Australian Flexible Learning Framework

supporting e-learning opportunities

Managing Learner Information

Important considerations for implementing e-portfolios in VET

April 2009

Final Report

flexiblelearning.net.au

Australian Government

Department of Education, Employment and Workplace Relations

Acknowledgements

The researchers, Alan Bevan, Geoff Hendrick, and Jerry Leeson, gratefully acknowledge the willingness of professionals from across the Australian vocational education and training sector to respond to interview requests and surveys. The authors also wish to express thanks for the encouragement and support from key representatives from the Australian Flexible Learning Framework, particularly Allison Miller, Business Manager, E-portfolios, and Owen ONeill, Business Manager, E-standards for Training.

Table of contents

A

Executive summary

The purpose of this report is to identify the privacy and security requirements for learner content in e-portfolios. This report, produced by the national training system's e-learning strategy, the Australian Flexible Learning Framework (Framework[1]), is based on consultation across the Australian vocational education and training (VET) sector and desk research.

Classifying e-portfolios services and learner information

An underpinning classification for the report is the likely types of e-portfolio services, ranging from:

- a service provided by the Australian Government or other national agency for all Australians
- a national service for all in Australian education and training
- a national service for the VET sector
- a localised service provided for learners and staff at a training institution or a cluster of institutions.

The report also classifies 'learner information' which might be held in an e-portfolio. Three primary classifications are used:

- the location of the content – on a primary e-portfolio or external location
- the owner of the content – the learner or a third party
- the publisher of the content – again, the learner or a third party.

These classifications become underpinning definitions for considerations of ownership, privacy, verification, access control and security.

Defining common learner attributes

Many organisations also hold learner information in repositories such as student management systems (SMS), which would be useful for an e-portfolio to access. In order for organisations to effectively allow access to this information, a common understanding of the types of information being held about a learner needs to be determined.

The ability to define the common attributes of a 'learner' for the VET sector would better enable access to this information, and this report considers a number of ways common learner attributes for the VET sector can be defined.

Ownership

Both learners and e-portfolio service providers need to understand their obligations under copyright law. Not all content within an e-portfolio will be owned by the learner, and the learner will need support to understand about licensed use of such content, including both implicit and explicit licenses. The service provider may need to provide a functionality that allows the learner to limit access to third party content to licensed users. They also need to give consideration to custodial issues associated with the storage and archiving of e-portfolio content.

Privacy

Australian privacy law is currently a somewhat confusing array of overlapping

[1] http://flexiblelearning.net.au

legislation. However, in all cases, the intent of the law is to protect the privacy rights of individuals in cases where agencies are collecting and storing personal information. Passive collection of data by virtue of giving learners the opportunity to store personal information on an e-portfolio service would not appear to be a prime focus. Nevertheless, e-portfolio service providers find themselves in a custodial role with regard to personal information and an expert privacy impact assessment would be prudent.

Active collection of personal information, such as qualifications data, would in almost every case be already conducted in a manner compliant with privacy law. However, further advice may be needed if there are new management practices arising out of e-portfolio use, such as providing third party access to this data as part of a qualifications verification service.

Verification

Stakeholders surveyed as part of this work did not generally regard verification of student work within an e-portfolio to be a new challenge. Almost unanimously, they felt that this issue was no different to the challenge faced by educators in the non-electronic world. They suggested professional judgement is the main basis of verification. However, some suggested ways of supporting verification though technology or through endorsement. Verification channels could also be specified to help relying parties easily obtain third party verification.

However, respondents considered the verification of qualifications data to be of a different order. Three alternative models for qualifications verification are described in this report. It is recommended that the Australian VET sector's approach to a qualifications verification service align with that of the higher education community.

Identification, authentication and access control

The report suggests that an effective e-portfolio service will allow a learner to flexibly give access to whoever the learner chooses. This presents a particular challenge for identity management and authentication. This report considers current approaches to identity management within the Australian VET community and more broadly.

Approaches to authentication of previously identified users who wish to access an e-portfolio service include enabling the provision of a URL or password and trust network approaches.

Respondents to the survey held the view that learners need to have control over who can access an e-portfolio and the parts of the e-portfolio that are exposed for different visitors. Access rights for institutional staff were also recognised as being important.

Summary of recommendations

The following recommendations are directed to the Flexible Learning Advisory Group (FLAG), for the development of generic information and resources for use by managers of learner information considering implementing an e-portfolio system in the VET sector. Implementation of these recommendations would be managed by the Framework's E-portfolios business activity[2], with the support of the Framework's E-standards for Training business activity[3]. Where relevant, a whole of education and training

[2] The E-portfolios business activity supports the development of national e-portfolio standards to improve the portability of learner-collected evidence of learning. This will support a learner's ability to move between training and other forms of education, learning and employment: http://flexiblelearning.net.au/e-portfolios

[3] The E-standards for Training business activity focuses on developing national standards to

approach would be sought through Australian Information and Communications Technology in Education Committee (AICTEC[4]).

Common learner attributes

Recommendation 1: *The auEduPerson specification has been created to support scenarios for authentication in a specific environment. The VET sector should identify and describe scenarios for authentication in its environment and then assess the applicability of specifications such as auEduPerson.*

Recommendation 2: *The MIAP*[5] (Managing information across partners) *approach in the UK should be further investigated to understand potential benefits for the Australian VET context*

Ownership

Recommendation 3: *Generic legal advice should be sought concerning:*

- *the need for explicit or implied licence before third party materials can be published*
- *template licence agreements which can be used to secure third party agreement to include content in an e-portfolio*
- *liabilities associated with defamation, breach of copyright, obscenity and indecency when publishing their materials on an e-portfolio.*

Recommendation 4: *Template policies should be commissioned, concerning content removal, storage and access to address issues associated with learner transition.*

Privacy

Recommendation 5: *A suitably qualified legal officer/agency should be engaged to provide a privacy impact assessment with regard to e-portfolio services and develop generic agreement templates between e-portfolio service providers and learners. Alternatively a whole of education and training approach could be sought through AICTEC.*

Verification

Recommendation 6: *The suitability of the QualSearch22, Purple Passport27 and Digitary29 approaches should be examined as possible models for the verification of electronic records of qualification within the VET sector. This review should take into account the activities of the Australian Higher Education National Diploma Supplement project*[6]*.*

---

underpin essential e-learning infrastructure, conducting research into new technology areas and providing guidance materials and tools to support the effective use of emerging technologies: http://flexiblelearning.net.au/e-standards

[4] AICTEC is a national, cross-sectoral committee responsible for providing advice to all Australian Ministers of Education and Training on the economic and effective utilisation of information and communications technologies in Australian education and training: http://aictec.edu.au

[5] http://miap.gov.uk

[6] http://www.dest.gov.au/sectors/higher_education/publications_resources/profiles/proposal_for_an_australian_higher_education_graduation.htm

Access control including identification and authentication

Recommendation 7: *Development of Trust federation use cases for the VET sector to identify possible business drivers for a trust federation in VET. This activity also needs to be informed by parallel activities in the other education sectors.*

Recommendation 8: *There should be consideration of the option of providing a central OpenID identity service with business rules that limit its population to current or previously enrolled learners within the VET sector.*

Supporting e-portfolio service providers

Recommendation 9: *A VET learner information management framework should be produced, which provides guidance for e-portfolio service providers about:*

- *seeking further legal advice to confirm the appropriateness of the generic advice in its specific circumstances*
- *providing learners with administrative access controls that control guest access to identified sets of content*
- *seeking further legal advice about privacy laws applicable for their specific circumstances with regard to both active and passive data collection*
- *requiring learners to formally declare that content they publish is either their own (or is appropriately licensed and labelled third party content) either as part of the publishing routine or when agreeing at the outset to the terms and conditions of e-portfolio use*
- *recommending that, whenever possible, learners provide contact details whereby material attributed to third parties (such as references and testimonials) can be verified*
- *providing learners with the means of authenticating users through password or OpenID.*

Introduction

This report was commissioned by the national training system's e-learning strategy, the Australian Flexible Learning Framework (Framework), as a component of its E-portfolios business activity for 2008. The purpose of the study is to identify the privacy and security requirements for learner information in relation to e-portfolios.

The study considers the types of content that may be found in an e-portfolio, the security and privacy considerations which may apply to these types of content, user definition and identification, authentication and access issues, and the verification of content.

Scope

The scope of this research report was to:

- identify definitions used to describe learners and to consider the appropriateness of the auEduPerson specification
- identify the types and categories of content stored in an individual learner's e-portfolio
- consider content privacy and security issues
- identify and discuss identification and authentication options
- identify and discuss content verification options.

Audience

This report has been commissioned by the Australian vocational education and training (VET) sector, nevertheless, much of the content is applicable more widely. For this reason, a number of the recommendations suggest consideration be given to escalating activity to the peak cross-sectoral Australian Information and Communications Technology in Education Committee (AICTEC).

Report methodology

The report's analysis and findings are based on both desktop research and consultation with key stakeholders.

The sources for the desktop research are listed in the bibliography.

Stakeholders consulted were categorised in two groups. One set was composed of educational leaders from across the Australian VET sector. The second was composed of ICT experts within VET institutions and jurisdictions. All of these people were identified through members of the national E-standards Expert Group.

Context

This report was written in the context of considerable simultaneous inter-related activity in Australia with regard to e-portfolios. A major higher education research paper, the *Australian ePortfolio Project Final Report*[7] was released in October 2008. Consultation for a *VET E-portfolio Roadmap strategic document*[8] and the *E-portfolios for RPL Assessment* report[9] were also simultaneously undertaken in late 2008. An important precursor to these studies was the report published in April 2007, *Developing E-portfolios for VET: Policy issues and interoperability*[10].

The *Australian e-Portfolio Project Final Report* provides valuable policy and practice context background, both nationally and internationally.

This *Managing Learner Information Report* provides excellent descriptions of the multiple purposes and models of e-portfolios, as well as the need for e-portfolios to cater for lifelong learners. The e-portfolio can be many things to many people, however in the first stages of this report, it is necessary to form some views about who the e-portfolio service provider may be, how a learner may be defined and what types of content is likely to be found in an e-portfolio.

The service provider

Fundamental to any consideration about privacy, security and access control, is a prior consideration about who is the e-portfolio service provider[11]. It is the service provider who is ultimately responsible for these obligations.

However, determining who will be the service provider is not immediately clear. It will be driven by the even more fundamental question: ‘’*For which group(s) of people is the e-portfolio service provided?*’’.

It is necessary to address these matters immediately as the various possible answers will impact on the subject of this report.

For whom

Respondents to the research conducted for this report [respondents] indicated varying views about the group(s) of people for whom an e-portfolio service should be provided. These views can be classified under four categories:

1. E-portfolios for all Australians

Some respondents argued that everyone is a ‘learner’, therefore an e-portfolio must be for all.

Many commented that the e-portfolio must cater for lifelong learning, only some of which is formally undertaken. In this context, the e-portfolio was seen as a consistent tool which captures the often disconnected episodes of formal learning as well as providing a place to record informal learning.

One respondent commented that a new arrival to Australia ought to have the right to establish an e-portfolio, irrespective of the fact that they may have never attended an

[7] Hallam et al., 2008

[8] Framework (to be released in 2009)

[9] Perry, 2009

[10] Curyer, Leeson, Mason and Williams, 2007

[11] See Glossary on page 42 for definition of capitalised terms

Australian education or training institution.

2. E-portfolios for students across the whole of education and training

Underpinning this model was the understanding that there are numerous broad services that already exist for whole of life purposes, such as MySpace and Facebook. In contrast, an e-portfolio was seen by some to have a focus more on formal study and career.

However, learning is not limited to a single sector, jurisdiction or institution, therefore the e-portfolio was seen by some as needing to be a service offered across all sectors.

Respondents acknowledged that engagement with education and training is not necessarily continuous, particularly for the VET sector, and that under this model, education and training institutions would need to provide a service that spans these gaps. This consideration again led to the e-portfolio being seen as a cross-sectoral education and training service covering the whole of life.

3. E-portfolios for the whole of the VET sector

This model is comparable to the previous, except that the focus beyond the VET sector was more on industry than on other sectors of education.

There was an assumption about interoperability – the possibility of transferring an e-portfolio developed in one sector to the e-portfolio environment of another.

Given the inclusion of employment experiences, it was acknowledged that this model needed to be a whole of life service.

4. E-portfolios for students (and staff) at an institution

This model has its roots in current practice where a number of respondents talked about e-portfolios that their institution currently offers. In most cases, this type of e-portfolio was closely related to the business of teaching and learning, often including the submission and assessment of assignments and having close links to learning management systems.

Once again, this model assumed an interoperability solution in order for e-portfolios to be transferred to other environments.

There was an acceptance of the need for an alumni service to cater for student needs after leaving the institution.

A generic name

The foregoing illustrates the range of people who may wish to develop an e-portfolio. A generic name is needed for consistent use in this paper which covers this range. One respondent suggested ‘proponent’, however, on balance, the word ‘learner’ was more commonly used by respondents and is therefore used generically used in this paper to cover all the possibilities described above. It is important to note however that it is used to cover all users of an e-portfolio, with teaching staff potentially also being learners.

By whom

These alternatives regarding the prospective user groups for an e-portfolio throw some light on whom the service provider might be. In turn, understanding the service provider is a prerequisite to an examination of the privacy law obligations and liabilities that are incurred as these laws differ for different agencies.

1. E-portfolios for all Australians

If an e-portfolio service is not to be directly linked to education or training ‘customers’, the service provider would presumably not need to be drawn from the education or training community. Instead, it could be:

- a public sector service (presumably a service of the Australian Government given that it would not be limited to a state or territory jurisdiction), or
- one provided by the private sector, either as:
    - as for-profit body, or
    - a not-for-profit, perhaps a philanthropic agency.

It is possible of course that the education and training sector could offer such a broad service (and/or be closely involved in its design). Given this models all encompassing scope, if the VET sector is to be involved, it would seem inevitably to resolve to an Australian Government service, presumably in this case coordinated by the Department of Education, Employment and Workplace Relations (DEEWR[12]).

2. E-portfolios for students across the whole of education and training

In order to have a mandate from the Australian education and training ‘industry’, such a service would need to be under its control. Whilst the operations of the service could well be outsourced, the responsible entity would need to be a body which has a national leadership role in the education and training community or perhaps is owned by that community. Such bodies appear limited to:

- DEEWR
- A company owned by the Ministers and given a mandate from their owners to provide this service; this company preferably would have a cross-sectoral role.
- Some other entity that receives an endorsement to provide such a service from the combined senior decision makers across the sectors.

It must also be acknowledged that it would also be possible for a body to claim this role without formal endorsement or mandate. Many agile companies have established niche markets on the Internet by virtue of innovation, timing and marketing. The right service at the right time can encourage crowd ‘swarming’ behaviour that establishes its position irrespective of any formal mandate. For example, services like Google, MySpace, Facebook and Linkedin have unquestioned market position without any formal mandate. It is conceivable that an e-portfolio service could be created for use within education and training and achieve ‘market’ pre-eminence by virtue of similar user swarming behaviour.

12 http://deewr.gov.au

3. E-portfolios for the whole of the VET sector

This option is comparable to the previous. For similar reasons, the candidate bodies would be:

- DEEWR
- A company owned by the Ministers and given a mandate from their owners to provide this service. In this case, an option would be a company with a VET training agenda such as TVET, or one with an ICT focus such as education.au.
- Some other entity that receives an endorsement to provide such a service from the senior decision makers of the VET sector.

4. E-portfolios for students (and staff) at an institution

In this case, the e-portfolio service provider would be the institution. Note that in cases where a group of institutions agree to jointly provide the service, the institutions are likely to remain as individual responsible entities but this would ultimately depend on the terms of the agreement they reach governing the service provision.

In summary

Respondents were of the view that an e-portfolio service is needed to cater for lifelong learning. Many commented that there ought to be a single service provided at a national level. Some thought that this was not incompatible with the concept of institution level e-portfolio service provision as long as there was the potential of portability between any institution level e-portfolio service and a longer term national one.

Some respondents commented about the need for an e-portfolio service to accommodate more than just formal education and training: that it also needs to capture informal learning. Others noted that it should transcend just vocational training, covering all sectors of education and training. One respondent commented that there can be simultaneous formal education occurring for an individual and that it would be inappropriate to expect such a person to have more than one e-portfolio.

The recurring theme was one of the needs to accommodate life-long learning with a consistent and enduring service.

From this analysis, it would appear that the body providing an e-portfolio could be any one or more of the following:

- the Australian Government (most probably through the agency of DEEWR)
- some other public sector agency (state or territory based)
- a private sector, for-profit body
- a private sector, not-for-profit agency such as:
- a philanthropic body
- a Ministerial company, such as TVET or education.au
- an education or training institution.

However the weight of feedback leans toward a national service of some form.

Defining common learner attributes

In order to build services which provide information to an e-portfolio system (or other service) across and between organisations and jurisdictions, some common data definitions are required to enable this information to be interoperable or interchangeable. As such, an initial investigation into three potential sources for defining a 'learner' in VET and his or her common attributes was conducted:

- AVETMISS13 statistical reporting requirements
- registered training organisations' (RTOs) student management systems (SMS)
- the auEduPerson specification.

AVETMISS statistical reporting requirements

In VET, each RTO is required to supply statistical information about student enrolment, progress and completion. Typically, this information is stored in a SMS and then exported to meet reporting requirements.

In the UK, the MIAP initiative is repurposing similar types of statistical information already provided to the government by training and education providers to populate learner records (initially focusing on qualifications information) for all learners. Although MIAP is based upon the existence of a national unique learner number[14] (UK-ULN) this approach is an interesting example of repurposing existing information to add new value.

RTOs SMS

To better understand how learner information is stored in SMS, a small survey was carried out with selected TAFE ICT Managers to understand the types of information currently being supported by existing SMS. The following organisations were surveyed:

- Kangan Batman TAFE (QLS, STARS SMS)
- TAFE Tasmania (QLS SMS)
- DET NSW (various SMS used).

Although this sample cannot necessarily be considered representative of the entire sector, it does highlight some of the potential challenges facing VET organisations as information service providers. Table 1 overleaf summarises the types of information held in SMS categorised in terms of the content models developed later in this paper.

[13] The Australian Vocational Education and Training Management Information Statistical Standard
[14] http://www.miap.gov.uk/lrs/uln/

Table 1: Learner attributes stored within surveyed SMS

Information category	Attributes
Learner identity and attributes	Unique student ID Name, address, phone, email Employer Ethnicity, sex, residency, birth date Photo image
Enrolment, course and timetable information	Course/session level enrolment
Assessment	Academic record, awards, competencies, prior learning
Student content	Record of completion of online learning, records of participation in course work

It should be noted that student ID numbers are unique only within the SMS and are not unique in relation to each other. This will make verification of a single learner across different education and training sector organisations more difficult as there is no unique way of identifying that learner.

Sharing and exchanging data about learners

All three SMS survey respondents have developed their own in-house methods to exchange SMS data with other systems and organisations.

Kangan Batman TAFE

Internally, Kangan Batman TAFE exchanges data between its two SMS systems and with the institution's financial system. There is currently no data exchange with the learning management system (LMS). Data is manually uploaded to Skills Victoria and provided to Centrelink as CSV files.

Current and past students have no direct online access to their achievement records on Kangan Batman's SMS, QLS. This can only be achieved through a verbal or written request, subject to satisfactory proof of identity being provided.

Tasmanian Polytechnic (formerly TAFE TAS)

Tasmanian Polytechnic has developed a number of internal system-to-system data interchange methods. In addition to this, it has developed a web interface to its SMS data which allows students to access their results over the internet. Tasmanian Polytechnic has also developed a standards-based (IMS Enterprise) data exchange between its SMS (QLS) and LMS (WebCT).

Tasmanian Polytechnic's current students also have access to their results via a web interface. There is currently no system to allow past student access to their results.

TAFE NSW

TAFE NSW has purchased an enterprise services bus (ESB) to provide an enterprise-wide infrastructure to drive its many integration requirements across its systems.

TAFE NSW provides logged-on access to a range of services for students. Students can:

- view personal details, enrolment details and unit/module results
- view employer details

- change contact details
- request a transcript of results
- view notifications and calendar information such as scheduled TAFE NSW final examinations.

TAFE NSW also supports access by past students to the Student Portal and Student eServices.

The auEduPerson specification

The auEduPerson specification provides a set of recommended attributes to describe users of the Australian Access Federation for Higher Education (AAF)[15]. This specification is the shared data model for describing people (including students and staff) associated with universities participating in the AAF. The auEduPerson attribute recommendations aim "*to establish a common language for the exchange of data between identity and service providers which, if allowed, will increase an individual member's ability to interoperate with other members of the federation*"[16], and allow information to be shared between organisations through a single/simple sign on approach.

The auEduPerson specification is based on the eduPerson specification originating in the USA.

Table 2: auEduPerson Core attributes

Attribute	Definition
auEduPersonSharedToken	A unique identifier
displayName	Preferred name of a person to be used when displaying entries.
eduPersonAffiliation	Specifies the person's relationship(s) to the institution (eg student, staff, etc)
eduPersonEntitlement	URI (either URN or URL) that indicates a set of rights to specific resources
eduPersonScopedAffiliation	Specifies the person's affiliation within a particular security domain
eduPersonTargetedID	A persistent, non-reassigned, privacy-preserving identifier for a user shared between an identity provider and service provider
mail	Email address

If the auEduPerson were adopted by the VET sector, some modifications to this specification would be required, particularly to the controlled vocabularies used to describe the various types of affiliation a person has with the institution. A more fundamental review would be to align auEduPerson elements with the existing data elements required by AVETMISS reporting, and maintain a single source of attributes describing a learner in VET, if this was possible. Further investigation is required to map these two data models.

[15] General information on AAF: http://www.aaf.edu.au For a discussion of the AAF within a VET context: http://e-standards.flexiblelearning.net.au/news.htm#a11
[16] AAF (2008). Attribute recommendations for AAF Participants. Retrieved October 2008 from http://www.aaf.edu.au/documentation.

Recommendation 1: The auEduPerson specification has been created to support scenarios for authentication in a specific environment. The VET sector should identify and describe scenarios for authentication in its environment and then assess the applicability of specifications such as auEduPerson.

Recommendation 2: The MIAP approach in the UK should be further investigated to understand potential benefits for the Australian VET context.

Content – types, classification and ownership

Having considered the likely bodies which could be the e-portfolio service provider, it is necessary to consider the types of content that might be found in an e-portfolio. How can it be classified? Who owns it? How can its authenticity be verified?

Content types

Respondents were asked to consider the types of content they anticipated might form part of an e-portfolio. They were also asked to suggest possible classifications of this content.

Responses about content type typically included:

Personal information

- about oneself
- hobbies, interests
- family information.

Work history

- CVs, resumes
- references
- evidence of work related achievements.

Learning experience

- examples of material produced at a learning institution
- formative assessments
- learning journals.

Evidence of academic achievement

- summative assessments
- qualifications.

Collaborative content

- mentor or employer comments
- group work.

Content classification

Content was classified by:

1. The purpose of the content

This is the classification used in the list above:

- personal information
- work information
- learning experience
- academic achievement.

2. Digital file type

For example:

- media files
- photographs
- video
- flash
- word processing documents
- spreadsheets
- databases
- PowerPoint.

3. Access

This could mean a simple binary classification of ‘private’ versus ‘public’, or more likely, a complex set of access rules which allow different groups to have access to different sets of content. Such a classification is likely to be constantly changing, subject to the varying activities of the e-portfolio owner.

4. Publisher

Content published by the owner of the e-portfolio is of a different class to content that may be contributed by a third party such as a teacher or employer.

5. Ownership

This topic will be discussed in more detail on page 8 of this report, however it is useful to acknowledge that there is a difference between content that the learner directly owns and content that is about the learner but owned by a third party. For example, and institution can hold academic records about a student which the student will not directly own despite, in most cases, having certain rights relating to that data granted under the Privacy Act. Both types of content have a place in a comprehensive e-portfolio.

6. Content that is physically located on the primary e-portfolio site versus content held in a third party external repository which could be cross referenced by the user

Perhaps the most significant example of such external content was the concept of an external, validated qualifications authority which could be referenced by the e-portfolio owner in order to give validation of academic achievement to selected audiences. However, there are numerous other types of external content that might be

cross-referenced, for example, personal web sites, social networking content and so forth.[17]

Some respondents responded differently to the question about content classification by saying that any classification ought to be the responsibility of the learner. Some suggested a 'folksonomy' tagging approach. Others suggested learners might want to assign metadata which could for example classify by industry or employer to enable dynamic grouping of content to meet certain user needs. For example, if the e-portfolio owner wished to present content to a prospective employer in a given industry, such metadata tagging could potentially facilitate ease of filtering content to suit that purpose.

All of these approaches to content classification have validity, however, for the purpose of this paper, multiple approaches are less helpful. Instead, categories 4-6 above appear to offer the most relevance for the focus of this report. A matrix of these three can be developed as illustrated in Table 3 overleaf.

[17] Note this classification has introduced the concept of a distinction between a primary e-portfolio service and external e-portfolio content. (Downes, 2008) argues that the whole of an e-portfolio consists of external content:

"E-portfolios involve distributed content. That is to say content that is located not in one place on the World Wide Web, not in one place on the internet, but rather in multiple locations."

For the purposes of this paper however, it is assumed that in addition to external content, there may be a primary e-portfolio service which is the 'home base'. Following Downes' logic, it may be possible to have a portfolio consisting entirely of external content, but most respondents also assumed the existence of a primary e-portfolio site.

E-portfolio content classification - determining the publisher

Table 3: E-portfolio content classification - determining the publisher

Publisher	Content owner	Location	
		On the primary e-portfolio	**External**
Learner	Learner	For example: • course work • CV • journals • personal details.	For example: • personal website • social networking site content.
	Third party	For example: • references • work done by the learner while under contract to a third party.	For example: • work done for the employer – published on employer's website • depending on the terms and conditions of social networking sites, ownership of content published on some of these could be assigned to the third party.
Third party	Learner	For example: • third party professionally produced content, published on the primary e-portfolio, commissioned by learner.	For example: • third party professionally produced and hosted e-portfolio, commissioned by learner.
	Third party	For example: • formative assessment.	For example: • transcripts of results, qualifications or professional memberships.

An even simpler classification is possible using only the 'owner' and 'location' axis. This classification is helpful for access and security considerations, see Table 4 overleaf.

E-portfolio content classification – determining the owner

Table 4: E-portfolio content classification – determining the owner

Content owner	Location	
	On the primary e-portfolio	**External**
Learner	For example: • personal details • course work • CV • journals • third party professionally produced content, published on the primary e-portfolio, commissioned by learner.	For example: • personal website • social networking site content • third party professionally produced and hosted e-portfolio, commissioned by learner.
Third party	For example: • references • work done by the learner whilst under contract to a third party • formative assessment.	For example: • work done for employer – published on employer's website • transcripts of results.

Ownership

Respondents almost unanimously suggested that the owner of e-portfolio content ought to be the learner (the person who is the subject of the e-portfolio). Behind these responses were sound beliefs about individuals being responsible for their own learning, beliefs about respect and empowerment – particularly for adult learners, and recognition that the point of constancy in an individual's life-long learning journey, is the individual himself or herself.

These views also reflected the importance of giving the learner control over the use of the e-portfolio, including who is given permission to access it and what parts of the content can be viewed by others.

However, control over e-portfolio functionality is not the same thing as ownership of the content, and unfortunately, the attractive proposition of the learner as the owner of all the content does not entirely pass scrutiny. Indeed, many respondents conceded that reality would probably prove different from the preferred position.

Table and Table have already foreshadowed that there are likely to be multiple content owners. Charlesworth and Home, 2004, whilst speaking from a UK law perspective, also confirm that ownership is complex.

Content owned by the learner

As illustrated in these tables, a significant amount of the content published on either the primary e-portfolio site, or externally, will be content owned by the learner. It is recognised that it is important to develop explicit ownership policies, however there is an assumption that content produced by a learner in the course of their studies ought to be the property of that learner.

Indeed, learner-owned content can include not only content created by the learner but also content commissioned by the learner from a third party. Commissioned content

could include professionally produced e-portfolio material. Such commissioned work could become commonplace, much in the same way as professional (paper based) resume services are readily accessible today. Ownership of such professionally produced content would be dependent on the terms under which it is commissioned, however, suffice it to say, that it is feasible for the learner to purchase the copyright.

Note, however, that Australian law makes a distinction between copyright and moral rights. The latter rights are non-transferrable, therefore the third party would retain these rights. Nevertheless, for the purpose of this paper, it is accepted that there can be content produced by the Learner or a third party for which the copyright is owned by the learner. Learners would have the right to freely use such content in the manner contemplated by the survey respondents.

Content owned by third parties

Other types of content exist where the ownership is almost certainly not vested in the learner. Copyright law can be complex and this report is not legal advice. The reader ought not to rely on the opinions expressed without verification from a person properly qualified to express opinions about copyright law. Nevertheless, it is likely that ownership of substantial amounts of material authored by third parties would not reside with the learner.

For example, a reference written for the learner by a third party is unlikely to be owned by the learner. Instead, copyright would be held either by the author of the reference, or, depending on employment conditions, could commonly be owned by the third party's employer. Whilst the learner could reasonably claim to have an implied licence to use the reference, s/he does not have the right to edit the work, nor claim ownership.

There are also times when the learner's own work is not owned by the learner. Respondents pointed to examples of work undertaken by an individual as part of his/her employment. In most cases, copyright in such work would be vested in the employer. Such content may be highly relevant for an e-portfolio and the learner may be well advised to seek licence to publish it there, but permission to publish is not the same thing as ownership.

A licence to publish can be implied or explicit. In either case, the learner would be advised to ascertain the limitations and conditions of the licence and to operate within those boundaries.

In summary

In the broadest terms, e-portfolio content is likely to comprise material that is owned by the learner as well as material that is owned by third parties. It is also possible that moral rights may be held by a third party over material for which the learner holds the intellectual property. In the case of content owned by a third party, the learner needs to take care to ascertain the limitations and conditions of use and to act accordingly.

Copyright law is complex. It is unlikely that detailed expert opinion about ownership of e-portfolio content could be offered without reference to specific content examples and in specific contexts. However generic legal opinion could be sought which could then in turn be considered in the specific circumstances of each e-portfolio service provider.

Implications for e-portfolio service providers

E-portfolio service providers need to take reasonable steps to ensure they are not providing a service which publishes unlicensed material owned by third parties. To that end, appropriate legal advice should be sought. Such advice is likely to include the importance of explicit agreement between the service provider and learner about restricting publishing to material which is appropriately licensed for that purpose.

Further, given that licensed use may be limited to certain individuals and for certain

purposes, it is likely that a fundamental requirement of an e-portfolio service will be to have the capacity to limit access to sets of content to properly identified and authenticated users. Such access controls will be discussed in more detail on page 32.

Lastly, as a custodian of e-portfolio materials, the e-portfolio service provider has a long term obligation. In the ePISTLE project[18], users were most concerned about what would happen to their work once they had moved on from the institution in which it had been created. Service providers need to establish a clear policy on content removal, storage and access to address this issue.

Implications for learners

Learners will need support to understand the distinction between their own materials and materials owned by third parties. Further, the distinction between implied licence for use and explicit licence can be difficult to grasp.

E-portfolio service providers need to provide advice to learners about these matters. It will also be helpful to provide template licence agreements that learners could use in order to formally secure release of third party materials for use within an e-portfolio.

Learners may also need help to understand that even when publishing their own content, there are legal implications to be considered. Charlesworth and Home (2004 and 2006) suggest that many learners will be unaware of the potential liability they, and the institution, may be under with regard to issues such as defamation, breach of copyright, obscenity and indecency when publishing their materials on an e-portfolio. For example, Downes, 2008 cites a case in the United Kingdom where legal action was taken against a university resulting from a student's posting about a fellow student and a teacher.

Institutions should consider providing written guidance to Learners (and to staff) concerning publishing on the web using institutional resources. This could be strengthened by actively teaching about such matters as part of the institution's digital literacy program.

Recommendation 3: Generic legal advice should be sought concerning:

- ***the need for explicit or implied licence before third party materials can be published***
- ***template licence agreements which can be used to secure third party agreement to include content in an e-portfolio***
- ***liabilities associated with defamation, breach of copyright, obscenity and indecency when publishing their materials on an e-portfolio***

Recommendation 4: Template policies should be commissioned, concerning content removal, storage and access to address issues associated with learner transition

Privacy

Preamble

The follow section of this paper examines issues associated with e-portfolios and privacy law. However, it is appropriate at the outset to acknowledge that most organisations have already considered privacy legislation in the context of their current e-learning activities. As such, it is anticipated that e-portfolio activities ought not to create a major set of new responsibilities and liabilities. Instead, in most cases it will be

[18] http://www.jisc.ac.uk/whatwedo/programmes/edistributed/epistle

more a matter of accommodating the e-portfolio within current practice and policy. Nevertheless, for the purpose of this paper, it is prudent to revisit privacy legislation and consider the possible impact on e-portfolio use.

Legislation

The consideration of ownership and copyright introduced complexity to the matters under consideration in this paper. However, the current[19] Australian privacy landscape is more complex again as it is governed by a patchwork of laws. It consists of obligations which contain multiple exceptions. This situation is further clouded by the fact that there is Australian legislation relating to privacy at both a state/territory and Commonwealth level.

These Acts apply to relevant government agencies and to private sector organisations which are performing a service for the Government. The Australian Government Act also applies to private sector organisations which have an annual turnover of more than $3 million.

All of the Acts contain privacy principles which deal primarily with personal information about individuals. However, in the case of the Australian Government Act, there are different principles which apply to the public and private sectors. The principles applicable to the public sector are called the Information Privacy Principles[20]. For the private sector, there are National Privacy Principles[21].

In addition, the legislation also addresses conduct which, while not a breach of a principle, is nevertheless an interference with the privacy of an individual.

The nature of the information under consideration is also a factor in determining if privacy laws apply. For example, the Acts make distinctions between personal information and health information. However, not all of the information likely to be held in an e-portfolio would be of a nature covered by these Acts.Table 5 overleaf provides a simplified summary of the sets of legislation.

[19] A report by the Australian Law Reform Commission released in August 2008 recommends 'that the Privacy Act be redrafted and restructured to achieve significantly greater consistency, clarity and simplicity.'

[20] See Appendix 1

[21] See Appendix 2

Table 5: Australian legislation relating to privacy

Legislation	Applicable to
Commonwealth Privacy Act 1988 with December 2001 Amendments - **National Privacy Principles**	Private sector organisations (including not-for-profits) with an annual turnover of more than $3 million
Commonwealth Privacy Act 1988 with December 2001 Amendments - **Information Privacy Principles**	The Australian and ACT governments and their public sector agencies (including contractors working for these agencies)
Separate state and territory privacy laws. Note that: Victoria and Northern Territory privacy laws contain the same **National Privacy Principles** from the Privacy Act 1988 as per Type 1 above. Queensland's privacy laws contain the same **Information Privacy Principles** from the Privacy Act 1988 as per Type 2 above. Western Australia's privacy laws contain principles which are very comparable but not identical to the **National Privacy Principles**. South Australia and New South Wales privacy principles are not identical with either set of national principles, but comparable to both.	The relevant state and territory governments and their public sector agencies. In addition, most of these Acts give powers for Privacy Commissioners to investigate and conciliat e privacy breaches by organisations and individuals who are not public sector agencies.

Therefore, determining whether legislation applies, and if so, which legislation, requires being clear about the entity concerned as well as the nature of the information under consideration.

We have previously concluded that there are a range of agencies which could conceivably provide e-portfolio services.

Table 6 overleaf postulates probable applicable law (once again with the proviso that this does not constitute legal opinion):

Table 6: Agencies and the possible applicable legislation for e-portfolios

Agency	Possible applicable legislation
The Australian Government (eg DEEWR)	Commonwealth Privacy Act 1988 with December 2001 Amendments - **Information Privacy Principles**
State or territory based public sector agency	Separate state and territory privacy laws (other than the ACT which is covered by the Commonwealth Act)
A private sector, for-profit body	When the annual turnover is greater than $3m: Commonwealth Privacy Act 1988 with December 2001 Amendments - **National Privacy Principles** When acting as a contractor to an Australian Government agency: Commonwealth Privacy Act 1988 with December 2001 Amendments - **Information Privacy Principles** In most cases: Subject to review by State or Territory Privacy Commissioners
A private sector, not-for-profit agency such as a philanthropic body	As per the private sector for-profit body above
A private sector, not-for-profit agency such as a Ministerial company	As per the private sector for-profit body above
An education or training institution	Multiple possibilities exist dependent on the ownership of the institution and its annual financial turnover. Specific legal advice would need to be sought. In the case of TAFE institutes, ownership varies between jurisdictions, with some being State owned and others being incorporated bodies.

This simple table illustrates the complexities in determining applicable privacy laws. Indeed it is possible that agencies could be subject to both state/territory and Commonwealth law.

Nevertheless, whilst there is a maze of privacy legislation, some broad comments can be made.

Passive collection of personal information

Privacy laws address the collection of personal information. The laws are intended to protect the rights of individuals over that information. This is of significance for e-portfolios because:

- Not all the content on an e-portfolio would be likely to be deemed to be ‘personal information’.
- If the learner is the prime publisher on an e-portfolio and the learner has full editing control over that content, obligations regarding an individual’s rights over the information have, at least in part, been met.

However, these circumstances do not abrogate an e-portfolio service provider from all responsibility. Even as a passive collector of individual information (such as when a

learner chooses to publish personal details), the service provider is placed in a custodial position which would imply some privacy law obligations in most cases.

Active collection of personal information

As illustrated previously in Table 6, some e-portfolio content may be published by a third party. Where that third party is also the e-portfolio service provider, privacy laws become increasingly significant. A particular example would be the case of an educational institution hosting an e-portfolio service and publishing assessment material.

Summative assessment

Some content, such as learner summative assessment results, would be particularly sensitive to privacy law consideration. However, it is likely that educational institutions have already received legal advice about the collection and management of this data. The e-portfolio business driver is unlikely to generate new summative assessment data collections with new privacy law implications. However, e-portfolios could lead to new management practices such as making this data available as verified transcripts for authorised users. Such use would need to be subject to legal advice in order to remain compliant with privacy law.

QualSearch

A useful example of innovative use of assessment data and associated privacy law issues is the Australian QualSearch[22] service. QualSearch is a service of the Queensland Tertiary Admissions Centre (QTAC). It provides registered users such as tertiary institutions and recruitment agencies with a qualifications verification service. It does this by requesting information from the institutions holding relevant assessment data and presents this in response to the query.

Clearly there are significant privacy implications in this process. However, the process is made compliant with privacy law by:

- Students signing an agreement at their enrolled institution which permits the assessment data to be released for QualSearch purposes
- QTAC entering legal agreements with institutions and recruitment agencies regarding access to the data.

Access to a verified qualifications service would appear an exceptionally valuable e-portfolio functionality. QTAC's QualSearch is a working example of just such a service which has been developed in a manner consistent with privacy law requirements.

Formative assessments

Formative assessments could in some ways present a greater challenge for e-portfolio service providers than summative assessment data. The privacy law implications for the latter are relatively self-evident. Institutions knowingly collect this data, are aware of its personal and sensitive nature, and largely would treat it in careful compliance with privacy law.

However, formative assessments could easily pass under an institution's radar. Teacher grading and assessment comments represent a long-standing practice in education and training. Comments which once would have been written at the end of the learner's paper or on physical project work, could potentially be published electronically in a learner's e-portfolio. Indeed, many respondents commented that this is an important function of an e-portfolio. However, this material is in fact sensitive, personal information and e-portfolio service providers will need to take active steps to

[22] http://www.qualsearch.com.au/

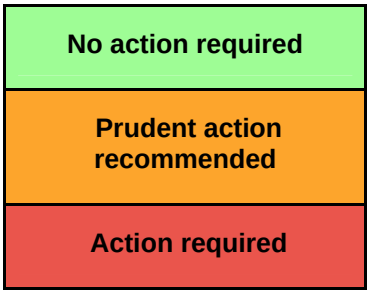
comply with privacy law. In cases where the e-portfolio service provider is the employer of the teacher, the private formative assessment information collection could be seen as an active collection and one where the obligations are greater than just ‘custodial’.

Compliance with privacy laws

Given the complex matrix of applicable privacy laws, content types and host agencies, it is not feasible in this document to analyse every variation. Each e-portfolio service providing agency should seek legal advice to determine the applicable privacy law and to address its obligations under those laws.

However, whilst there are differences in privacy laws, there are also significant similarities. Table 7 overleaf considers one scenario where an agency acts as an e-portfolio service provider and collects data either actively or passively as considered briefly above. In this scenario it is assumed that National Privacy Principles (or state/territory ‘mirror’ laws) apply[23]. The scenario does not consider externally hosted material, however in cases where an agency considers exporting data to such an external agency, advice would need to be sought regarding privacy implications.

In order to visually demonstrate implications, the analysis has been colour-coded according to the following legend:



Once again, the proviso must be given that the following does not represent legal advice.

[23] See Appendix

Table 7 – Scenario One: Consideration of privacy law implications by e-portfolio service providers governed by the National Privacy Principles

National Privacy Principles	Active collection		Passive collection	
	Material already collected and stored by the institution – eg qualifications	New types of publishing by the agency - eg formative assessment	Publishing by the learner	Publishing by a third party - not the host agency
2. Collection	E-portfolio use is unlikely to lead to the active collection of additional data sets by institutions.	The agency needs to seek advice as to whether or not this material is 'personal information'. If it is, the agency must ensure the learner is aware of the publishing of material as per the National Privacy Principles.	This principle addresses the responsibility of agencies actively involved in collecting data. The act of holding data submitted by the learner at the learner's volition, would not appear to be applicable to this privacy principle.	The agency providing the e-portfolio service has a custodial duty, despite not being the publisher. It would be prudent therefore to ensure that the contribution of materials by a third party is explicitly approved by the learner.
3. Use and disclosure	If it is proposed to make new use of existing data collections for the purpose of the e-portfolio function, it would be prudent to seek the individual's consent. However, if it could be deemed that the secondary purpose of making the data available for the e-portfolio is closely related to the primary purpose of the collection, and that the individual would expect it made available in this way, no consent may be needed.	Even if the data were deemed to be 'personal information', the primary purpose of the collection would be to provide the learner with access to that material. Assuming that the learner controls who else gains access to the data, this appears consistent with this privacy principle.	Publishing e-portfolio material by the learner appears entirely consistent with the intent of this principle, especially if the learner is in control over who is given access.	If third-party materials are published at the explicit request of the learner, and the learner controls the use and disclosure of that data, this appears consistent with this principle.

4. Data quality	The use of existing materials for the purpose of an e-portfolio would not impact on data quality.	Assuming this material is deemed to be 'personal information' there is an obligation on the agency to ensure it is accurate, complete and up-to-date.	An organisation must take reasonable steps to ensure that the personal information it collects, uses or discloses is accurate, complete and up-to-date. Given that this personal information about the learner will have been contributed by the learner, it is likely that this would be construed to be 'taking reasonable steps'.	Reasonable steps in this case would appear to include: limiting publishing to those third parties explicitly nominated by the learner, and providing advice to the learner about limiting third-party access to those who could reasonably be relied upon to contribute accurate and well informed data.
5. Data security	If an agency agrees to make available existing data for e-portfolio purposes, it will need to take reasonable steps to ensure that in the process of doing so, it does not increase the vulnerability of that data through any form of unauthorised access.	The agency is obligated to take reasonable steps to prevent unauthorised access to this material.	The agency is obligated to take reasonable steps to prevent unauthorised access to this material.	The agency is obligated to take reasonable steps to prevent unauthorised access to this material.
6. Openness	Whilst no new obligations are placed on an agency, if new forms of access are proposed for e-portfolio purposes, it would be good practice to make its data management policies accessible from any new gateway.	Data management policies would need to be developed and published with regard to e-portfolio materials.	Data management policies would need to be developed and published with regard to e-portfolio materials, including materials contributed by the learner.	Data management policies would need to be developed and published with regard to e-portfolio materials, including materials contributed by third parties with approval of the learner.

7. Access and correction	The proposal to provide access to this data improves the agencies' compliance with this principle. No further action required.	It will be necessary for the learner to be given full visibility of any third party published material. The learner would also need to be able to request corrections to errors of fact.	In the case of material being published by the learner, there would be full compliance with the requirements of this principle, assuming that the learner is later able to make further edits.	In addition to directly approving any third party publishing, it will be necessary for the learner to be given full visibility of any third party published material. The learner would also need to be able to either directly correct, or be able to request corrections to errors of fact.
8. Identifiers	Not applicable. No new identifier is anticipated to be required.	Any identifier used for the purpose of managing the e-portfolio will need to comply with this principle which prohibits the use of personal identifiers used by other government agencies.	Any identifier used for the purpose of managing the e-portfolio will need to comply with this principle which prohibits the use of personal identifiers used by other government agencies.	Any identifier used for the purpose of managing the e-portfolio will need to comply with this principle which prohibits the use of personal identifiers used by other government agencies.
9. Anonymity	Not applicable. The E-portfolio business activity does not propose any transactions by the learner with a regard to this data.	Not applicable.	It would appear unlikely that the act of publishing information on an e-portfolio could be interpreted as entering a transaction with an organisation.	Not applicable.
10. Trans-border data flows	To comply with this principle, it would be prudent for an agency to limit data access to read only and not offer data export of agency collected material.	The E-portfolio business activity may require portability of published materials. Given that external data transfer is permissible with the individual's consent, access controls will need to limit export rights to the learner concerned.	The E-portfolio business activity may require portability of published materials. Given that external data transfer is permissible with the individual's consent, access controls will need to limit export rights to the learner concerned.	The E-portfolio business activity may require portability of published materials. Given that external data transfer is permissible with the individual's consent, access controls will need to limit export rights to the learner concerned.

11. Sensitive information	Whilst some current agency collections, such as achievement data, would be sensitive information, given that no to the new data collection is contemplated, this principle is not applicable in this case.	Assuming that the data is deemed 'personal information' the learner is required to give consent to content being contributed to the e-portfolio. An e-portfolio system should have the capacity to bar publishing until such time as consent is given.	The collection of sensitive information is permissible under this principle with the consent of the individual concerned. Material published by the learner clearly has the learner's consent.	The learner is required to give consent to content being contributed to the e-portfolio by a third party. Assuming the learner has control over all external third-party publishing, consent could be assumed. However, it would be prudent for an agency to include consent to such publishing in its use agreement with the learner.

General principles for privacy law compliance

An e-portfolio service has the potential to introduce new ways of handling information by an institution. In order to ensure compliance with privacy laws, an institution which either provides an e-portfolio service, or passes data to an e-portfolio service provider, needs to be clear about:

- the nature and scope of its data processing
- the flows of data that occur
- administrative and technical responsibilities and
- the legal implications of all data flows.

Almost certainly, this will mean e-portfolio service providers will need to enter formal agreements with both learners and any relevant third parties.

Further, because there will inevitably be future changes to administrative or technical process, policy needs to be establish that will ensure that a re-evaluation of data privacy considerations and the supporting legal fabric will form part of any procedural change.

Liabilities

Finally, it is useful to consider the potential liabilities which could flow from a breach of privacy law. Once again, this is made complex by the maze of Australian privacy laws and jurisdictions. However, taking the Commonwealth Act as guide, whilst there are no criminal penalties, the Commissioner is empowered to make a declaration which includes:

- Requiring the respondent to 'perform any reasonable act or course of conduct to redress any loss or damage suffered by the complainant'[24]
- The awarding of compensation.

Such declarations will take into account, 'injury to the complainant's feelings or humiliation suffered'[25]

There is no specified limitation of liability under the Commonwealth Act.

Moving forward

As we have seen, e-portfolio service providers are exposed to legal risks associated with the collection and use of personal information, irrespective of whether or not this collection is active or passive. Specific legal advice is needed in each case, however, once again, the immediate issue is the model of e-portfolio service provision as discussed on page 6.

If there is to be more than one e-portfolio service provider, there would be value in seeking generic legal advice which would be applicable in all cases in order to avoid the duplication of such work. This could be extended to the development of template agreements between the service provider and learners.

Individual e-portfolio service providers would then need to build on this advice in seeking further opinion about their specific circumstances.

Specialist privacy law agencies exist in Australia and it may be appropriate to request a privacy impact assessment from one of these. Once again, there may be wisdom in seeking an opinion on behalf of the whole education sector, through AICTEC.

---

[24] Privacy Act 1988 – Sect. 52
[25] Op. cit.

Recommendation 5: A suitably qualified legal officer/agency should be engaged to provide a privacy impact assessment with regard to e-portfolio services and develop generic agreement templates between e-portfolio service providers and learners. Alternatively a whole of education and training approach could be sought through AICTEC.

Verification

If e-portfolio content is to be relied upon for substantial purposes - such as assessment, recognition of prior learning, or employment application - verification of the authenticity of the material is important. Once again however, it is useful to make a distinction about different types of content. In this case, it is perhaps most useful to consider the classification of content by publisher.

Learner published content

Respondents commonly expressed the opinion that they did not expect the e-portfolio to solve the problem of verification of learner published content. Respondents said that the issue is no different to the verification challenge faced by teachers and employers prior to the 'invention' of e-portfolios. It has always been the case that when teachers have been presented with student work, judgement has been required as to its authenticity. Similarly, when employers receive job applications which make certain assertions about skills and experiences, the employer has needed to ascertain the accuracy of those claims. If the application contained references or testimonials, the employer has always needed to consider the authenticity of these documents.

Respondents suggested that the solution to this problem has always been professional judgement and separate verification processes. For example, checks can be made with employers about prior learning claims, or with the author of a testimonial.

Effective job applications provide guidance as to how assertions can be verified, giving contact details of referees. Respondents suggested that learners using e-portfolios need to adopt the same approaches. One said that expecting an e-portfolio to resolve this issue was a 'furphy'.

However some respondents suggested that learners submitting material ought to formally agree that they are the owner of the material or have a license to use it. Such agreement could be made generically when agreeing at the outset to the terms and conditions of e-portfolio use, although more regular acknowledgement may be appropriate in some contexts. Further, authorship of third party content ought to be clearly acknowledged in every instance.

Verification with technology

Whilst teacher judgement is unlikely ever to be made redundant, technology can also offer some assistance with verification.

One respondent spoke of the use of technology to provide evidence of competencies. He described experiments with the use of mobile phones and also with video cameras built into optical glasses as means of recording competency. The use of such novel approaches would appear to present a natural synergy with the concept of the e-portfolio. The multi-media potential of the electronic portfolio does offer opportunities for verification that may not have been feasible with more traditional portfolios.

Such recording of work in progress is less likely to be an option when it comes to written work however. Detection of plagiarism represents a particular challenge for

verification of a student's work. The concern is sufficiently serious for the UK Joint Information Systems Committee (JISC[26]) to form a JISC Plagiarism Advisory Service. This service conducted a review of the top eleven plagiarism detection solutions available in the UK. Such electronic tools could be helpful to highlight potential risks in e-portfolios.

Training organisations which support the use of e-portfolios may well wish to consider the provision of plagiarism detection tools as a strategy to support teachers in the verification of student work submitted electronically, including via an e-portfolio.

Endorsement

Another view was that social networking sites achieve a weight of credibility for an individual through the endorsement of colleagues and friends. For example, 'Linkedin' allows the establishment of professional networks. Reputable associations made on that site work to give some validity to an individual's claims. Depending on how an e-portfolio is structured, there may be the option of similar social networks on either the primary e-portfolio site, or alternatively the external e-portfolio content could include a reputable social networking service which could give at least some validity to a learner's claims.

Endorsement was not seen to be of the same order as 'verification', rather, it was a middle ground option that could add some weight to validity.

Third party content

Qualification data

Whilst it may be reasonable to expect parties relying on learner published content to take judicious steps to verify authenticity, there would appear to be a different order of expectation with regard to third party published material. This was particularly the view held by respondents with regard to an institution's summative assessment/ qualifications data where there was support for there being some means of verifying such content.

It is interesting to note the position adopted by the Australian Higher Education National Diploma Supplement project, which has investigated producing a standardised qualifications document for all Australian universities. That project took the view that the authenticity of electronic documents is more problematic than paper ones:

> *"The Graduation Statement will be issued in hard copy and, when feasible, also in electronic format in order to maximise the utility to graduates. …Recognising the lower security levels of electronic documents, the hard-copy format should be treated as the primary document." (Proposal for an Australian Higher Education Graduation Statement, 2008)*

The report also assumes the need for 'out of band' verification processes:

> *"Institutions will be responsible for providing a verification mechanism for stakeholders who seek to verify the authenticity of a Graduation Statement.'*

However, Recommendation 6 of the report suggests a mechanism for working towards an electronic qualifications verification service.

> *"Discussions should be held with QualSearch about the possibility of it gaining a full national coverage of universities and adding functionalities to provide access to copies of Australian Higher Education Graduation Statement information by graduates, universities, employers and other stakeholders."*

[26] http://jisc.ac.uk

QualSearch – a cross-sectoral approach?

Of particular relevance is the final recommendation:

> *"… while the terms of reference did not include reference to vocational and training awards, consideration should be given to whether a single model might serve both higher education and VET awards."*

There appear to be good reasons for giving serious consideration to a joint qualifications model as per this recommendation. The increasing blurring of the demarcation between VET and higher education make a single qualification statement appealing. From the perspective of parties which may rely on such statements, particularly employers, recruitment firms and enrolling institutions, a standardised approach seems particularly useful.

If such an approach were to be adopted, this, coupled with the Recommendation 6 of that report introduces the concept of a single, integrated verified electronic qualification service.

The earlier discussion on page 22 about QualSearch described its well developed legal framework for handling private information. QualSearch is already well established not only for the Australian Higher Education Community, but also for numerous TAFE institutes, particularly on the eastern coast. It is well placed to expand to provide a qualifications verification service for TAFE institutes across the whole of the sector, and quite probably, do so in a manner integrated with the approach taken by the higher education community.

Such a service would be a major platform for the external e-portfolio content contemplated in this paper. However, it is not without limitations. For example, the qualification data is held in institutional repositories which are interrogated by QualSearch in response to a query from a licensed user of the service. The results to such a query are not instantaneous, generally taking around 24 hours. Further, licensed users are limited. At present they represent enrolling institutions and some major recruitment firms. It is understood however that there are plans to expand its licensed user base to include other bodies such as industry associations.

These 'limitations' can also be seen as QualSearch's strengths. By only harvesting data on demand, the results served by QualSearch represent the most up to date data set drawn live from the authoritative sources. Further, there is a manual checking step by QualSearch staff before results are released, which may result in a brief delay but is very significant in terms of quality assurance. The obvious benefits in these processes could outweigh the 24 hour lag.

Secondly, the restriction on the user group is valuable in ensuring only appropriately licensed users get access to this personal information.

Given the quality of QualSearch's processes, its established position and growth prospects, and its recognition in the AHEGS Report, it would appear to be worthy of serious consideration as an endorsed accredited qualifications verifications provider.

Verification of all qualifications

QualSearch appears capable of providing a qualifications verification service for accredited qualification data stored in either TAFE institute or jurisdictional student management systems. What is less clear is QualSearch's capacity to verify qualifications in cases where the data is not held in either of those sources, such as non-accredited qualifications. In these cases, the lack of substantial repositories of this data would pose a serious difficulty to the QualSearch model.

Secondly, QualSearch appears unlikely to be able to deliver lighter-weight qualifications such as skills and achievements.

Alternative models have been developed in the United Kingdom which appears to

address these issues.

Purple Passport

Purple Passport[27] provides an online qualification verification service through the establishment of a national network of accredited verifiers.

An individual's passport is set up by an employer, training provider, recruitment agency, or by the individual, with the individual's identity confirmed by one of the verifiers. The role of the verifier is to sight substantive evidence, such as original documentation.

The passport web page contains a 'skill profile' to record skills, qualifications and achievements. For each record, the verifier is named, although there is an option to record 'unverified' skills. The passport offers the option of filtering by industry sector.

This appears to be an excellent third party product which would be of significant benefit, particularly in the context of e-portfolios. It does however require a network of verifiers to be established. A judgement needs to be made about the cost-benefit of such a service, however the model is a serious contender as a lighter weight verification service, available for all, able to record more than just formal qualifications, with no lag time in viewing qualifications, and not limited to a narrow licensed user base.

Digitary

The European Bologna Process[28] has been the genesis for new data exchange standards between European Higher Education Institutions.

Digitary[29] is an Irish company, closely involved in these standards activities. Digitary specialises in secure document production and authentication. Its activities include the 'issuing, storing, distributing and authenticating (of) official electronic documents online.

Digitary supports institutions to use 'advanced electronic signatures' for issuing documents that are both legally-valid and tamper-evident. It also provides a mechanism for allowing users to set access controls to allow chosen audiences to view the documents.

These authenticated documents could be used for a full range of qualification certification, ranging from formal graduation certificates through to skills verification statements, or even references. However, Digitary's current model appears to be institution based, with the institution both issuing and hosting the documentation. Such an approach is less likely to be appropriate for the many small private RTOs within the VET sector. Nevertheless, the potential exists to develop a national service to support such agencies.

Whether the Digitary approach could be scaled to accommodate the authentication of non-institution based documentation would need further investigation, however it is likely that any solution for small RTOs could also be used for employers and other groups.

It is understood that early contact has been made between Digitary and the Australian Higher Education National Diploma Supplement activity. This development suggests a watching brief for the VET sector. If the higher education community adopted the Digitary model, rather than QualSearch, this would be very significant for the VET sector's decision making.

---

[27] http://www.purplepassport.com/
[28] http://ec.europa.eu/education/policies/educ/bologna/bologna_en.html
[29] http://www.digitary.net/

Other third party content

Respondents felt that the verification of less formal types of third party material appears to be comparable with the verification of learner content. Given that its nature is likely to be disparate, a comprehensive formal verification model appears unlikely. Comments from respondents about the need for those relying on the data to form judicious opinions and to independently check veracity, also apply to this data type.

Such checking would be aided by the third party content including contact details, for example, to verify references and testimonials. The inclusion of such an 'audit trail' could form part of the good practice guidelines for e-portfolio use.

Recommendation 6: The suitability of the QualSearch, Purple Passport and Digitary approaches should be examined as possible models for the verification of electronic records of qualification within the VET sector. This review should take into account the activities of the Australian Higher Education National Diploma Supplement project

Access control including identification and authentication

A fundamental functionality requirement for an e-portfolio is the capacity to give access to authorised individuals and to prevent access by unauthorised people. Authorised individuals could include:

- the learners themselves
- the learner's peers and/or family
- teachers and educational administrators
- employers or potential employers
- recruitment agencies
- Job Network providers
- anyone else the learner chooses.

The immediate challenge is to have a mechanism to:

1. Initially identify these individuals.
2. Authenticate them as being that same known individual at each visit.
3. Control their access to those parts of the site that the learner, or in some cases the institution, may determine.

This challenge was commonly understood by the respondents who suggested that the learner should have primary decision making rights about who can access their e-portfolio. They also suggested that the learner needs to have control over which parts of the e-portfolio are made visible to those given access. However, respondents also acknowledged that in some circumstances, institutional staff will need access to at least parts of the e-portfolio for assessment purposes; it may not be feasible for such access to be controlled by the learner.

These requirements for identification, authentication and access control need further consideration.

Identification

A brief history

User identification represents a particularly challenge in an online world. In 1993, *The New Yorker* published what is now a famous cartoon by Peter Steiner, showing a dog sitting at a computer, saying to another dog, 'On the Internet, nobody knows you are a dog!' This humorous observation has come to symbolise the problem of identity management in an online world.

The problem is no longer regarded as a laughing matter. With the growing use of the internet for virtually all of life's transactions - commerce, banking, registration, government services, etc – the need to properly identify individuals in a virtual world has become critical. Couple this with the now almost routine attempts at identity theft on the Internet, and the situation represents a major threat to the Internet industry. As such, major companies in the industry are giving the problem sharp focus.

Nevertheless, there is not yet any widespread identity meta-system. An initial attempt by Microsoft to provide such a solution was treated with suspicion or hostility. Microsoft's Passport service was opposed by industry peers because of its potential to allow Microsoft too dominant a position in the identity landscape. It was also opposed by various privacy commissioners who regarded the aggregation of individual identity data in this way to represent a serious threat to individual liberties.

The Microsoft Passport experiment did however stimulate the formation of the Liberty Alliance, composed of multiple industries seeking to nullify this threat by developing standards for identity management and 'circles of trust'. Unquestionably, the Liberty Alliance standards will be an important plank in the identity management platform of the future.

Indeed, as this report was being drafted, Liberty Alliance announced the formation of the 'HR-Education Special Interest Group' which aims to 'increase data portability in Education and HR sectors especially for Employability and Life Long Learning purposes' by producing Liberty Identity Services Interface Specifications (ID-SIS) for this sector.[30]

Identity management in Australian education and training

However, as is implied by the need to form this new Liberty Alliance Special Interest Group, there is still much work to be done to resolve identity management for education and training.

In Australia, the AICTEC Learner Identity Management Framework Project, Framework report (v3.0), 2006 suggests:

> *"In general, the existing Learner information and identity management environments and systems across all sectors of Education are ill-suited to: …- providing Learner … empowerment across all stages of education – eg through the deployment of …. e-portfolio facilities…".*[31]

Whilst acknowledging the privacy risks associated with identity management, the report recommends a framework which should include 'identity resolution', 'policy enforcement' (including user authentication), and a 'trust scheme'.

AICTEC received this report in 2006 and further work has been commissioned in 2008. However, it is still the case that learner identity management remains fragmented.

---

[30] http://wiki.projectliberty.org/index.php/HR-EDU_SIG

[31] Framework Report – v3.0 – Page 7

From a VET sector perspective, the episodic nature of learner engagement and the life-long learning perspective embraced by the sector present particular challenges for identity management, but a challenge that remains crucial for effective e-portfolio use.

Beyond education and training

From an e-portfolio perspective, the challenge of identity management for education and training represents only one part of the problem space. As previously acknowledged, e-portfolios need to be able permit access to identified individuals from most walks of life. In fact, the flexibility envisioned by respondents suggests there can be no limits placed on the categories of individuals to whom a learner may wish to provide e-portfolio access.

Moving forward

Having acknowledged that identification represents a serious challenge for e-portfolio use, there are a number of positive initiatives and opportunities that can be considered:

1. The recent positive move by Liberty Alliance to look at identity management standards from a life long learning perspective.
2. The current AICTEC engagement with the issue for Australian education and training, particularly in the context of the Australian Government's commitment to a digital education revolution.
3. The generally widespread quality of identity management by at least the larger training institutions, for staff and in most cases, for enrolled learners.
4. The potential to leverage from the identity management of other target groups such as industry association members, job network and recruitment agencies.
5. The fact that learners are most likely to want to give access to their e-portfolios to individuals already known to them.

The first two points above give grounds for optimism. The last three points provide a base for moving ahead with both networks of trusted users and more flexible approaches. These points are considered later in this report.

Authentication

Authentication refers to the confirmation that an individual seeking access to an e-portfolio is in fact a previously identified person. Typically, authentication systems rely on one of three things: what the individual knows (eg a password), what the individual has (eg a smart card), or what the individual is (eg iris scan read by some form of a biometric reader).

Authentication can either occur at the entry to the service in question – for example at the e-portfolio access point, or, in cases where the e-portfolio service orovider enters a trust relationship with an identity provider, it can occur at log on to the identity provider. The latter model describes a trust relationship. Such arrangements are variously referred to as circles of trust, trust federations, trust networks, or access federations.

Authentication of whom and to what

When considering authentication options, it is necessary to consider both the type of user likely to be seeking access and the location of the e-portfolio content. Table 8 overleaf summarises these variables and suggests likely options for authentication.

Table 8: Likely options for authentication

Type of identification	Primary e-portfolio	Restricted external e-portfolio content		Public external e-portfolio content
		Learner owned eg social networking site	Third party owned eg QualSearch	
Individual with identity managed by a trusted identity provider, eg the learner or teaching staff at an institution	Trust federation – subject to individual's attributes meeting access policy	Trust federation – subject to individual's attributes meeting site access policy	Trust federation or password controlled – either option subject to separate agreements between the learner, institution, third party (QualSearch) and individual seeking access	Authentication not required
Individual known to learner	Learner provides a password or URL or accepts an identifier provided by the individual such as an OpenID	Learner provides a password or URL or accepts an identifier provided by the individual such as an OpenID	Password controlled – subject to separate agreements between the learner, institution, third party (QualSearch) and individual seeking access	Authentication not required
Individual unknown to learner	No access unless learner chooses to give public access to some sections	No access	No access	Authentication not required

In summary, likely options for authentication fall in to three categories:

- Trust network
- Password or URL provided by the learner or by a third party
- OpenID accepted by the learner.

Each option deserves further comment.

Trust networks

Trust networks are also known as trust federations, access federations or circles of trust. Whatever the name, a trust network removes the burden of user identification and authentication from the service provider through the service provider being able to trust the identity provider to handle these functions. Once implemented, they can be an efficient means of giving users single sign-on access to a wide range of services.

A trust federation requires trustworthy identity providers. The federations usually operate through generic identity assertions being passed between the identity provider and the service provider. For example, it is likely that the assertion may include the individual's role and affiliation, such as 'teacher at X institution'. It is less common for a trust federation to identify an individual's name.

A trust federation can be useful for generic e-portfolio roles, such as a teacher at an institution needing to access a learner's e-portfolio in order to assess project work. In this case, the local institution can manage the identity and e-portfolio service provider can give access to generic classes of users (such as teacher) based on a trust relationship established with the institution.

On the other hand, such a trust federation is less likely to be effective in handling more flexible and granular demands, such as giving access to users whose identity is not managed by a major institution, or allowing the learner to control access at the granularity of a specific individual.

Australian Access Federation

In 2005, the Australian Government commissioned the development of an Australian trust federation for the higher education research community. Named the Australian Access Federation (AAF), it is modelled on similar academic networks being developed internationally.

Anticipated to be launched in 2009, the AAF will utilise two technologies – PKI and Shibboleth. Both provide robust and secure trust services. The Shibboleth functionalities are enhanced by the development of a suite of software packages to assist the identity and service providers – see Appendix 4.

The AAF will define levels of assurance (using a matrix of identity and authentication standards) and a user data schema (auEduPerson – see page 12). These definitions, the federation policies and agreements and the software developments, all offer potential benefits for the VET sector.

On the other hand, the robustness of this solution comes at a price in terms of complexity to implement. JISC infoNet reports that, 'Initial implementations have raised a number of concerns such as the level of technical knowledge required and the technical infrastructure to support Shibboleth.'[32]

However, once correctly implemented, it is a secure and reliable solution. Perhaps a greater concern is the limitations on its use outside of formal training. Brant, 2006

[32] http://www.jiscinfonet.ac.uk/infokits/e-portfolios/access

notes that, ‘Shibboleth is a solution for individual access while registered with the institution where the e-portfolio is held; once an individual has left the institution, the scenario alters.’

The VET sector will need to consider if the rigidity of a trust federation is able to accommodate the flexible learning requirements of the sector.

Password or URL

Respondents did not believe complex authentication systems were required for most e-portfolio content. A quite common view was that a learner emailing a URL to give access to chosen content would be quite sufficient for most purposes. A refinement would be the option of the learner setting a password and emailing both the URL and password to selected individuals.

Whilst not particularly secure, respondents saw a simple solution such as this to be suitable for the business need. It certainly provides a simple solution and is perhaps sufficient for access to relatively non-sensitive information.

Third party qualification verification services, such as QualSearch, will require more active password control management (including a lost password service) and a more rigorous limitation of access to only licensed users. Nevertheless, passwords are currently used by that service and this solution appears fit for purpose.

Inevitably, however, passwords present problems for both the service provider and the individual seeking access to the service. For the service provider, there is the challenge of initially identifying each user and then the need to accept responsibility of the provision of passwords, including the need to respond to lost password queries. For the individual using the service, there is the challenge of remembering multiple passwords for accessing multiple services.

OpenID

User centric identity framework solutions are emerging to address these shortcomings with password approaches. They can offer trust federation style single sign-on functionalities even in cases where there is no identity provider actively managing user identification.

OpenID has received rapid adoption as a means of providing a single sign on in the rapidly growing world of web 2.0 technologies where users create their own identities on multiple social networking sites.

The OpenID authentication protocol was published in early 2005 and has become rapidly successful. OpenID gained further support when in 2007 major companies announced their support and later formed an OpenID Foundation. At the time of writing this paper, there are over 25,000 websites accepting OpenID login compared to approximately 500 in 2006. With hundreds of millions of OpenID users, it appears exceptionally well established.

OpenID identities can be self asserted and stored on an OpenID identity service. For the user, this offers a simple single login solution. Such functionality could relatively easily be made available on an e-portfolio service if the service provider gave learners the functionality of permitting access to selected OpenIDs. For example, a learner could give a prospective employer access to his/her e-portfolio, by setting permissions to accept the OpenID identifier for that employer. In this case, the learner accepts responsibility for identifying the employer and ascertaining their OpenID. The learner then approves access to the e-portfolio based on the authentication provided by that OpenID.

OpenID as a trust network

Whilst OpenID can provide a simple and mutually convenient means of managing authentication of users known to a learner, it could also offer more sophisticated trust network benefits if required. For example, a learner may wish to give access to a class of users, some of whom are unknown individuals. An example might be the case of a learner wanting to allow all recruitment agencies to have access to their e-portfolio.

In this case, if the recruitment industry was prepared to establish an industry specific OpenID identity service, open only to recruitment agencies, it would be possible for all identities from that service to be white-listed for access at the learner's request. A similar model already exists with Microsoft's HealthVault[33] service where only Verisign or TrustBearer OpenID accounts are accepted. While that decision appears to have been based on security considerations, the approach could also be considered in order to achieve other business requirements.

Similarly, a national identity service could be provided for learners, with OpenID an obvious candidate technology. Respondents commonly recognised the challenge of e-portfolio access in a life long learning context. If the e-portfolio service were to be limited to those who either are, or once were, learners, there needs to be some identity service which transcends current institutional enrolment. A national service with business rules that limited identities to such individuals could offer a solution to that challenge.

Such a national service could be provided as a peer service for any national e-portfolio service provision. Even without a national e-portfolio service provider, a national VET OpenID identity service could resolve the problem of the identification and authentication of learners in order to gain access to the learner's e-portfolio service irrespective of changing e-portfolio service providers.

Such a national service would need to investigate privacy concerns and it is anticipated that learners would need to have the right to opt out, or the ability to delete their identity record at any time. There would also need to be strict security enforced to prevent unauthorised access to such data.

Information cards

Whilst Table 1 made no reference to information cards[34], it is important to acknowledge the potential future significance of this approach. If OpenID is the 'hare' of user centric identity frameworks, information cards may prove to be the 'tortoise' that wins the race.

The formation of the Information Card Foundation[35] in July 2008, with strong industry representation, suggests that this too will be a force in the future. Information cards represent an effective way for an individual to manage his/her digital identity. It can integrate with other approaches such as Shibboleth or OpenID. It can also handle a full range of user identification approaches from self asserted identities through to the most highly verified identity service provision. It is more secure than OpenID because OpenID and all other single sign-on solutions are at high risk of serious identity threat by 'phishing'. Perhaps most significantly, it resolves the point of identity aggregation to the user's desk, thereby avoiding the privacy concerns associated with external aggregation.

Microsoft made an early release of information card compatibility by bundling

[33] http://www.healthvault.com/
[34] http://informationcard.net/
[35] http://informationcard.net/members

Windows CardSpace[36] in Vista in 2007. Whilst not yet widely implemented by other operating systems and, consequently neither by service providers, information cards could well emerge as the universal 'identity meta-system' that will provide the authentication architecture for the e-portfolios of the future.

National e-Authentication Framework

A discussion about authentication would not be complete without acknowledging the current work of the national Online and Communications Council and the work it has commissioned to develop a National e-Authentication Framework[37]. This framework will, among other things, provide a common language to describe assurance levels for user identification and authentication. Trust networks require such a language to be shared between identity providers and relying parties. This, and comparable levels of assurance work undertaken by the AAF, need consideration if any form of trust federation were to be used for e-portfolio services.

Next steps

In order to consider the appropriate response to the opportunities presented through trust federations, the VET sector needs to consider various applicable use cases and then, assuming that the use cases are seen to be compelling, to evaluate the various options for moving forward.

At the same time, the sector needs to maintain a watching brief on both the higher education AAF and any developments with a trust federation for schools funded under the current Digital Education Revolution policy.

Access control

Respondents were quite unanimous in their belief that the learner should have control over the parts of the primary e-portfolio that should be accessible to invited individuals. This means that, in addition to the need to identify and then authenticate guests, there needs to be access controls to govern their ability to view and contribute to various parts of the primary e-portfolio site.

This requirement suggests the need for administration tools to be available to the learner within the primary e-portfolio service. These tools need to enable the learner to have granular control to provide different permissions for different guests and to have full flexibility to display or hide various parts of the e-portfolio.

Some respondents also acknowledged that there are situations in which institutions or e-portfolio service providers also need an administrative right of access. For example, access may be necessary to remove offensive material. However, the need to exercise such rights can be minimised by reminder strategies such as offensive material notification links appearing on all pages.

Access controls can also be provided in some instances for learners to determine access to external e-portfolio content as demonstrated by Digitary in the UK.

Recommendation 7: Development of trust federation use cases for the VET sector to identify possible business drivers for a trust federation in VET. This activity needs to be informed also by the parallel activities in the other education sectors.

---

[36] http://windowshelp.microsoft.com/windows/en-us/help/7dc9c520-9d16-473d-b21b-413ac7226fb61033.mspx

[37] http://www.finance.gov.au/e-government/security-and-authentication/authentication.html

Recommendation 8: There should be consideration of the option of providing a central OpenID identity service with business rules that limit its population to current or previously enrolled Learners within the VET sector.

Supporting e-portfolio service providers

Due to the generic nature of the information which e-portfolio service providers need to provide to learners via their e-portfolios, it is considered pertinent that sector wide resources are developed and shared.

Recommendation 9: A VET learner information management framework should be produced, which provides guidance for e-portfolio service providers about:

- ***seeking further legal advice to confirm the appropriateness of the generic advice in its specific circumstances***
- ***providing learners with administrative access controls that control guest access to identified sets of content***
- ***seeking further legal advice about privacy laws applicable for their specific circumstances with regard to both active and passive data collection***
- ***requiring learners to formally declare that content they publish is either their own (or is appropriately licensed and labelled third party content) either as part of the publishing routine or when agreeing at the outset to the terms and conditions of e-portfolio use***
- ***recommending that, whenever possible to do so, learners provide contact details whereby material attributed to third parties (such as references and testimonials) can be verified***
- ***providing learners with the means of authenticating users through password or OpenID.***

Glossary

E-portfolio	'A purposeful collection of information and digital artefacts that demonstrates development or evidences learning outcomes, skills or competencies.'[38]
E-portfolio content	Content published either on the primary e-portfolio or as external e-portfolio content**.**
External e-portfolio content	Content hosted externally to the primary e-portfolio but linked (cross-referenced) to it.
E-portfolio service provider	The agency providing the primary e-portfolio service.
Learner	The person who is the subject of the e-portfolio.
Owner	The person (or entity) owning the intellectual property in material published on the e-portfolio.

[38] Cotterill SJ. What is an ePortfolio? ePortfolios 2007, Maastricht http://www.eportfolios.ac.uk/definition

Primary e-portfolio	The home location for the e-portfolio.
Publisher	The person who uploads the e-portfolio content to the server.
Respondents	People surveyed as part of this research exercise.
Third party	Any person or entity other than the learner.
Third party content	E-portfolio content owned by anyone other than the learner.
Third party published content	E-portfolio content published by anyone other than the learner.

Bibliography

Convergence e-Business Solutions Pty Ltd (March 2006), *Learner Identity Management Framework Project - Framework Report (V3.0),* AICTEC. - *http://www.aictec.edu.au/aictec/webdav/site/standardssite/shared/LIMF_Report_2006.pdf*

Australian Law Reform Commission, (August 2008), *ALRC Report 108, For Your Information: Australian Privacy Law and Practice,* Australian Law Reform Commission. - http://www.austlii.edu.au/au/other/alrc/publications/reports/108/

Brant, J. (July 2006), *Storage, access and related issues for eportfolios*.

Charlesworth, A., and Home, A. (2004), *Legal aspects of eportfolio systems: A short FAQ*. Retrieved from http://www.jisc.ac.uk/uploaded_documents/Legal_Aspects_FAQ.pdf

Curyer, S., Leeson, J., Mason, J., and Williams, A. (2007). *Developing e-portfolios for VET: Policy issues and interoperability*, Australian Flexible Learning Framework.

Downes (October 2008). *Half an hour: My digital identity*. Retrieved 17 October 2008 from http://halfanhour.blogspot.com/2008/10/my-digital-identity.html

Hallam, G., Harper, W., McCowan, C., Hauville, K., McAllister, L., Creagh, T., et al. (2008, October), *Australian ePortfolio Project - ePortfolio use by university students in Australia: Informing excellence in policy and practice - final report*. - http://www.eportfoliopractice.qut.edu.au/information/report/

JISC Infonet (n.d.), *JISC infonet - access, authentication and storage.* Retrieved 22 October 2008 from http://www.jiscinfonet.ac.uk/infokits/e-portfolios/access

OECD (2002), *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*

Perry, W. P. (March 2009), *E-portfolios for RPL Assessment*. - Australian Flexible Learning Framework

Centre for the Study of Higher Education, The University of Melbourne, and Centre for Higher Education Management & Policy , University of New England (May 2008) *Proposal for An Australian Higher Education Graduation Statement.* – http://www.dest.gov.au/sectors/higher_education/publications_resources/profiles/documents/ahegsfinalreport_pdf.htm

Appendix 1 – Consultation responses

The following records the responses to questions asked of the educational leaders as part of this research.

1. What types of content could be stored on an e-portfolio? How would you classify them?

Classify by:

- file type – text, images, sounds, podcasts
- purpose – academic results, examples of work, references
- publisher – first person or third person
- access – public or private
- current work developed for a learning institution
- personal information such as hobbies, interests
- previous work history
- family information
- media files, photos, video, flash, word documents, spreadsheets, database, PowerPoint
- evidence of work, resumes, assessments, learning journals – across whole of learning experience.

Comments:

- Dubious about putting authenticated results on the e-portfolio. Huge task to get agreement.
- Can put up evidence of achievement, CVs etc.
- Classify by industry, employer, RPL (recognition of prior learning) application. C.f. content management system – lots of different types of content with different privileges.

Types of content:

Audio; video; digital stories; blogs; reflections; written assessment; teacher feedback; work history; scanned testimonials; goal setting; personal philosophy; links to papers and presentations done; workshops developed or attended; testimonials from own students if they are also tutors; Google documents; links to personal web page; toolbox created or customised; artefacts.

Elearnspace Classification:

- personal information
- education history
- recognition, awards, certificates
- reflective page
- course work, assignments, project and instructor comments
- previous employers comments, testimonials
- personal goals, plans, philosophies, interests
- presentations, papers

- personal activities, volunteer work, associated testimonials
- professional development undertaken
- resources developed and web pages designed
- skills passport – showing meeting legislative requirements, eg responsible serving of alcohol for hospitality students
- competencies, statements of results, skill based training programs, testimonials from enterprise, recognition documentation
- examples of student work, projects, CVs, employability skills.
- categories: education and work place
- documents, web links, videos, scanned certificates, photographs, blog content
- diverse content – anything multi-media, tagged resources, assessment, documents, scanned certificates, web links. Classification should be by folksomonic tagging, not driven by any hierarchical approach. Proponents should be able to use their own language – key words, not a taxonomic approach.

2. Who owns this content? Do the ownership rules need to be changed for different types of content?

- Person who publishes it owns it.
- Where it is stored might impact on ownership – c.f. rules for some social networking sites where host owns the content. When content is held by a third party, perhaps it is owned by that party.
- Complexity grows with the number of contributors.
- Because the learner needs to be able to remove content, therefore it needs to be owned by the learner.
- Example of a year 10 boy getting a negative report from a school principal which is fixed for life. The learner should have the ability to remove or edit out.
- Individual who is putting together the e-portfolio must own the content.
- Intellectual property issues can arise – for example when producing work as part of employment.
- Student in TAFE sector
- Teacher resources – RTO would be owner.
- Teacher is a learner and therefore might have own materials too.
- Learner owns the content but conversely the organisation needs the evidence for the AQTF auditing purposes.
- Ownership rules should stay constant.
- Individual student, RTO, or regulator may have a stake.
- Learner.
- Other content like transcripts would be owned by the institution.
- Primarily owned by the person who set up the e-portfolio. Linked third party content might be different however. Staff who create an e-portfolio might not own the content if it was material produced as part of employment.
- Difficult to identify who owns the content – can relate to verification – example

given of work being published that actually belongs to another.

- Copyright in any material produced by students subsists in the student except in cases where there is a mutual agreement between the parties to the contrary.

3. Do you think privacy and security issues vary depending on the type of content? How?

- Yes. Onus should be placed on the individual publisher.
- Privacy should be at the discretion of the e-portfolio owner. They control the rules about who sees what.
- Hard for a user to claim rights of privacy when choosing to put oneself in this type of environment. Hopefully safer than MySpace, but everyone going in to it would need to know that there is the potential for the content to be viewed beyond the audience expected.
- 'Buyer beware'.
- The e-portfolio owner should have the right to determine content that they wish to keep secure and private – therefore the system should offer this as the default for all content and then allow the owner to determine who can have access and to what they can have access.
- There might also be other less secure and more public services that a user could contribute to, such as a learning object repository.
- Up to the student to determine privacy rules, but the organisation's needs make this tricky.
- All should be private and secure but organisation needs access.
- Not publicly available on the web.
- Format needs to be one that can't be altered – numbered, recorded, meet AQTF guidelines
- Content like results transcripts would have higher security requirements.
- Need to be able to publish material that can't be changed.
- The owner needs the right to determine who has access to various parts of the e-portfolio.
- Existing policies about disclosure of personal information need to be reconsidered in the context of e-portfolios. Students need to be able to control what information should be released.

4. Privacy legislation places an onus on an organisation to 'take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.' What do you think such 'reasonable steps' might be for student e-portfolio information?

- Consider whether an educational institution should host this in the first place?
- Depends on type of content though. Academic transcripts are the responsibility of the institution. But other types perhaps should be held in a system either owned by the learner or by the third party host.
- Should educational institutions control the types of content that can be published?
- Similar to what is currently done with enrolment information. Sees it as being stored out there in the ether.

- CDU only allows students to access the e-portfolio via LMS with password control. Minor's parents to sign permission.
- There is an expectation that the content is private but there is always a possibility that privacy can be breached.
- Existing organisational policies and procedures.
- Password protection
- Ability to release to a third party.
- Fully private status.
- Each student has private password.
- AQTF guidelines as a rulebook. Regulatory organisations. industry sectors.
- A technical issue.
- Student needs to have control to prevent access by unauthorised people.
- Access should only be for those for whom the learner wants to grant access.

5. What categories of users might be given access to some or all of an e-portfolio? What might be the circumstances governing this access? Who should decide who is given access?

- Should be the prerogative of the e-portfolio owner (learner) to determine – other than academic transcripts.
- Who else might be given access?
    - family and friends
    - prospective employers
    - RPL person
- at discretion of the e-portfolio owner.
- The owner must determine access. Can't force people to put work in this environment and then not give control over access.
- Assessor or lecturer may need to be given access, but prerogative still with user.
- Student should have the right to give access to anyone they choose, eg:
    - teacher
    - non-teaching staff, eg library, student support
    - employers
    - consultancy places
    - online forums
    - administrator, course coordinator
    - tutor, person running the course
    - student
    - notion of mandatory parts which tutors need to be given access to.
    - auditors – funding bodies
    - prospective employers

- other educators, eg trainee teachers
- institutional right of access and student control
- learners
- RTOs
- industry associations
- learners have final say
- future employers
- RPL purposes with institutions
- alumni purposes – institution staff
- the learner, the institution, employers, recruitment agencies. Access determined by the e-portfolio owner.

6. Do you have any thoughts about how the various users of an e-portfolio might initially have their identities confirmed and then authenticated each time they visit?

- Within an organisation identities and profiles can be established. Externally the owner should decide who has access and be responsible for identification and authentication.
- The owner should be responsible. It is feasible to give unique log on names and passwords.
- An email address might be sufficient.
- Might also open to certain groups.
- Students would be managed through unique ID numbers for students
- The student should then be responsible for identifying and giving access to those s/he wishes to give access to.
- Owner can invite and give passwords. Limited time frame.
- Legal advice – information acts
- Over-arching reason??
- Learner to be able to provide the third party with a link.
- Up to the learner to identify who they wish to give access to and then send either a link or a password to the view they want to make visible to that person.
- Learner to identify who they wish to give access to and then the e-portfolio service provider to provide passwords or other means of controlled access that can be managed by the student. A student may also wish to make some content public. The option of varying access rights would be helpful.
- The individual themselves ought to control who can access it. Data mining e-portfolios might tempt some organisations but it must not happen. Access could be given to employers, training providers, teaching staff, anyone the individual may wish to give access.

7. What impact might third party access have on security and privacy issues?

- The e-portfolio owner should have the capacity to give access to third parties for a limited period of time and access to a sub-set of the content. The e-portfolio needs to offer this functionality to the user.
- Tricky! Hard to restrict. Be aware that it might go beyond the person you intend.
- This is a risk!
- New tools are being developed however which might solve this problem eventually.
- A concern – content can be downloaded. Wikis can be locked, but attachments can be downloaded.
- Open for plagiarising.
- Risk of the third party being given access and then misusing it.
- Internal staff need controls as they already do for the SISs. Eg tracking people who go in and have a look at records. Authorities limit behaviours based on roles.

8. Who should have the ability to publish and update content in an individual's e-portfolio?

- The individual owner.
- The institution to update academic records.
- Individuals to decide who else has access.
- The individual to decide.
- If there is to be a section for assessors to review work and make comments, this should be quarantined from other sections – privacy issue.
- The person who owns the e-portfolio.
- A lecturer may be able to contribute comments but not do so in a way that affects the integrity of the e-portfolio.
- The owner of the e-portfolio has to have the right and also the option of giving read/write access to third parties to selected content.
- Learners.
- Employers.
- The individual who owns the e-portfolio, institute staff for feedback purposes.
- The learner and anyone they wish to allow to do so. In cases where offensive material is published, the institution ought to have the right to remove it.

9. How might the authenticity of content published in an e-portfolio be verified?

- The users to use existing methods/strategies.
- Should be done outside of the e-portfolio – can't expect a system to do everything. Person using the information is responsible for verifying it.
- Like any other form of assessment – the person needs to back up with additional questions. If I receive an assignment I feel uncertain about, I need to make further enquiries. Judicious judgement.
- Difficult. Look at something like signing a verification notification. Include something like an intricate password.

- Extremely difficult c.f. normal process. A vexed process.
- The user of the information needs to validate it.
- There are examples of technologies with special cameras or mobile phone technologies can be used to give evidence of competency.
- Don't rely on it as stand alone evidence – seek verification from a third party.
- Institutions need to give mechanism for verification, eg internal institution phone number (for content within its control).
- Don't think this is the job of the e-portfolio service provider – it is the teacher or employer's job to verify. Could provide contact details for verification. Peer review.
- Students should be required to submit a legal document to say that they are the owners of the work and that it is original.

10. What types of information are held externally that may be of value for an individual's e-portfolio?

- Academic records – from the central system?
- Other data might be like CRM data, for example where they have worked etc - but unlikely.
- Could be useful to have secure links to verified Third party records (if it can be done).
- We have a LMS that gives access to results for a particular unit.
- The overall results are held in a SMS which is not accessed by students. In principle support the idea of a student giving another person access to SMS results.
- Transcripts of results.
- Records of professional development completed.
- Content in a learning management system.
- Feedback received.
- RPL documentation – includes letters from previous employers, photographic evidence, work place assessments, could be scanned.
- Records, grades.
- Where there are other web sites that show additional work, communities of practice perhaps, etc, these can be linked.
- Qualification data – can link also to LMS and pull in content from, eg Moodle.
- Could be any of the web 2.0 social sites. The e-portfolio could be an aggregator of external sites.
- A mechanism to allow results data to be made available and a means of verifying made available, such as a telephone number, etc.

11. Can you suggest ways in which this content could be accessed for e-portfolio purposes?

- Keep the unique student number. Create business rules that allow access even after leaving active engagement with the institution.
- Link.

- Largely a technical question.
- Sees e-portfolio as a small area within a wider compendium of tools available to a student, eg grades, calendars, mail, their home page.
- Systems integration.
- Imported from LMS.

12. If the learner wished to include some of this content in his/her e-portfolio (eg achievement data), how might this be verified? Could there be different types of verification for different types of content, eg RPL, employability skills, assessment, employment, testimonials?

- Thin portfolio – read only option for verified content beyond.
- Same comment as before – up to the user of the system to verify.
- Be able to back it up with physical documents
- Verify via a contact person within the institution
- Use strategies outside of the e-portfolio
- Signed by an official of an organisation, seal of company

13. If learners are to be given certain rights and privileges with regard to the use of an e-portfolio, there may need to be some consistency in the definition of learner. How would you define a 'learner' for the purposes of e-portfolio management?

- Consider beyond VET and take a whole of life perspective. While in VET, defined by student number.
- We should be talking about owners, not learners. Could be used for purposes beyond learning. Should be available to everybody, such as a newly arrived immigrant who goes straight in to work.
- Anticipates the users of e-portfolios to be motivated by study or career requirements, not hobby.
- Everyone is a learner – ought not be narrowed to education.
- Person registered by an RTO or higher institution as participating in a course. Portability issue important to the adult and community education (ACE) sector.
- Some-one developing knowledge, understanding, skills, associated with a task new to the learner.
- Learner is the wrong label – better defined as the user of the e-portfolio. If the purpose of the e-portfolio is related to study or future work and established by an institution, then the user will have been a learner once.
- Learner can be anyone. Must bear in mind 'simultaneous learning' where learning occurs formally and informally at the same time.
- Uncomfortable with the notion of a dichotomy between student and teacher – both could be users of an e-portfolio.

Appendix 2 – Commonwealth Information Privacy Principles

Principle 1 - Manner and purpose of collection of personal information

1. Personal information shall not be collected by a collector for inclusion in a record or in a generally available publication unless:
   (a) the information is collected for a purpose that is a lawful purpose directly related to a function or activity of the collector; and
   (b) the collection of the information is necessary for or directly related to that purpose.
2. Personal information shall not be collected by a collector by unlawful or unfair means.

Principle 2 - Solicitation of personal information from individual concerned

Where:

(a) a collector collects personal information for inclusion in a record or in a generally available publication; and

(b) the information is solicited by the collector from the individual concerned;

the collector shall take such steps (if any) as are, in the circumstances, reasonable to ensure that, before the information is collected or, if that is not practicable, as soon as practicable after the information is collected, the individual concerned is generally aware of:

(c) the purpose for which the information is being collected;

(d) if the collection of the information is authorised or required by or under law - the fact that the collection of the information is so authorised or required; and

(e) any person to whom, or any body or agency to which, it is the collector's usual practice to disclose personal information of the kind so collected, and (if known by the collector) any person to whom, or any body or agency to which, it is the usual practice of that first mentioned person, body or agency to pass on that information.

Principle 3 - Solicitation of personal information generally

Where:

(a) a collector collects personal information for inclusion in a record or in a generally available publication; and

(b) the information is solicited by the collector:

the collector shall take such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is collected:

(c) the information collected is relevant to that purpose and is up to date and complete; and

(d) the collection of the information does not intrude to an unreasonable extent upon the personal affairs of the individual concerned.

Principle 4 - Storage and security of personal information

A record-keeper who has possession or control of a record that contains personal information shall ensure:

(a) that the record is protected, by such security safeguards as it is reasonable in the circumstances to take, against loss, against unauthorised access, use, modification or disclosure, and against other misuse; and

(b) that if it is necessary for the record to be given to a person in connection with the provision of a service to the record-keeper, everything reasonably within the power of the record-keeper is done to prevent unauthorised use or disclosure of information contained in the record.

Principle 5 - Information relating to records kept by record-keeper

1. A record-keeper who has possession or control of records that contain personal information shall, subject to clause 2 of this Principle, take such steps as are, in the circumstances, reasonable to enable any person to ascertain:

   whether the record-keeper has possession or control of any records that contain personal information; and

   if the record-keeper has possession or control of a record that contains such information:

   the nature of that information;

   the main purposes for which that information is used; and

   the steps that the person should take if the person wishes to obtain access to the record.

2. A record-keeper is not required under clause 1 of this Principle to give a person information if the record-keeper is required or authorised to refuse to give that information to the person under the applicable provisions of any law of the Commonwealth that provides for access by persons to documents.

3. A record-keeper shall maintain a record setting out:

   the nature of the records of personal information kept by or on behalf of the record-keeper;

   the purpose for which each type of record is kept;

   the classes of individuals about whom records are kept;

   the period for which each type of record is kept;

   (a) the persons who are entitled to have access to personal information contained in the records and the conditions under which they are entitled to have that access; and

   the steps that should be taken by persons wishing to obtain access to that information.

4. A record-keeper shall:

   make the record maintained under clause 3 of this Principle available for inspection by members of the public; and

   (a) give the Commissioner, in the month of June in each year, a copy of the record so maintained.

Principle 6 - Access to records containing personal information

Where a record-keeper has possession or control of a record that contains personal information, the individual concerned shall be entitled to have access to that record, except to the extent that the record-keeper is required or authorised to refuse to provide the individual with access to that record under the applicable provisions of any law of the Commonwealth that provides for access by persons to documents.

Principle 7 - Alteration of records containing personal information

1. A record-keeper who has possession or control of a record that contains personal information shall take such steps (if any), by way of making appropriate corrections, deletions and additions as are, in the circumstances, reasonable to ensure that the record:

   is accurate; and

   is, having regard to the purpose for which the information was collected or is to be used and to any purpose that is directly related to that purpose, relevant, up to date, complete and not misleading.

2. The obligation imposed on a record-keeper by clause 1 is subject to any applicable limitation in a law of the Commonwealth that provides a right to require the correction or amendment of documents.

3. Where:

   (a) the record-keeper of a record containing personal information is not willing to amend that record, by making a correction, deletion or addition, in accordance with a request by the individual concerned; and

   (b) no decision or recommendation to the effect that the record should be amended wholly or partly in accordance with that request has been made under the applicable provisions of a law of the Commonwealth;

   the record-keeper shall, if so requested by the individual concerned, take such steps (if any) as are reasonable in the circumstances to attach to the record any statement provided by that individual of the correction, deletion or addition sought.

Principle 8 - Record-keeper to check accuracy etc of personal information before use

A record-keeper who has possession or control of a record that contains personal information shall not use that information without taking such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is proposed to be used, the information is accurate, up to date and complete.

Principle 9 - Personal information to be used only for relevant purposes

A record-keeper who has possession or control of a record that contains personal information shall not use the information except for a purpose to which the information is relevant.

Principle 10 - Limits on use of personal information

1. A record-keeper who has possession or control of a record that contains personal information that was obtained for a particular purpose shall not use the information for any other purpose unless:

   (a) the individual concerned has consented to use of the information for that other purpose;

(b) the record-keeper believes on reasonable grounds that use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person;

(c) use of the information for that other purpose is required or authorised by or under law;

(d) use of the information for that other purpose is reasonably necessary for enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue; or

(e) the purpose for which the information is used is directly related to the purpose for which the information was obtained.

2. Where personal information is used for enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue, the record-keeper shall include in the record containing that information a note of that use.

Principle 11 - Limits on disclosure of personal information

1. A record-keeper who has possession or control of a record that contains personal information shall not disclose the information to a person, body or agency (other than the individual concerned) unless:

(a) the individual concerned is reasonably likely to have been aware, or made aware under Principle 2, that information of that kind is usually passed to that person, body or agency;

(b) the individual concerned has consented to the disclosure;

(c) the record-keeper believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or of another person;

(d) the disclosure is required or authorised by or under law; or

(e) the disclosure is reasonably necessary for the enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue.

2. Where personal information is disclosed for the purposes of enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the purpose of the protection of the public revenue, the record-keeper shall include in the record containing that information a note of the disclosure.

3. A person, body or agency to whom personal information is disclosed under clause 1 of this Principle shall not use or disclose the information for a purpose other than the purpose for which the information was given to the person, body or agency.

Appendix 3 – National Privacy Principles

1. Collection

1.1 An organisation must not collect personal information unless the information is necessary for one or more of its functions or activities.

1.2 An organisation must collect personal information only by lawful and fair means and not in an unreasonably intrusive way.

1.3 At or before the time (or, if that is not practicable, as soon as practicable after) an organisation collects personal information about an individual from the individual, the organisation must take reasonable steps to ensure that the individual is aware of:

(a) the identity of the organisation and how to contact it; and

(b) the fact that he or she is able to gain access to the information; and

(c) the purposes for which the information is collected; and

(d) the organisations (or the types of organisations) to which the organisation usually discloses information of that kind; and

(e) any law that requires the particular information to be collected; and

(f) the main consequences (if any) for the individual if all or part of the information is not provided.

1.4 If it is reasonable and practicable to do so, an organisation must collect personal information about an individual only from that individual.

1.5 If an organisation collects personal information about an individual from someone else, it must take reasonable steps to ensure that the individual is or has been made aware of the matters listed in subclause 1.3 except to the extent that making the individual aware of the matters would pose a serious threat to the life or health of any individual.

2. Use and disclosure

2.1 An organisation must not use or disclose personal information about an individual for a purpose (the secondary purpose) other than the primary purpose of collection unless:

(a) both of the following apply:

(i) the secondary purpose is related to the primary purpose of collection and, if the personal information is sensitive information, directly related to the primary purpose of collection;

(ii) the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose; or

(b) the individual has consented to the use or disclosure; or

(c) if the information is not sensitive information and the use of the information is for the secondary purpose of direct marketing:

(i) it is impracticable for the organisation to seek the individual's consent before that particular use; and

(ii) the organisation will not charge the individual for giving effect to a request by the individual to the organisation not to receive direct marketing communications; and

(iii) the individual has not made a request to the organisation not to receive direct marketing communications; and

(iv) in each direct marketing communication with the individual, the organisation draws to the individual's attention, or prominently displays a notice, that he or she may express a wish not to receive any further direct marketing communications; and

(v) each written direct marketing communication by the organisation with the individual (up to and including the communication that involves the use) sets out the organisation's business address and telephone number and, if the communication with the individual is made by fax, telex or other electronic means, a number or address at which the organisation can be directly contacted electronically; or

(d) if the information is health information and the use or disclosure is necessary for research, or the compilation or analysis of statistics, relevant to public health or public safety:

(i) it is impracticable for the organisation to seek the individual's consent before the use or disclosure; and

(ii) the use or disclosure is conducted in accordance with guidelines approved by the Commissioner under section 95A for the purposes of this subparagraph; and

(iii) in the case of disclosure—the organisation reasonably believes that the recipient of the health information will not disclose the health information, or personal information derived from the health information; or

(e) the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent:

(i) a serious and imminent threat to an individual's life, health or safety; or

(ii) a serious threat to public health or public safety; or

(ea) if the information is genetic information and the organisation has obtained the genetic information in the course of providing a health service to the individual:

(i) the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety (whether or not the threat is imminent) of an individual who is a genetic relative of the individual to whom the genetic information relates; and

(ii) the use or disclosure is conducted in accordance with guidelines approved by the Commissioner under section 95AA for the purposes of this subparagraph; and

(iii) in the case of disclosure—the recipient of the genetic information is a genetic relative of the individual; or

(f) the organisation has reason to suspect that unlawful activity has been, is being or may be engaged in, and uses or discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities; or

(g) the use or disclosure is required or authorised by or under law; or

(h) the organisation reasonably believes that the use or disclosure is

reasonably necessary for one or more of the following by or on behalf of an enforcement body:

(i) the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law;

(ii) the enforcement of laws relating to the confiscation of the proceeds of crime;

(iii) the protection of the public revenue;

(iv) the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct;

(v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal.

Note 1: It is not intended to deter organisations from lawfully co operating with agencies performing law enforcement functions in the performance of their functions.

Note 2: Subclause 2.1 does not override any existing legal obligations not to disclose personal information. Nothing in subclause 2.1 requires an organisation to disclose personal information; an organisation is always entitled not to disclose personal information in the absence of a legal obligation to disclose it.

Note 3: An organisation is also subject to the requirements of National Privacy Principle 9 if it transfers personal information to a person in a foreign country.

2.2 If an organisation uses or discloses personal information under paragraph 2.1(h), it must make a written note of the use or disclosure.

2.3 Subclause 2.1 operates in relation to personal information that an organisation that is a body corporate has collected from a related body corporate as if the organisation's primary purpose of collection of the information were the primary purpose for which the related body corporate collected the information.

2.4 Despite subclause 2.1, an organisation that provides a health service to an individual may disclose health information about the individual to a person who is responsible for the individual if:

(a) the individual:

(i) is physically or legally incapable of giving consent to the disclosure; or

(ii) physically cannot communicate consent to the disclosure; and

(b) a natural person (the carer) providing the health service for the organisation is satisfied that either:

(i) the disclosure is necessary to provide appropriate care or treatment of the individual; or

(ii) the disclosure is made for compassionate reasons; and

(c) the disclosure is not contrary to any wish:

(i) expressed by the individual before the individual became unable to give or communicate consent; and

(ii) of which the carer is aware, or of which the carer could reasonably be expected to be aware; and

(d) the disclosure is limited to the extent reasonable and necessary for a purpose mentioned in paragraph (b).

2.5 For the purposes of subclause 2.4, a person is responsible for an individual if the person is:

(a) a parent of the individual; or

(b) a child or sibling of the individual and at least 18 years old; or

(c) a spouse or de facto spouse of the individual; or

(d) a relative of the individual, at least 18 years old and a member of the individual's household; or

(e) a guardian of the individual; or

(f) exercising an enduring power of attorney granted by the individual that is exercisable in relation to decisions about the individual's health; or

(g) a person who has an intimate personal relationship with the individual; or

(h) a person nominated by the individual to be contacted in case of emergency.

2.6 In subclause 2.5:

child of an individual includes an adopted child, a step child and a foster child, of the individual.

parent of an individual includes a step parent, adoptive parent and a foster parent, of the individual.

relative of an individual means a grandparent, grandchild, uncle, aunt, nephew or niece, of the individual.

sibling of an individual includes a half brother, half sister, adoptive brother, adoptive sister, step brother, step sister, foster brother and foster sister, of the individual.

3. Data quality

An organisation must take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up to date.

4. Data security

4.1 An organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.

4.2 An organisation must take reasonable steps to destroy or permanently de identify personal information if it is no longer needed for any purpose for which the information may be used or disclosed under National Privacy Principle 2.

5. Openness

5.1 An organisation must set out in a document clearly expressed policies on its management of personal information. The organisation must make the document available to anyone who asks for it.

5.2 On request by a person, an organisation must take reasonable steps to let the person know, generally, what sort of personal information it holds, for what purposes, and how it collects, holds, uses and discloses that information.

6. Access and correction

6.1 If an organisation holds personal information about an individual, it must provide the individual with access to the information on request by the individual, except to the extent that:

(a) in the case of personal information other than health information—providing access would pose a serious and imminent threat to the life or health of any individual; or

(b) in the case of health information—providing access would pose a serious threat to the life or health of any individual; or

(c) providing access would have an unreasonable impact upon the privacy of other individuals; or

(d) the request for access is frivolous or vexatious; or

(e) the information relates to existing or anticipated legal proceedings between the organisation and the individual, and the information would not be accessible by the process of discovery in those proceedings; or

(f) providing access would reveal the intentions of the organisation in relation to negotiations with the individual in such a way as to prejudice those negotiations; or

(g) providing access would be unlawful; or

(h) denying access is required or authorised by or under law; or

(i) providing access would be likely to prejudice an investigation of possible unlawful activity; or

(j) providing access would be likely to prejudice:

(i) the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law; or

(ii) the enforcement of laws relating to the confiscation of the proceeds of crime; or

(iii) the protection of the public revenue; or

(iv) the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct; or

(v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of its orders;

by or on behalf of an enforcement body; or

(k) an enforcement body performing a lawful security function asks the organisation not to provide access to the information on the basis that providing access would be likely to cause damage to the security of Australia.

6.2 However, where providing access would reveal evaluative information generated within the organisation in connection with a commercially sensitive decision making process, the organisation may give the individual an explanation for the commercially sensitive decision rather than direct access to the information.

Note: An organisation breaches subclause 6.1 if it relies on subclause 6.2 to give an individual an explanation for a commercially sensitive decision in circumstances where subclause 6.2 does not apply.

6.3 If the organisation is not required to provide the individual with access to the

information because of one or more of paragraphs 6.1(a) to (k) (inclusive), the organisation must, if reasonable, consider whether the use of mutually agreed intermediaries would allow sufficient access to meet the needs of both parties.

6.4 If an organisation charges for providing access to personal information, those charges:

(a) must not be excessive; and

(b) must not apply to lodging a request for access.

6.5 If an organisation holds personal information about an individual and the individual is able to establish that the information is not accurate, complete and up to date, the organisation must take reasonable steps to correct the information so that it is accurate, complete and up to date.

6.6 If the individual and the organisation disagree about whether the information is accurate, complete and up to date, and the individual asks the organisation to associate with the information a statement claiming that the information is not accurate, complete or up to date, the organisation must take reasonable steps to do so.

6.7 An organisation must provide reasons for denial of access or a refusal to correct personal information.

7. Identifiers

7.1 An organisation must not adopt as its own identifier of an individual an identifier of the individual that has been assigned by:

(a) an agency; or

(b) an agent of an agency acting in its capacity as agent; or

(c) a contracted service provider for a Commonwealth contract acting in its capacity as contracted service provider for that contract.

7.1A However, subclause 7.1 does not apply to the adoption by a prescribed organisation of a prescribed identifier in prescribed circumstances.

Note: There are prerequisites that must be satisfied before those matters are prescribed: see subsection 100(2).

7.2 An organisation must not use or disclose an identifier assigned to an individual by an agency, or by an agent or contracted service provider mentioned in subclause 7.1, unless:

(a) the use or disclosure is necessary for the organisation to fulfil its obligations to the agency; or

(b) one or more of paragraphs 2.1(e) to 2.1(h) (inclusive) apply to the use or disclosure; or

(c) the use or disclosure is by a prescribed organisation of a prescribed identifier in prescribed circumstances.

Note: There are prerequisites that must be satisfied before the matters mentioned in paragraph (c) are prescribed: see subsections 100(2)

and (3).

7.3 In this clause:

identifier includes a number assigned by an organisation to an individual to identify uniquely the individual for the purposes of the organisation's operations. However, an individual's name or ABN (as defined in the *A New Tax System (Australian Business*

Number) Act 1999) is not an ***identifier***.

8. Anonymity

Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation.

9. Transborder data flows

An organisation in Australia or an external Territory may transfer personal information about an individual to someone (other than the organisation or the individual) who is in a foreign country only if:

(a) the organisation reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are substantially similar to the National Privacy Principles; or

(b) the individual consents to the transfer; or

(c) the transfer is necessary for the performance of a contract between the individual and the organisation, or for the implementation of pre contractual measures taken in response to the individual's request; or

(d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the organisation and a third party; or

(e) all of the following apply:

(i) the transfer is for the benefit of the individual;

(ii) it is impracticable to obtain the consent of the individual to that transfer;

(iii) if it were practicable to obtain such consent, the individual would be likely to give it; or

(f) the organisation has taken reasonable steps to ensure that the information which it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with the National Privacy Principles.

10. Sensitive information

10.1 An organisation must not collect sensitive information about an individual unless:

(a) the individual has consented; or

(b) the collection is required by law; or

(c) the collection is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual, where the individual whom the information concerns:

(i) is physically or legally incapable of giving consent to the collection; or

(ii) physically cannot communicate consent to the collection; or

(d) if the information is collected in the course of the activities of a non profit organisation—the following conditions are satisfied:

(i) the information relates solely to the members of the organisation or to individuals who have regular contact with it in connection with its activities;

(ii) at or before the time of collecting the information, the organisation undertakes to the individual whom the information concerns that the organisation will not disclose the information without the individual's

consent; or

(e) the collection is necessary for the establishment, exercise or defence of a legal or equitable claim.

10.2 Despite subclause 10.1, an organisation may collect health information about an individual if:

(a) the information is necessary to provide a health service to the individual; and

(b) the information is collected:

(i) as required or authorised by or under law (other than this Act); or

(ii) in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation.

10.3 Despite subclause 10.1, an organisation may collect health information about an individual if:

(a) the collection is necessary for any of the following purposes:

(i) research relevant to public health or public safety;

(ii) the compilation or analysis of statistics relevant to public health or public safety;

(iii) the management, funding or monitoring of a health service; and

(b) that purpose cannot be served by the collection of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained; and

(c) it is impracticable for the organisation to seek the individual's consent to the collection; and

(d) the information is collected:

(i) as required by law (other than this Act); or

(ii) in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation; or

(iii) in accordance with guidelines approved by the Commissioner under section 95A for the purposes of this subparagraph.

10.4 If an organisation collects health information about an individual in accordance with subclause 10.3, the organisation must take reasonable steps to permanently de identify the information before the organisation discloses it.

10.5 In this clause:

non profit organisation means a non profit organisation that has only racial, ethnic, political, religious, philosophical, professional, trade, or trade union aims.

Appendix 4 – Shibboleth software for AAF

Several software packages have been developed to support AAF.

Shibboleth Attribute Release Policy Editing Tools

Shibboleth provides for privacy protection through Attribute Release Policies (ARPs). Release of user attributes from an Identity Provider (IdP) to a Service Provider (SP) is determined by the IdP's ARPs. ARPs contain a set of rules specifying which attributes to release for institution members in general, or for specific individuals.

ShARPE and Autograph are two open source applications for managing Shibboleth Attribute Release Policies via a GUI. ShARPE is used by IdP administrators to define site and group ARPs, and Autograph is used by IdP members to define individual ARPs based on individual privacy requirements.

Shibboleth Federation Management Tools

Federation Manager is a tool to manage centrally institutional participation entry within Shibboleth in the AAF. It offers flexible configuration of entities as well as strong enforcement of the AAF Operational Requirements and Recommendations Document.

Service Description is a mechanism for the Service Provider (SP) administrator to inform other members of the Federation about the services available from the SP.

Customised metadata ensures that the IdP and SP only receive information about their respective partner institutions. An IdP need only know about SPs (services) that are potentially applicable to its end-users, and by the same token an SP can restrict the set of IdPs that may be able to access a service.

Where Are You From (WAYF) is a federation service that aids users to choose their IdP within the large number of IdPs available in the Federation. The WAYF is also referred as Home Institution Discovery Service, or simply Discovery Service. As the SP has no knowledge regarding the user’s IdP location, it uses the WAYF to redirect user to select the correct IdP.

Collaboration Toolkit for Virtual Organisations (IAMSuite)

IAMSuite provides a common environment for researchers to perform collaboration in a Virtual Organisation (VO) context. Users from different institutions can gather in a common place, share resources, and collaborate without the need to worry about common infrastructure such as security (authentication and authorisation).

People Picker

People Picker allows SPs to pick a federation user and give them access to its resources. Based on trusted IdP records within the Federation, SPs are able to discover authoritative user information (name and email) from People Picker. Information discovered manages the user’s privacy restrictions as well as the restrictions of the institution to which they belong.

Federated White Pages

Federated White Pages uses the People Picker tool to allow end-users to discover information about the other end-users in the Federation. This service is a protected resource allowing convenient access to participating IdPs from a single location.

Federated Services

This is an umbrella for a range of collaborative services that can be offered centrally in a Shibboleth Federation. These services are shared across multiple servers.

Federation members use the tools as service, without knowledge of, or the need to own, the infrastructure.

Users can access a growing number of Shibbolised services such as wikis, learning and content management tools, mailing lists, repositories, blogs, chats, forums, software development tools, news feeds, with more being available in the future.

Federated Entitlement Service

FES is a centralised service in a Federation that allows both IdP and SP administrators to share and assign a range of entitlements to their users to help a SP enforces its authorisation. The SP receives acceptable user's entitlements from which it can perform checking and mapping to authorisation rules to see whether the user is allowed to gain access to the particular resources in question.

Shibboleth Federation Hosted Services

Unlike other Shibboleth Federations, AAF will provide some commonly needed tools for its Members. These tools enable Federation end-users to collaborate with other users securely in real time. These Federation tools, which would otherwise require considerable local maintenance from each Member to run individually, can more efficiently be provided as a suite of hosted services available from the Federation for use by Members.

Some of the tools already in deployment include Federation Chat Helpdesk, Shibbolised SubEtha Mailing List, Shibbolised OpenMeeting, with others to come in the future.

For more information contact:

E-portfolios Business Activity

Phone: (08) 8348 4075

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

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

Australian Flexible Learning Framework

Phone: (07) 3307 4700

Fax: (07) 3259 4371

Email: enquiries@flexiblelearning.net.au

Website: flexiblelearning.net.au

GPO Box 1326

Brisbane QLD 4001