is associated with an e-portfolio and extent to which e-portfolio use and access is logged	
UPP 4 - Openness UPP 5 - Use and disclosure UPP 8 - Security	Supports MLIs or service provider management of access to e-portfolio by allowing fine-grained access controls based, for example, on assigned roles and/ identity based access	
UPP 5 - Use and disclosure UPP 8 - Security	Allows learner to hold and manage sensitive information with confidence that it will not be inadvertently disclosed or accessed inappropriately	
UPP 5 - Use and disclosure UPP 8 - Security	Caters for full range of learner privacy preferences in matters such as: <ul style="list-style-type: none"> <li>• who can see what and when</li> <li>• who can add what information and when etc</li> </ul>	
UPP 4 - Openness UPP 5 - Use and disclosure UPP 8 - Security	Supports accountability by service providers, MLIs by providing for logging of all access to e-portfolios and for logs to be available for monitoring by service provider and learner	
UPP 5 - Use and disclosure UPP 8 - Security	Provides for learners or service providers to permanently delete information from an e-portfolio	
UPP 5 - Use and disclosure	Provides for learners to be able to take the e-portfolio or a copy of the contents with them when ending a relationship with a particular e-portfolio service provider	
UPP 7 - Data quality	Provides for stable e-portfolio content, and makes sure that descriptions of e-portfolio features highlight any risks to data quality (accuracy, complete, up-to-date and relevant)	
UPP 8 - Security	Able to meet formal e-portfolio security standards, and security issues, including encryption of sensitive material, specified by service providers	

<b>E-PORTFOLIO SOFTWARE AND SYSTEM ASSESSMENT CHECK LIST</b>		
<b>Privacy principle</b>	<b>E-portfolio design – privacy features</b>	<b>Yes/No</b>
UPP 9 - Access and correction	Supports service provider obligations to be able to give learners access to personal information about themselves, including logs of access to the e-portfolio by the learner or others	
Learner education and support	Support flexibility in user interfaces and allows for information about privacy options, privacy risks, and responsibilities to be placed where learners are likely to see and understand it	
<b>Privacy principles</b>	<b>Considerations when e-portfolio to be hosted on another organisation's system</b>	
UPP 3 - Notice UPP 4 - Openness UPP 5 - Use and disclosure	Is there a contract, or terms and conditions of service and privacy policy and do these accord with the service provider and learner expectations?	
UPP 5 - Use and disclosure UPP 8 Security	Will e-portfolio be accessible on internet, in what circumstances?	
UPP 5 - Use and disclosure UPP 8 Security	Will personal information be disclosed to application developers or other third parties?	
UPP 6 - Direct marketing	Will personal information be disclosed to advertisers?	
UPP 6 - Direct marketing	Is it possible for learners to opt-out of receiving advertising and is it easy to opt-out?	
UPP 8 - Security	Will personal information be deleted from the host's system at the end of the arrangement?	
UPP 11 - Cross border data flows	Will e-portfolio information, including personal information, be held outside Australia?	

## Appendix 3: E-portfolio use cases and privacy compliance issues

This section is intended to complement the earlier material by providing some examples for service providers. For each use case the major issue to consider are identified.

### **1. Using an e-portfolio to enter accredited training**

Jane has been working for a number of years as an early childhood worker at the local childcare centre. She has undertaken a variety of projects and job roles, including acting as the Director of the centre while her manager was on leave. During this time Jane has been using the e-portfolio supplied by her employer to plan activities and manage the work she is responsible for.

Jane is now required to gain a formal qualification as part of her Centre's re-accreditation process and she approaches her local training organisation to gain this qualification. As Jane has considerable experience in this area, the training organisation suggests Jane goes through an RPL (recognition of prior learning) process to determine the skills she already has. Jane is able to share evidence in her e-portfolio with the training organisation to demonstrate which skills she already possesses. She will also be able to provide her employer with an electronic academic transcript/parchment through her e-portfolio, which demonstrates she has the required qualification.

#### ***The major privacy issues here are likely to be:***

- From the employer's perspective, as the e-portfolio service provider who provides Jane with an e-portfolio partly to help her manage her childcare role, questions include will Jane's use of the e-portfolio for an RPL process compromise childcare client confidentiality (UPP 5, UPP 8).
- From Jane's perspective, does the e-portfolio tool give her enough control so that she can be confident the RTO will only view necessary information in the RPL process (UPP 8).
- If Jane is going to provide the RTO with online access to her e-portfolio, Jane and the employer will want to be confident that she can safely give the RTO access without compromising system or content security (UPP 8).
- Depending on the conditions under which the employer offers Jane the e-portfolio she may also want to be sure that in giving her employer access to her qualifications she can be confident other content will remain confidential (UPP 8).
- The employer may also want to be certain of the veracity of the qualifications viewed however that issue is not strictly a privacy question.

### **2. Using an e-portfolio to support workplace training and assessment**

Jonas is a production line shift worker with a major manufacturing company. A number of his fellow workers will be retiring in the coming years, and so Jonas' employer has offered him a work-based traineeship as part of their succession planning to fill these on-coming vacancies.

With the support of a workplace mentor, Jonas is able to undertake a large proportion of his training on the job, and collects the evidence of his new skills through the

training organisation's e-portfolio that his off-the-job assessor has helped him to develop. Jonas' off-the-job assessor receives regular emails notifying him of the work Jonas has uploaded into his e-portfolio which demonstrates the new skills he is developing. Jonas' off-the-job assessor then marks and comments on this work within Jonas' e-portfolio, as feedback for both Jonas and his workplace mentor, who can also access Jonas' e-portfolio.

***The major privacy issues here are likely to be:***

- The RTO will need to make sure Jonas is aware of the parties accessing his e-portfolio and what they will be able to look at (UPP 2 and UPP 3).
- If the e-portfolio system allows Jonas to control access, his ability to understand and use the system effectively to protect his privacy will be an issue – the RTO might want to offer specific training and support (UPP 5 and UPP 8 and privacy good practice).
- If the RTO uses a third party online service provider to host the e-portfolio system it will need to review a range of matters including what information the third party records about use of the e-portfolio system, whether it discloses any details to other parties (including application developers, or marketers) and whether the e-portfolio is held in within Australia or overseas. Both the Jonas and the employer may need advice about these matters (UPP 8, and privacy good practice).

### ***3. Using an e-portfolio to gain employment***

Jamie has been running her own home garden maintenance business for several years. Recently she became interested in using some of her creative talents and enrolled in a 'Garden Design' accredited course at her local college.

As part of her course work, Jamie has been developing an e-portfolio supplied by the college, which contains examples of the work she has been doing for her own clients as part of her business, as well as the work which has been set by her instructor at the college to complete. Jamie's e-portfolio also allows her access to her course results from the training organisation's student management system.

Jamie will finish her qualification this semester and would like to formally start her own garden design business, using examples from her e-portfolio to promote the types of work she undertakes to potential clients, as well as to gain membership of the Professional Garden Designers Association by electronically demonstrating she has the required qualification and skill to be a member. At the end of her course, Jamie will need to export a copy of her college e-portfolio, which she can save either onto a CD or import into a compatible e-portfolio system.

***The major privacy issues here are likely to be:***

- The college allows Jamie to access her course results via her e-portfolio and so it will need to be sure that this access is secure and controlled, for example can it be certain that Jamie cannot see other results, and cannot amend any details (UPP 5 and UPP 8).
- As it is allowing Jamie to use her e-portfolio for her own purposes, as well as to meet course requirements, it would need to have told her about the options (and any limitations) for her to take the e-portfolio content with her at the end of the course (UPP 2, UPP 3, UPP 9 and privacy good practice).

#### **4. Providing an e-portfolio service**

As an organisation with learners of varying training needs, the XYZ Training Company has recognised the need for a more flexible and learner centred approach to training. After attending a local e-learning showcase event, they further investigated incorporating an e-portfolio system into their suite of e-learning tools, which consisted of a learning management system, a wiki and a virtual classroom.

In the initial roll out of the e-portfolio, the system was trialled with *Certificate III in Aged Care* learners, who were able to record and communicate with their trainer during their work placements. After the success of the pilot program, three other industry areas, Hairdressing, Automotive and Hospitality, have started using the e-portfolio system.

- The XYZ Training Company is scaling up its use of e-portfolios.
- It appears to be focussed on using e-portfolios for time limited course specific purposes which may affect learner access to the e-portfolio content after they complete a course.
- It also appears to be using free, open source software and an internet service provider, with possibly greater potential for risk for learners if they include inappropriate material or inadvertently provide wider access than they intended.
- Key areas for privacy action would be:
  - deciding on appropriate use and content for e-portfolio for each course and if/how this will be monitored (UPP 1, and UPP 5)
  - making sure learners are aware of appropriate use and possible monitoring and security risks (UPP 2, UPP 8 and best privacy practice)
  - understanding how personal information will be handled by the internet service provider, what privacy options are available and how these can be managed and advising learners of the risks and strategies (UPP 8 and good privacy practice)
  - deciding if learners will be able to take e-portfolio content with them at the end of the course or if not whether the e-portfolio will remain accessible to the learner.

## Appendix 4: List of Australian privacy laws

Jurisdiction	Key privacy law <sup>19</sup>	Agencies or organisations covered <sup>20</sup>	Regulator and additional information
Australian Government	<p>Privacy Act 1988 (Cth)  <a href="http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/">http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/</a></p> <p>The Information Privacy Principles apply to agencies.            National Privacy Principles apply to most private sector organisations. Small businesses (including community or not-for-profit organisations) may be exempt if they do not 'trade' in personal information and are not health service providers as defined in the Privacy Act.</p> <p>Small businesses can use the privacy checklist at  <a href="http://www.privacy.gov.au/materials/types/brochures/view/6053">http://www.privacy.gov.au/materials/types/brochures/view/6053</a>            to find out if they must comply with the Privacy Act.</p>	<p>Australian Government Agencies            Private sector organisations including community and not for profit organisations unless exempt (for example because they are small businesses, handle health information or are contractors to the Australian Government).</p>	<p>Australian Privacy Commissioner  <a href="http://privacy.gov.au">http://privacy.gov.au</a></p>
ACT	<p>Privacy Act 1988 (Cth) as amended  <a href="http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/">http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/</a></p>	<p>ACT agencies and contractors except when handling health information when other rules apply.</p>	<p>Australian Privacy Commissioner  <a href="http://privacy.gov.au">http://privacy.gov.au</a></p>
NSW	<p>Privacy and Personal Information Protection Act 1998 (NSW)  <a href="http://www.lawlink.nsw.gov.au/lawlink/privacynsw/ll_pnsw.nsf/pages/pnsw_03_ppipact">http://www.lawlink.nsw.gov.au/lawlink/privacynsw/ll_pnsw.nsf/pages/pnsw_03_ppipact</a></p>	<p>NSW agencies and contractors except when handling health information when other rules apply.</p>	<p>NSW Privacy Commissioner  <a href="http://privacy.gov.au">http://privacy.gov.au</a></p>
Northern Territory	<p>Information Act 2002 (NT)  <a href="http://www.austlii.edu.au/au/legis/nt/consol_act/ia144/">http://www.austlii.edu.au/au/legis/nt/consol_act/ia144/</a></p>	<p>NT agencies and contractors.</p>	<p>Information Commissioner  <a href="http://www.privacy.nt.gov.au/">http://www.privacy.nt.gov.au/</a></p>
Queensland	<p>Information Privacy Act 2009 (QLD)  <a href="http://www.austlii.edu.au/au/legis/qld/consol_act/ipa2009231/">http://www.austlii.edu.au/au/legis/qld/consol_act/ipa2009231/</a></p>	<p>Queensland agencies and contractors except when handling health information when other rules apply.</p>	<p>Office of the Information Commissioner  <a href="http://www.oic.qld.gov.au/">http://www.oic.qld.gov.au/</a></p>

<sup>19</sup> In addition to the privacy laws listed here, a range of other laws set out privacy provisions or regulate the handling of personal information in specific circumstances: <http://privacy.gov.au/law>

<sup>20</sup> This is a short summary of a complex area – organisations may need to seek legal advice if they are not clear on which law applies.

Jurisdiction	Key privacy law <sup>19</sup>	Agencies or organisations covered <sup>20</sup>	Regulator and additional information
South Australia	South Australia has issued an administrative instruction requiring its government agencies to generally comply with a set of Information Privacy Principles it has established.	South Australian agencies.	Privacy Committee of South Australia <a href="http://www.archives.sa.gov.au/privacy/committee.html">http://www.archives.sa.gov.au/privacy/committee.html</a>
Tasmania	Personal Information Protection Act 2004 (TAS) <a href="http://www.austlii.edu.au/au/legis/tas/consol_act/pipa2004361/">http://www.austlii.edu.au/au/legis/tas/consol_act/pipa2004361/</a>	Public and local government sectors and the University of Tasmania.	
Victoria	Information Privacy Act 2000 (VIC) <a href="http://www.austlii.edu.au/au/legis/vic/consol_act/ipa2000231">http://www.austlii.edu.au/au/legis/vic/consol_act/ipa2000231</a>	Victorian agencies and contractors except when handling health information when other rules apply.	Victorian Privacy Commissioner <a href="http://privacy.vic.gov.au">http://privacy.vic.gov.au</a>
Western Australia	Currently no specific privacy law in WA		The Act is administered by the Department of Justice and complaints may be made to the <a href="#">Tasmanian Ombudsman</a> . General information on the Act is hosted on the <a href="#">Department of Premier and Cabinet website</a> .

## Appendix 5: Resources

Privacy resources	
1	Australian Flexible Learning Framework, <i>Managing Learner Information – Important considerations for implementing e-portfolios in VET</i> final report, April 2009: <a href="http://pre2005.flexiblelearning.net.au/newsandevents/E_PORTFOLIOS_09/Managing_Learner-Info_V0-93_FINAL.pdf">http://pre2005.flexiblelearning.net.au/newsandevents/E_PORTFOLIOS_09/Managing_Learner-Info_V0-93_FINAL.pdf</a>
2	<i>Budde:e E-security Education Package</i> – This package is designed to raise the e-security awareness of Australian primary and secondary school learners and help them stay smart online: <a href="http://www.staysmartonline.gov.au/games-videos/budde">http://www.staysmartonline.gov.au/games-videos/budde</a>
3	Charleswork A, Home A, <i>Legal Aspects of ePortfolio Systems: A Short FAQ</i> : Centre for IT & Law, University of Bristol, JISC Study <a href="http://www.jisc.ac.uk/uploaded_documents/Legal_Aspects_FAQ.pdf">http://www.jisc.ac.uk/uploaded_documents/Legal_Aspects_FAQ.pdf</a>
4	Cisco Systems - Internet Business Solutions Group, <i>Safe To Play: A Trust Framework For The Connected Republic- A Point of View</i> , Global Public Sector Practice, Post-Nobel Final, February 2008 available at: <a href="http://www.iispartners.com/downloads/2008-02Safe-to-play-white-paper-V9POST-NOBELFINALVERSIONFeb08.pdf">http://www.iispartners.com/downloads/2008-02Safe-to-play-white-paper-V9POST-NOBELFINALVERSIONFeb08.pdf</a>
5	Kallenbach, Paul, Minter Ellison Lawyers, <i>Managing legal risks in the use of social networking sites (SNS) by universities</i> , July 2009: <a href="http://www.minterellison.com/public/connect/Internet/Home/Legal+Insights/Articles/A-HEF-A-Managing+legal+risks">http://www.minterellison.com/public/connect/Internet/Home/Legal+Insights/Articles/A-HEF-A-Managing+legal+risks</a>
6	Kift S, Harper W, Creagh T, Hauville K, McCowan C, Emmett, D <i>ePortfolios: Mediating the minefield of inherent risks and tensions</i> . In <i>Proceedings ePortfolios Australia – Imagining New Literacies</i> , RMIT University, Melbourne, 2007.
7	<i>Advice on identity management</i> . Kim Cameron has develop seven laws on identity management: <a href="http://www.eportfolio.eu/identity/publications/cameronslaws">http://www.eportfolio.eu/identity/publications/cameronslaws</a> <a href="http://www.identityblog.com/stories/2004/12/09/thelaws.html">http://www.identityblog.com/stories/2004/12/09/thelaws.html</a>
8	Lochee H, Crane S, Phippen A, <i>Trustguide: final report</i> , October 2006: <a href="http://www.bristol.ac.uk/law/research/centres-themes/law-it/jisc1/kptutguid.pdf">http://www.bristol.ac.uk/law/research/centres-themes/law-it/jisc1/kptutguid.pdf</a>
9	Office of the Privacy Commissioner's <i>Guide to Privacy for Small Business</i> : <a href="http://www.privacy.gov.au/business/small">http://www.privacy.gov.au/business/small</a>
10	Office of the Privacy Commissioner, <i>Guidelines to the Information Privacy Principles</i> : <a href="http://www.privacy.gov.au/materials/types/guidelines">http://www.privacy.gov.au/materials/types/guidelines</a>
11	Office of the Privacy Commissioner, <i>Guide to handling personal information security breaches</i> : <a href="http://www.privacy.gov.au/materials/types/guidelines">http://www.privacy.gov.au/materials/types/guidelines</a>
12	Office of the Privacy Commissioner, <i>Guidelines to the National Privacy Principles</i> : <a href="http://www.privacy.gov.au/materials/types/guidelines">http://www.privacy.gov.au/materials/types/guidelines</a>
13	Office of the Victorian Privacy Commissioner, <i>Privacy Impact Assessment Guide</i> : <a href="http://www.privacy.gov.au/materials/types/guidelines">http://www.privacy.gov.au/materials/types/guidelines</a>
14	Office of the Victorian Privacy Commissioner – privacy training material: <a href="http://www.privacy.vic.gov.au/privacy/web.nsf/content/public+sector+training">http://www.privacy.vic.gov.au/privacy/web.nsf/content/public+sector+training</a>