Ultranet Privacy Impact Assessment

Executive Summary

and

Overview of Recommendations and DEECD Actions

SalingerPrivacy

Privacy Impact Assessment Report

The Ultranet

Prepared for Victorian Department of Education and Early Childhood Development

19 March 2010

EXECUTIVE SUMMARY

The Ultranet

The Ultranet is a $60M information and communications technology system that will be implemented from 2010 in every Victorian government school, covering the school years P-12. The Ultranet will store rich data "about a student's progress from year to year and from school to school", which "will underpin knowledge management processes and strengthen educational planning at all levels; for teachers, schools and DEECD's central and regional offices" (1).

Once the rollout is complete there will be approximately 45,000 teachers using the Ultranet, as well as around 550,000 students and perhaps 900,000 parents. There will also be approximately 2,000 corporate users from DEECD regional and head offices, as well as around 12,000 non-teaching staff in schools.

The primary functions to be offered to users of the Ultranet will be:
• Home spaces for all users
• eXpress spaces for students and teachers
• a Directory of users within each school
• Community spaces for students, parents and teachers
• Collaborative Learning spaces for students and teachers
• Design spaces for teachers
• Learner Profile, accessible by teachers, students and parents, which will pull together a variety of student data
• Learning Tasks – where learning items (e.g. homework or assignments) are set by teachers and lodged by students, and feedback and observations are recorded, and
• Content for students and teachers.

A detailed explanation of each of these functions, as well as information about system design, a map of data flows and how personal information will be collected, stored, used and disclosed in the Ultranet, are found in Chapter 2 of this report.

(1) Ultranet Business Case, v0.7, May 2009.

This privacy assessment

Privacy generally refers to a person's ability to control how their personal information is handled throughout the life cycle of that information – how it is collected, stored, accessed, checked, used and disclosed. The process and objectives of a Privacy Impact Assessment (PIA), and our methodology in conducting this PIA, are set out in Chapter 1.

Chapter 3 of this report reviews the Ultranet project described in Chapter 2 as against a set of privacy principles, the information privacy principles (IPPs).
Where relevant, we have also considered the health privacy principles (HPPs), as well as the right to privacy in the Charter of Human Rights and Responsibilities.

Inherent in our analysis is a set of questions that must be asked of each IPP:

• Will the project comply with this privacy principle?
• Will the project meet community expectations about this privacy principle?
• What else can be done to minimise risk and maximise protections in relation to this privacy principle, without compromising the project's objectives?

Against each privacy principle, recommendations are made to maximise the privacy enhancing possibilities, and/or minimise the privacy invasive risks of the Ultranet project. Our recommendations have been prioritised in terms of importance, on a scale from Desirable through Important to Critical.

Chapter 4 includes further recommendations relating to the privacy control environment – the policies, procedures and structures which affect accountability for privacy compliance.

Findings: the privacy impacts

The Ultranet delivers a significant privacy positive outcome for students, through the easy access that will be afforded to students (and their parents on their behalf) to all the data held about them in relation to attendance, teacher observations, progress and achievements.

There are also some negative privacy impacts – or privacy risks - of the Ultranet, as it is currently designed. However we believe that each one of these risk areas can be mitigated in part or in whole, without significantly affecting the Ultranet's objectives.

Strategies to address these risks include some system design changes, the development of comprehensive materials to communicate with users about their privacy rights and responsibilities to others, and the development of robust policies and procedures to support the Ultranet project. We have made 49 recommendations across Chapters 3 and 4, which we have grouped together here and in Chapter 5 under seven themes.

An Ultranet User Guide

There are a number of ways in which personal information will be collected, used and disclosed via the Ultranet, each of which requires some notification to the subjects of that personal information. Users will also need to develop some understanding of what steps they can take to protect their own privacy, as well as their responsibilities to protect other people's privacy.
Examples include:
• notification about the use of school photos in the Ultranet
• notification about the use of demographic data in the Ultranet
• notification about the collection of Household and sibling link information
• notification about the collection and storage of data by CSG, including the Helpdesk
• notification about audit logging of teachers' use of the Ultranet
• explanation of who can see what data in the Ultranet, and
• explanation of what is and is not appropriate use of the Ultranet.
Privacy notices are often drafted in overly legalistic terms, and thus tend to be ignored by the audience for whom they are intended. Even the terms 'privacy notice' and 'privacy policy' tend to make most people's eyes glaze over.

We have therefore suggested the development of a single Ultranet User Guide, which would incorporate all of the above legal requirements, as well as guidance for users on both the technical and normative (appropriate behaviour) aspects to using the Ultranet.

We have set out, in Appendix A, a suggested table of contents for an Ultranet User Guide. The suggested contents are intended to meet the Department's various legal obligations, but in a format that should be useful and interesting to Ultranet users.

Recommendations 3, 7, 8, 9, 10, 11, 12, 21, 36, 37 and 41 relate to the development of an Ultranet User Guide and its suggested contents.

Preventing misuse of student data

One of the Ultranet's strengths is its ability to collect, collate and succinctly display a rich variety of data about students. However as with any store of value, some people will be tempted to misuse that data for their own purposes.

The challenge for the Ultranet project is to design a means by which to minimise the risk of misuse of student data, without unduly restricting access for those staff who have a legitimate need to access the data.

We have recommended a business rule to define legitimate access:
The only purpose for which teachers may use student data from the Ultranet is when it is necessary to enable the teacher to fulfil their official teaching or pastoral care duties to that student.

We have also recommended a set of access controls, supplemented by transparency and audit logging of access, to enforce that business rule.

Recommendations 13, 14, 15, 30 through 35 and 46 relate to preventing the misuse of student data.

Addressing social networking risks

The eXpress Landing page in the Ultranet is designed to work much like a typical social networking site, with users able to write comments and upload material as a form of communication and self-expression.

There is a significant privacy risk posed by the eXpress Landing page, which is that by hosting a social networking site, the Department will be collecting all manner of personal information about users (and indeed the personal information of third parties about whom users might write or upload images), without the Department having any need for that information. This is contrary to the first privacy principle, which states that government agencies may only collect personal information that is necessary for their lawful functions.

The eXpress Landing page may also facilitate the posting of material by or about third parties, which could breach a third party's privacy or copyright. The use and disclosure of material found on an eXpress space will be difficult for the Department to control.

Thus the very existence of this ‘space’ may increase the risk of other types of privacy breaches.

We have recommended the removal of the eXpress Landing space. In the alternative, we have recommended some changes to minimise the risk of other privacy breaches.

Recommendations 1, 19, 20 and 22 relate to eliminating or minimising the privacy risks posed by the eXpress Landing space.

Ensuring lawful authority to collect or use personal information

There are some specific legal restrictions around the use of the Victorian Student Number (VSN). We have recommended immediate action to clarify and progress the ability of IDAM to use the VSN to provision student identities into the Ultranet.

Some existing forms will also require minor amendments to their privacy notices, to ensure the subjects of personal information understand how their personal information will be used in relation to the Ultranet.

To protect the Department from the risk of breaching the ‘Direct collection’ privacy principle, users uploading material to the Ultranet will be required to certify that they have the appropriate permission if someone else’s personal information is included in the material. We have recommended some wording for the certification screen.

Recommendations 2, 4, 5, 6 and 16 offer mechanisms to ensure legal authority exists before personal information is collected or used in relation to the Ultranet.

Other small steps to minimise the risk of privacy breaches

We have suggested a number of ways in which minor adjustments can be made to improve privacy protection, such as:
• the use by CSG of only masked or dummy data in the development and test environments
• the use of time-outs and maximum session times, and techniques to prevent users from saving their usernames and passwords in their internet browsers
• collecting only month and year of birth, instead of the precise date of birth of students, for use in reporting
• ensuring corporate users generating reports cannot identify individual students, by limiting report parameters to groups larger than five individuals,
and
• ensuring there are effective policies and procedures for schools and CSG to manage requests from law enforcement agencies and other third parties for data from the Ultranet.

Recommendations 17, 18, 23, 24, 25, 27, 28, 29 and 40 each offer a way in which a minor adjustment can be made to improve privacy protection.

Setting effective data retention periods

Marks and observations that were once written only on returned homework will now be kept in the Ultranet. This poses a temptation for that data to still be used when it has become out of date, or is no longer presented in context. For students, this poses a risk that negative information persists beyond its 'use by' date, and results in typecasting of that student.

This data quality risk is best resolved through well-considered data retention periods, to ensure that data is disposed of – or at least rendered 'invisible' to Ultranet users – once it is no longer serving its primary purpose.

We have recommended the development of data retention rules for the Ultranet, and we have suggested some appropriate time periods after which data should become 'invisible', and time periods after which data should de deleted.

Recommendations 42 through 44 relate to data retention and disposal.

Project transparency, assurance and governance

Privacy obligations are only as effective as their implementation and enforcement. Effective project oversight is critical to ensuring privacy protections will be upheld throughout the life of the Ultranet project.

We have suggested a number of measures be taken to ensure privacy and data security are effectively managed, now and into the future, such as:
• an immediate independent Information Security Threat and Risk Assessment of IDAM and the Ultranet
• a yearly independent audit of information security
• a clear chain of communication and action in the case of a data security breach
• a post-deployment oversight committee, including the appointment of an Ultranet Privacy Officer or involvement of the DEECD Privacy Unit, and
• the publication of this PIA Report.

Recommendations 26, 38, 39, 45 and 47 through 49 relate to ensuring the effective transparency, oversight and governance of the Ultranet project well into the future.

Glossary and acronyms

Charter	Victorian Charter of Human Rights and Responsibilities
Child	a person under the age of 18 years
DEECD	Department of Education and Early Childhood Development
ESL	English as a second language
ETR Act	Education Training and Reform Act 2006 (Vic)
ETR Regulations	Education Training and Reform Regulations 2007 (Vic)
FUSE	Find, Use and Share quality Education: FUSE is a repository of digital content and resources for use by teachers and students
GUID	globally unique identifier – in this case, a 32-character
unique number	generated by IDAM for the purpose of identifying individual users of the Ultranet; the VSN will be used by IDAM to disambiguate students prior to creating the GUID
HPPs	health privacy principles, found in the HRA
HRA	Health Records Act 2001 (Vic)
ICT	Information and Communications Technology
IDAM	Identity Access and Management System - the Department's identity solution system
IPA	Information Privacy Act 2000 (Vic)
IPPs	information privacy principles, found in the IPA
LDAP	Lightweight Directory Application Protocol - an industry standard protocol for managing directory services. In this case, LDAP will be used to provide usernames and passwords from IDAM to the Ultranet.
Learning Contact	A Learning Contact is like a 'friend' on a social networking site: a fellow user with whom you share reciprocal special viewing and editing rights over your eXpress Landing space.
OGSE	Office for Government School Education
OSL	Oracle Student Learning; in the Ultranet this functionality is known as Learning Tasks
parent	a child's natural parent, step-parent, adoptive parent, foster parent, guardian, or any other person who has custody or daily care and control of the child
personal information	any information about an individual whose identity is apparent or can reasonably be ascertained from the information
PIA	Privacy Impact Assessment
Portfolio Viewer	A Portfolio Viewer is a user with viewing and posting rights over another user's eXpress Learning Goals and Learning Portfolio pages
PSM	Protective Security Manual, a government policy issued to all Australian Government agencies which includes principles, standards and procedures for the protection of government personnel, infrastructure and information
SIB	Student Information Bus – contains data from several sources including the CASES21 mirror
SIF / SIF-AU	Systems Interoperability Framework; an international standard protocol for sending school data. SIF-AU 1.0 is an Australian version to be used to send XML messages to the Ultranet.

SSL	Secure Socket Layer connection – a protocol used to encrypt data over the internet
TRA	Threat and Risk Assessment
VELS	Victorian Essential Learning Standards - State standards for all teaching, from Prep to Year 10.
VSN	Victorian Student Number
VSR	Victorian Student Register
ZIS	Zone Integration Server – an interoperability platform which allows DEECD to receive data from multiple sources, consolidate it, and send it on to the Ultranet. ZIS is an XML broker, and will ‘push’ data to the Ultranet by way of SIF messages.

OVERVIEW OF RECOMMENDATIONS FROM THE PIA REPORT AND SUMMARY OF DEECD ACTIONS TO ADDRESS THEM

Rec		Importance	Updated Actions
1	That the eXpress landing page functionality be removed from the Ultranet (or as an alternative, action Recommendations 19, 20, 22 and 35).	Important	eXpress landing page is accessible only by the student. Learning Contacts functionality has been removed. Feasibility of reinstating this functionality for senior secondary students will be investigated at a later date.
2	That the design of the Ultranet ensure that before users can upload objects to the Ultranet, they are first asked to certify that they have permission to publish that material if it contains information about (including images of) other people. **Note** The wording used should warn users that they can only publish personal information about another person if they have the consent of the other person, or if the information was drawn from a generally available publication or a document kept in a library, art gallery or museum for the purposes of reference, study or exhibition. It should also note that when relying on consent, if the personal information includes health information or sensitive personal information (information about a person's sexuality, ethnicity, race or religion, criminal record, trade union membership, political opinions and membership, and philosophical beliefs), the subject's consent must be express, not just inferred or implied. The warning note should ideally also include a link to the Ultranet Support Page and more information about privacy and copyright	Important	Warning for students and teachers prepared. Appears whenever content uploaded. All users can access privacy information from each page of the portal.
3	That prior to, or at the same time as, receiving their Ultranet account details, students and staff be notified how their existing personal information will be used in the Ultranet. **Note** Elsewhere we have recommended the development of an Ultranet User Guide (see Recommendation 9). The privacy notice explaining how existing personal information will be used in the Ultranet could be included in that User Guide.	Important	Will be included in User Guides for students, parents and staff, and in PowerPoint presentation to be delivered by schools to all staff
4	That prior to the 2011 school year, the DEECD template student enrolment forms be amended to reflect how personal information collected on those forms will be used in the Ultranet.	Important	Privacy notice accompanying enrolment form will include information about how personal information will be used in the Ultranet. Amendment of notice in progress with assistance of Legal Services. Opt out process for photos will be included in current documentation schools use re photo day permissions as detailed in rec 6.

5	That prior to the 2011 school year, DEECD staff employment forms be amended to include a privacy notice to reflect how personal information collected on those forms will be used in the Ultranet.	Important	Work in progress with HR and Legal Services to include in staff employment forms/accompanying privacy notice
6	That as a matter of priority, DEECD provides schools with a template privacy notice pertaining to Photo Day, which explains that students and staff may 'opt out' of having their photograph used in the Ultranet. DEECD should also supply schools with guidance on how to adjust the Cases21 flag when individuals opt out. **Note** We have provided separate advice to DEECD by way of draft wording of an advice to schools and template privacy notice with respect to Photo Day.	Important	Details of opt- out process will be provided in Parent User Guide to be distributed with Ultranet Welcome Letter. Opt out process for photos will be included in sec 6 of schools reference guide with a link to updated advice on school photos developed by Privacy unit and a link to the same advice on the Connections 2010 site
7	That prior to, or at the same time as, receiving their Ultranet account details, parents be notified how the personal information they supply will be used in the Ultranet to create a link between siblings, and what option they have to prevent this.	Desirable	Details will be provided when parents self-register with IDAM to access the Ultranet.
8	That the helpdesk page include a privacy notice for users seeking to access the Helpdesk. The privacy notice will need to explain that their Helpdesk call or online enquiry will be going to CSG not DEECD, and that any personal information they provide as part of their Helpdesk enquiry will be going out of Victoria to the CSG's Helpdesk in the ACT. **Note** Elsewhere we have recommended the development of an Ultranet User Guide (see Recommendation 9). The privacy notice to users with respect to the Helpdesk should also be included in that User Guide.	Desirable	All User Guides will include the following statement: 'The Ultranet Helpdesk is located in the ACT. Transmission of any information submitted as part of a query will comply with privacy requirements using trans-border data flow guidelines.'
9	That a single Ultranet User Guide be developed, to cover all users, which incorporates the necessary privacy notices and other privacy-related advice, as well as instructive material, as set out in Appendix A. **Note** See Appendix A for a suggested Table of Contents for an Ultranet User Guide.	Critical	Teacher User Guide completed Parent User Guide to be completed beginning September Student User Guide to be completed mid June
10	That the Ultranet User Guide (see Recommendation 9) also be made available in common community languages and in a screen-readable format for users with visual impairment.	Desirable	Parent User Guides will be provided online in common community languages and in in screen-readable format
11	That the Ultranet User Guide (see Recommendation 9) be made available to read in HTML and as a PDF download from the Ultranet site and that a link to the relevant page on the site be easily available to users from the Helpdesk page and by navigating from the privacy statement appearing on all pages on the site.	Important	All User Guides will be available as PDF downloads from the Ultranet site. Teacher User Guide can be downloaded now. Link to privacy statement is active on all Ultranet pages.

12	That prior to, or at the same time as, receiving their Ultranet account details, all users be given a copy of (or the URL of) the Ultranet User Guide, and informed that the Ultranet User Guide contains important privacy information they should read before they begin.	Important	URL will be included in Welcome Letters.
13	That DEECD adopt the following as an Ultranet business rule: The only purpose for which teachers may use student data from the Ultranet is when it is necessary to enable the teacher to fulfil their official teaching or pastoral care duties to that student.	Critical	Included in Teacher User Guides and in Powerpoint presentations that all schools are required to use with staff
14	That DEECD enforce the Ultranet business rule (see Recommendation 13) by means of access controls (see Recommendation 30) and audit logging (see Recommendation 35).	Critical	See recommendations 30 and 35 below
15	That DEECD document the Ultranet business rule (see Recommendation 13) in the Ultranet User Guide (see Recommendation 9), and further reinforce the message through staff training.	Critical	All schools are required to deliver Powerpoint presentation to all staff
16	That as a matter of urgency, DEECD seek legal advice on whether the use of the VSN for the purposes of provisioning identities in the Ultranet meets the legislative provisions in relation to authorised persons and purposes and if necessary that DEECD arrange the Secretary's authorization and publication of that authorisation in the Government Gazette.	Critical	Legal advice has been sought and confirms that the use of the VSN use for provisioning identities in the Ultranet is for a prescribed purpose and complies with legislative provisions
17	That DEECD require CSG to design the report-writing feature of the Ultranet such that if the size of the report results would contain data on less than five individuals, the report-writing feature will generate an error message that informs the user that the sample is too small to ensure anonymity of the subjects, and they should therefore alter their desired report parameters.	Desirable	This has been incorporated into Release 2 Business Requirements.
18	That DEECD alter the SIF message specifications to use only mm/yyyy (or 01/mm/yyyy) instead of dd/mm/yyyy for students' date of birth.	Desirable	To be implemented in Release 2
19	That DEECD ensure that the Learning Contact relationship remains a voluntary relationship, entirely at the user's discretion. **Note** This recommendation is only needed if Recommendation 1 (delete the eXpress Landing page) is not followed.	Desirable	No longer applicable
20	That DEECD require CSG to ensure that the default setting on the eXpress Landing page is for the user's list of Learning Contacts to be hidden from view. **Note** This recommendation is only needed if Recommendation 1 (delete the eXpress Landing page) is not followed.	Important	No longer applicable

21	That students be clearly informed about what data their parents can see about them via the Ultranet. **Note** Elsewhere we have recommended the development of an Ultranet User Guide (see Recommendation 9). The privacy notice to students explaining how their parents can see their data could be included in that User Guide.	Important	Will be included in Student User Guide
22	That the design of the Ultranet ensures that parent users cannot see their child's eXpress Landing page. **Note** This recommendation is only needed if Recommendation 1 (delete the eXpress Landing page) is not followed.	Important	No longer applicable
23	That DEECD advise schools to manage requests from any third parties for data from the Ultranet in accordance with the policy relating to law enforcement requests – namely, to ask the third party to put their request in writing, and for the school to then seek advice from either the privacy, legal services, student wellbeing, or conduct and ethics unit of the Department.	Important	DEECD policy exists and will be reinforced. Details of process schools must follow are provided in Protecting Information (Access and Correction), Bulletin 7, February 2007, www.eduweb.vic.gov.au/privacy/
24	That DEECD develop a policy for CSG to handle requests from any third parties for data from the Ultranet. The policy should ensure that CSG obtains any third party request in writing, and contacts the legal services unit of DEECD for advice before responding to the request. The policy should include procedures for requests received outside of normal DEECD office hours.	Important	DEECD policy exists re handling requests from third parties for access to DEECD data. Policy will form basis of procedures to be provided to CSG. Process will be included in CSG operational support procedures.
25	That DEECD ensure that CSG only use masked, scrambled or dummy data in the Ultranet development and testing environments.	Important	This is current practice
26	That DEECD commission an independent Information Security Threat and Risk Assessment to examine both IDAM and the Ultranet (including the Ultranet Helpdesk) prior to deployment. **Note** The IT Division of DEECD should be involved in setting the terms of reference for the ISTRA, and in evaluating the quotes or tenders obtained. The ISTRA should include penetration testing, a review of the information security classification conducted by CSG, and a review of the arrangements under which usernames and passwords are stored across three locations.	Critical	In progress
27	That DEECD require CSG to implement a password-protected time-out function, and a maximum session time function, for users of the Ultranet.	Important	15 min password protected timeout function and 4 hour maximum session time function implemented.

28	That DEECD require CSG to prevent browsers from using AutoComplete settings that would otherwise allow users to save their Ultranet username and password. **Note** While an 'Important' risk for Release 1, this recommendation becomes 'Critical' with respect to Release 2.	Critical	Functionality is in place
29	That DEECD issue instructions to IDAM Administrators that Welcome letters for new users of the Ultranet must be mailed or handed personally to each user.	Desirable	Schools will be advised of the issues around delivering welcome letters. It should be noted that IDAM requires verifying information from new users such as date of birth. From 2011, Welcome letters will be provided to parents as part of student enrolment process.
30	That DEECD instruct CSG to develop access controls in Learner Profile and Learning Tasks, such that: (a) for students identifiable (through the class timetabling data) as 'my students', a teacher can: • see detailed VELS progress • see collated absence data • see collated Observations • see learning items created by any teacher • create learning items • see items submitted by students against the learning items he/she created, and • create / edit feedback (assessments, Comments and Observations) against the learning items he/she created. (b) for students who are not 'my students', against whom the teacher selfselects as a Portfolio Viewer, a teacher can: • see detailed VELS progress • see collated absence data • see collated Observations, and • see learning items created by any teacher.	Critical	Solutions that will address this issue and recs 31-33 and 35-36 are being explored with CSG. Solution will be in place for Release 2.
31	That DEECD instruct CSG to create a new user group, 'school counsellor', who may have read-only access to VELS progress, collated absence data and collated Observations data about students. This access should ideally be on a self-selecting basis (i.e. only for students against whom the school counsellor has self-selected), so long as the fact of self-selection is hidden	Important	See rec 30

	to users other than the school counsellor and the subject student.		
32	That DEECD instruct CSG to ensure that all 'school counsellor' roles expire on 31 December each year.	Important	See rec 30
33	That DEECD issue instructions to School Principals and IDAM Administrators on how to provision a 'school counsellor' user, and the very limited circumstances in which this access role should be granted.	Desirable	See rec 30
34	That DEECD instruct CSG to ensure that all Portfolio Viewer roles expire on 31 December each year.	Important	Included in Release 2 Business Requirements.
35	That in addition to the standard logging of all create / edit / delete actions, there should be audit logging of read-only and print access by staff users to the Learner Profile and Learning Tasks spaces. **Note** This recommendation becomes 'Important' rather than 'Critical' if Recommendation 30 above is accepted.	Critical	See rec 30
36	That staff be warned about the use of audit logging to identify any examples of misuse of student data, including inappropriate browsing or printing of data. **Note** Elsewhere we have recommended the development of an Ultranet User Guide (see Recommendation 9). The privacy notice explaining how staff access will be logged in the Ultranet could be included in that User Guide.	Important	See rec 30
37	That users be warned to protect material printed about a student from the Ultranet, and not to share the printout with a third party without the student's (or their parent's) consent. **Note** Elsewhere we have recommended the development of an Ultranet User Guide (see Recommendation 9). The warning to users about printing data from the Ultranet could be included in that User Guide.	Important	Included in Teacher User Guide. To be actioned for Parent and Student User Guides.
38	That DEECD require CSG to commission a yearly independent audit of information security, including an audit of access to data by 'sysadmins', with the audit results to be reported to DEECD's ICT division.	Important	DEECD to commission independent audit
39	That DEECD establish a clear and documented chain of communication in the case of Ultranet data security breaches, as follows: CSG to notify OGSE and ITD; ITD to notify the Privacy Unit if there is personal information involved; the Privacy Unit to follow the Privacy Victoria guidelines in relation to notifying the Privacy Commissioner and/or the data subjects.	Important	ITD Risk Unit will provide CSG with written process to follow that aligns with current practice and includes notification to Privacy Unit.
40	That DEECD instruct CSG to remove the ability for teachers to make Observations 'internal'; all Observations recorded about a student in the	Important	To be included as part of Release 2 Business Requirements.

	Ultranet should be easily accessible by the student and their parents.		
41	That teachers be warned not to make any Comments or Observations that are unsubstantiated, based on hearsay, misleading, out of context, or irrelevant to a student's learning. **Note** Elsewhere we have recommended the development of an Ultranet User Guide (see Recommendation 9). The warning to teachers about the use of the Comment and Observation fields could be included in the User Guide.	Important	Included in Teacher User Guide.
42	That the OGSE work with the DEECD Document and Records Manager to develop a set of interim data retention rules, to form the basis of instruction to CSG. **Note** We have suggested a set of data retention rules above.	Important	This is being addressed through non-functional requirements. CSG has appointed a BA to be responsible for capturing DEECD's retention and disposal rules and processes
43	That the DEECD Document and Records Manager ensure the review of the Schools Retention and Disposal Authority in 2011 incorporates user-generated content stored in the Ultranet.	Important	As above
44	That the OGSE work with the DEECD Document and Records Manager and the ICT Division to develop a set of secure data disposal rules, to form the basis of instruction to CSG.	Important	As above
45	That a strategy be developed for post-deployment project oversight, incorporating the appointment of an Ultranet Privacy Officer or involvement of the DEECD Privacy Unit. **Note** We have suggested some duties of an oversight committee, above.	Important	Current Ultranet Board to determine details of process
46	That prior to deployment of Release 2, a demonstration version of Release 2 be developed and tested with separate focus groups of teachers, students and parents, to test community expectations with respect to teachers' access to student data in the Learner Profile and Learning Task settings.	Important	Not feasible within timeline.
47	That this Report be provided to the DEECD Privacy Unit.	Important	Actioned
48	That this Report be provided to the Victorian Privacy Commissioner.	Important	Actioned
49	That this Report be published on the DEECD website, with a link from the Ultranet Support page.	Important	Report summary will be published on Ultranet website, June 2010