

A CALL TO

Web Based Learning Systems (WBLS) hold great potential for making the University's resources more broadly available. This ARMS Bulletin describes WBLS and the various legal and records management issues for the University.

CONTENTS

Introduction—Web Based Learning Systems.....	1
WBLS and Legal Issues.....	1
Records Management Issues.....	2
Conclusion.....	5
Appendix—Records Keeping Guidelines.....	7

INTRODUCTION – WEB BASED LEARNING SYSTEMS

In August 1998, an issues statement on Web Based Learning Systems (WBLS) was prepared to make the University community aware of its legal responsibilities but also to provide a basis for 'risk assessment' in the WBLS environment. Most of the items addressed in this issues statement fall under the areas of Infrastructure Requirements, Interoperability, Electronic and Print Resources, and Evaluation and Value of WBLS as outlined in the January 13, 1998 Architecture group minutes.

http://www.wisc.edu/arch/task_force/wbls/

We can not hope to anticipate every eventuality that may occur in Cyberspace, but we can do our best as an institution to promote sound policy guidance and awareness of the issues and potential problem areas.

WBLS AND LEGAL ISSUES

There are numerous existing State and Federal records that impact electronic records. Wisconsin's Public Records Law and Open Records Law recognize electronically formatted documents to be "records." As such, they are subject to the same requirements as all other records stored on other types of media. Some of these requirements are outlined in other sections of this document. Electronic records are subject to

discovery and rules of evidence as are all other types of records. There are numerous Federal and State laws that impact specific types of records and information. The significant factor to remember is that these laws apply regardless of the type storage medium being used.

Developments in information technology have created a wide variety of legal concerns, and in general, records laws have not kept up with them. There are a variety of legislative efforts underway at State and Federal levels which predominately relate to strengthening privacy laws as they apply to information technology area. Recently, a Wisconsin State task force was created that will propose an administrative code on electronic records. The code is not likely to address specific technologies or storage media, but will govern the application of traditional records and information management practices in the electronic environment.

One legal area that is starting to catch up is authentication. Basically, this area addresses the question of how do we know a record when we create one or receive one? Traditionally, organizations have relied upon the paper copy of the record. In an all-electronic information system, retaining the paper record is not sufficient because it does not contain all the information about the record necessary for it to be a 'complete, accurate, and reliable record.' Several states have now enacted legislation enabling the use of electronic signatures. In addition to the use of electronic signatures, organizations need to be aware of record keeping requirements that can attest to the authenticity of the document. See ARMS Bulletin #2, "Creating Electronic Records" for further information about issues in this area.

RECORDS MANAGEMENT ISSUES

Records and information management issues in WBLS fall into the following categories:

- A. Access including security / privacy
- B. Appropriate use
- C. Authentication
- D. Retention and Disposition
- E. Preservation

A. Access, Including Security / Privacy

In this category, the University has obligations under both Federal and State laws. Any time student information is involved FERPA, the Family Educational Rights and Privacy Act, must be adhered to. This Federal law is very explicit regarding the management of student data and most particularly about accessing student record information. This includes forbidding such things as digitized photos of students placed on the Net without permission. Generally, it forbids disclosure without the student's written consent.

In addition to FERPA, we have State of Wisconsin laws relating to privacy and the maintenance of personally identifiable information. Wisconsin Statutes Chapter 19 outlines agency responsibilities with regard to the management of personally identifiable information including: development of rules of conduct, providing training to employees who manage such data, data collection responsibilities, and the use of computer matching programs. (Personally identifiable information means information that can be associated with an individual through one or more identifiers or other information or circumstances. While the computer matching programs provision might not be of direct application in WBLS, it should be noted that any type of student identifier used, or granting access to, an identifier could provide capability to do computer matching.

Wisconsin law also requires a notice on State agency forms that describes why information is being collected and the consequences for failure to complete the form. This notice requirement is receiving increased attention as forms are being added to Web based environments.

In the near future, we are likely to see increased attention paid to individual privacy and the Internet. For instance, recent legislation in Wisconsin introduces severe penalties for 'stealing another's identity.' It is imperative that great caution be exercised in expanding our use of the Internet, particularly the portions of WBLS that will administer and communicate personal identifiable data.

Recommendations: Access, Including Security/Privacy

- The University should adopt a privacy/access policy that will be featured prominently on the initial WBLS homepage screens, or accessible via a hot button that links directly to the policy statement.
- Notice of policies on access to student information should also be a part of the sign on screen whatever WBLS technology is used. The policy should indicate that absolute privacy can not be guaranteed but all reasonable precautions in both policy and technology have been undertaken. It should state that information that is requested and gathered/collected is limited to that which is needed for the participation and completion of the on-line course. If information will be retained and used for research purposes that should be noted at sign on as well. The Registrar's office, as managers of the official UW student record data, should review their current access policy to determine its applicability to WBLS systems.
- Monitoring or logging features of WBLS must protect student privacy. Information technology staff need to determine the minimal amount of information they need to collect to manage appropriately without compromising student privacy. [Jeffrey Savoy, DoIT Security Investigator is developing a retention proposal for security logs maintained on student computer accounts. This same policy could potentially be extended to logs maintained as part of a WBLS system because it is student related.]
- Policies need to be developed for those University staff who will be involved in WBLS to outline levels of responsibilities for data collection and distribution, especially concerning the collection of names, addresses, personal identifiers, grades, etc. that can be attributed to one individual. These procedures should include methods that will permit users to access their own records and correct misinformation or incorrect information. The policy should also address any secondary use of the data collected.

As an example, the Conference Leader Responsibilities statement developed for the use of the First Class Conference software meets many of these requirements and with modification could be used as a model for other WBLS technologies. The developers of this statement have already taken some of these issues into consideration.

- When WBLS is used by several institutions to collaboratively teach a course, adequate security precautions must be in place to insure the privacy of student record data transmitted between institutions.

B. Appropriate Use

Appropriate use involves two concepts: identifying the right technology tools to support a specifically identified need, and limiting the use of technology tools to those purposes that support the mission of the University. The Board of Regents at its June 1997 meeting adopted a "Policy on Use of University Information Technology Resources." This policy statement should be referenced with regard to limitations on use of Information Technology Resources.

WBLS systems will be applied to enhance and extend University learning resources to a broader community. WBLS users should be aware of the principle of minimization when collecting student related data. This principle states the least possible amount of student information should be collected to meet a legitimate institutional purpose. It requires that the institution identify what it minimally needs to collect, and refrain from collecting that which might 'be nice to know' or data that 'might be used in the future.' The rationale is that the risk of misuse increases when an organization starts collecting student related data more broadly than needed (and much of this falls in the personally identifiable category); obviously, in a Web based environment there is greater potential for misuse to happen than with closed paper files.

Recommendations: Appropriate Use

- The student related data elements that will be collected should be identified and WBLS should limit the collection of student data to those elements. A statement should appear on data collection screens that advises students of the purposes for collecting student information. [See recommendations in Access section.]

The collection of student record data should be coordinated with the Registrar's office since that office is the holder of official student record data for the University.

- The Regent Policy on the Use of Information Technology Resources should be referenced on the sign on screen to WBLS systems.
- A records retention disposition schedule should be developed for the student data in WBLS systems. The schedule should be referenced in the notice to students. See retention/disposition section below.

C. Authentication

In the electronic environment it is important to know 'how do I know what I really have?' How do I know that what I have received electronically is actually coming from a specific individual? Passwords, encryption, and digital signatures are used to authenticate electronic records. Obviously, the issues of authentication related very closely to security, access, and privacy issues but detailed discussion is beyond the scope of this document.

D. Records Retention and Disposition

WBLS systems will create and maintain records; and therefore, they will need to be managed in accordance with Wisconsin's public records laws and appropriate Federal laws. One of the basic elements of Wisconsin's Public Records Law is the requirement for records retention schedules or Records Retention Disposition Authorizations (RDAs). The RDA is the schedule document which is reviewed and approved at the campus level by the Campus Records Review Group and at the State level by the Public Records Board. A records schedule describes a particular records series and prescribes a retention period and disposition for it. A records schedule, once it is approved by the Public Records Board, is a legal document and demonstrates that the institution has analyzed the value of the records and data and has a consistent plan for their management.

The information in WBLS falls currently into three broad categories:

- Administrative educational records (i.e. student records)
- Information resources such as course outlines, handouts, instructional materials
- Course materials submitted by students.

Administrative records and course materials submitted by students would be considered official University records and subject to retention and disposition policies. Informational resources form a gray area. While course outlines and other materials are produced as part of performing the teaching function and therefore part of official University activity, these documents are often treated as faculty papers and not formally scheduled for retention and disposition.

Recommendations: Retention and Disposition

- The collection and retention of student record data must be coordinated with the Registrar's office. The Registrar's Office is the holder of official student record information. Policies and technological procedures need to be addressed that will define the relationship between the student record data base and WBLS systems. Technological procedures

should address how administrative data, grades, and courses will link to the main Registrar database.

- Retention and disposition policies must be factored in during the planning process. The Administrative Rule currently under development at the State level will likely mandate that retention and disposition be a component of systems at the conception stage. The technological enhancements needed to implement these policies are more easily and efficiently accomplished at the front end of systems planning than by after the fact customization.
- A number of campus wide as well as department specific records retention policies exist. Similar records managed by WBLs systems must comply with those existing retention requirements.

The following is a list of current campus-wide retention policies in the area of student records. NOTE: Many of these policies have sunset as per Stat. 16.61 (4) c., but they continue to serve as campus policy. The Registrar's office and others have been notified of the need to update these retention policies and revision efforts have been initiated. The implementation of ISIS has delayed development and consideration of retention issues.

RDA# 57 Outlines the informational content of the official student records and specifies that it will be retained permanently.

Supporting documentation and copies of student record documents are governed by RDA# 130/84.

RDA# 62 governs Graduate School Application files.

RDA# 377 governs Graduate Student Records-completed.

- Records in WBLs systems not covered already by either campus-wide or department specific retention policies must have appropriate retention policies prepared and submitted for approval.
- Appropriate disposition processes must be applied to the backup tapes to insure the complete deletion/erasure of data. It is recommended that separate backup procedures be applied to WBLs systems.

- Retention and Disposition requirements must be applied to E-mail if that is used and/or incorporated as a feature of WBLs systems.

E. Preservation

Some information maintained in WBLs may have long term retention value; particularly those informational resources that will be used again or in other WBLs courses. The UW may have a history of education need to secure some WBLs records to support research. The University Archives is currently developing an electronic archives policy for the campus. Of key importance in this area is the development of migration strategies for those informational components of WBLs that need to be moved forward as software and platform changes occur.

Recommendations: Preservation

- Faculty members will want to be apprised of preservation procedures so that materials such as course syllabi, handouts, etc. created and published on-line remain accessible to them for additional courses.
- To implement retention and preservation, WBLs systems should separately track the three basic categories of information.
- Preservation of student records beyond those needed by the Registrar's Office. Are there pieces of data that WBLs developers may want that are beyond those needs of the Registrar's Office?
- With preservation there are also additional questions about access. Is there access under FERPA to student record data that may be maintained by faculty members? This may be an awareness issue more than records management policy issue.

Other Issues and Recommendations

- Evaluation of WBLs courses may have implications for the faculty evaluation process. If on-line evaluations of courses are conducted, that information should be tracked and retained separately in accordance with the faculty and Academic Staff Personnel Records Retention Policy.
- Policy documents and other informational resources should be available as core documents for all potential WBLs users. Items such as privacy policy, ARMS bulletins, Board of Regents IT Policy, responsibility statements (First Class model), security policy, etc. should be established as guidance standards and

made available for all those contemplating WBLS system applications. Some of these items should be identified as minimum requirements for access to WBLS resources. Others should be identified as guidance for planning and implementation.

- Courses and educational program jointly sponsored with other institutions. In the joint agreements creating shared courses or jointly sponsored programs, such issues as ownership of records and information and liability ought to be address.
- Educom IMS Specification. The Educom Instructional Management Systems, IMS, specifications do address functional standards as they related to records 'creation' but are mostly silent about the corresponding need for record 'keeping.' [See <http://www.imsproject.org/specspr.html>].

These IMS requirements are going to make access for the general world easier to accomplish in a standardized fashion, but it will be incumbent upon the participating institutions to make sure their policies and technological requirements will mesh with those at the national level. Since records policies, such as those described in this issues statement, are largely missing from the IMS standards, we will need to define our own. How will our portion of the data, and of the metadata, be maintained at our institution? Who will be responsible for doing it? Who will see that things like policies, versions, re-versioning, etc. at our local level will be in synch with national policies?

The proposed standards are extremely useful, though, for their through systems analysis of the needs of distance education, for their delineation and definition of various processes and data elements, and not least because they define a common nomenclature for everyone to use.

It should be noted that the issues outlined in this document do not apply just to WBLS but reflective of non-paper based learning systems generally. The issues of access, appropriate use, security retention, and preservation will need to be addressed broadly as more nontraditional and technologically based learning systems are developed. It will be incumbent upon educational institutions to make sure that their local records and information management policies are in place, up to date, and consistent before launching into the global education environment.

CONCLUSION

This bulletin provides an overview of the records and information management issues in WBLS. Archives and Records Management Service is collaborating with DoIT on specific policies and procedures to address these important topics.

List of Major Points.

1. Awareness and Education.

As the University expands its role in providing Web based access to its educational resources, faculty and staff need to be aware of the records and information management risks inherent in using this technology and their responsibilities to minimize those risks to the greatest extent possible. State and Federal laws have generally not kept up with the developments in technology, but there are certain legal requirements that are valid regardless of the type of technology used to create and manage records and information. In the meantime we need to build awareness to these issues and provide guidance to faculty, staff, and students in terms of their responsibilities and what they minimally can do to avoid problems.

2. Ownership Issues.

With the potential for a great mix of records and information from a variety of sources being placed in a University supported technology, ownership issues will likely be of concern. We need to devise strategies and technological methods by which items can be delineated and separately managed and policies that will support those strategies.

3. Identity Theft.

This is a growing issue at the State and Federal levels. Policy statements need to make clear roles and responsibilities in terms of using the technology and accessing the information being created and stored in these technologies. Part of the solution in this area is strongly encourage University departments to collect only that information that is minimally needed to support a particular function or provide a service. The collection and possible access to student academic data is of special concern. The collection and use of student academic record data should be coordinated with the Registrar's Office since that office is the holder of official student record data for the University.

4. Authentication.

In the electronic environment, it is important to know "how do I know what I really have?" In other words, how do I know that the person identified as the sender is actually the sender. This is of concern in Info Labs and other areas in which computers are easily accessible and where there is high volume of traffic.

5. Retention and Disposition.

Web based learning systems like other electronic systems do create records, and as such need to be

appropriately managed including meeting the records appraisal and retention requirement. We need to provide guidance to faculty and staff on filing and classification schemes that will facilitate implementation of these requirements. The University will need to provide offices with the capability to implement retention and disposition requirements electronically.

Student records retention policies need to be updated. With the further use of Web based learning systems and the implementation of ISIS, these are issues are becoming critical to the protection of University interests in retention and preservation of student academic records and information.

6. Preservation.

Providing access to electronic information over time continues to be very problematic. The University needs to build awareness to this issue. Migration strategies need to become a common component information systems design.

These major points will be common to other electronically based information systems. Attention to them in a visible and emerging technological area such as the Web based Learning Systems area will greatly assist in addressing them elsewhere.

APPENDIX—RECORDS KEEPING GUIDELINES

1. Creation of records in WBLs

Several functions supported by WBLs will result in the creation of records because they will serve to document a transaction, whether that will be the enrollment in a course, completion of course requirements, issuance of grades, and others. It will be incumbent upon those administering a WBLs application to authenticate users (senders and receivers) and ensure that the reliability of the system can be documented, data can be accessed and retrieved in the normal course of business, and data maintained in WBLs is separately identified and maintained in accordance with the retention requirements outlined later in this document.

2. Data Collection

WBLs users are strongly encouraged to collect only that minimal amount of data necessary to carry out the prescribed function. If additional, non-course related data is collected from students, its purpose and use should be clearly noted to the participants at the outset.

If research use of WBLs is intended, particularly the collection of personally identifiable data, the user should check the campus Human Subject research guidelines to determine if other Federal reporting requirements apply. Certain categories of research are exempt from Human Subject reporting, but faculty are urged to read the Human Subjects Committee Guidelines for further information. Information collected from subjects for research purposes must be kept segregated from other WBLs data.

3. Placing Information on the Web

All users of WBLs are responsible for verifying the copyright status of information placed in WBLs supported applications. WBLs users are encouraged to follow appropriate content and style guidelines when placing materials on the Web. They must also follow University policies with regard to intellectual property and copyright. See UW System Financial and Administrative Policy (GAPP 27) Copyrightable Instruction Materials Ownership, Use and Control available at <http://www.uwsa.edu/fadmin/gapp/gapp27.htm>. WBLs users must be aware of copyright practices such as: fair use, rights clearance, and license. Additional copyright information is available at <http://www.wisc.edu/learntech/menus/copyrights.htm>.

4. Records Maintenance & Retention

- a. Records must be maintained and retained in accordance with existing campus-wide policies. The most likely cited retention policies are noted at the end of this document.
- b. Any records and data not covered by existing campus-wide retention policies must be appraised and scheduled as required by Wisconsin Statutes. Every effort will be made to develop campus-wide retention policies for WBLs to the greatest extent possible.
- c. All required systems documentation: program codes, data dictionaries, report descriptions, error logs, etc. must be maintained and kept up to date to support the retention and retrieval of records from the WBLs system until their retention life has expired. This requirement includes the ability to re-create records.
- d. On-line inactive records storage and archiving. WBLs users must identify the campus entity that will have responsibility for the storage of records outlined in this guideline. This responsibility could rest with department server, LAN administration, DoIT, other services.
- e. When retention times have expired, records are to be deleted from the system and from their backups.

5. Preservation

- a. Those records identified for long term preservation and which will be maintained in electronic format will need to have special care and handling to maintain their availability. It is advised that any data / records appraised to have value out beyond 3 years must have an identified migration strategy to ensure long term access and retrievability.
- b. Permanent student academic records data must be transferred to the Registrar's office for inclusion in the permanent student academic record.

6. Access & Retrieval

- a. The release of student record information is governed by FERPA, the Family Educational Rights and Privacy Act.

- b. Users are advised that Social Security Numbers are confidential and should not be used.
- c. All other information maintained in WBLS is governed by the Open Records law and faculty policies and procedures.
- d. Users are also cautioned about the incidence of identity theft. The collection of personally identifiable data, especially anything that can be used as a personal identifier, should be kept to a minimum and certainly not shared.

7. Security & Authentication

All users are responsible for identifying the appropriate level of authentication for the type of record/information being collected or transmitted. Users are cautioned that high end WBLS applications have the capability for a number of interactions which can include the collection and transmission of student academic information, some of which is confidential. Reference: 2.3.3 Levels of Authentication and 2.3.4 Security Administration. [Note: If current proposed legislation addressing electronic signatures is passed, an administrative rule on electronic signatures will be developed.]

If electronic signature technology is applied to areas within a WBLS application, consideration must be given to issues of access and retrievability past the conclusion of the particular course.

8. Categories of record data:

Student Records:

- a. Course materials submitted by students for a grade. RDA # 1081

This area would include electronically submitted papers, online quizzes /tests, electronically submitted assignments.

Retention: Retain 1 semester past the semester in which the course was taken and destroy/delete.

- b. Class Rosters RDA # 1082

Lists of students enrolled in the class.

Retention: The instructor is responsible for retaining the roster for 1 semester and destroy/delete.

- c. Final Grades Lists RDA # 1083

Final grades for the WBLS course. In WBLS, there is the capability for faculty to maintain the equivalent of a grade book; student name, ID code, and what other evaluative information the instructor determines to retain.

Retention: Destroy / delete 5 years from the semester in which the course was given.

- c. Correspondence / discussion group documentation. RDA# 1084

Correspondence and discussion group documentation captured in the form of e-mail messages, chat rooms, or other electronic forums.

Retention: Destroy/Delete one semester after course completion.

Course Evaluations:

- a. Student Evaluations & Summaries RDA # 712

High WBLS applications do have the capability to collect evaluative data on the course and course instructor.

Retention:

Tenured faculty: Retain 1 year from the end of the semester in which they are completed and destroy, provided a copy is transferred to the individual's permanent personnel file.

Probationary Faculty: Retain 6 years from the end of the tenure review process and destroy provided summaries are transferred to the individual's permanent personnel file.

TA's, Academic Staff: Retain 2 years from the end of the semester in which they were completed and destroy provided summaries are transferred to the individual's permanent personnel file.

Academic Administrative Information:

- a. Course syllabi and handouts. RDA # 657 &658

Retention: Destroy / delete after one set has been transferred to the UW Archives for preservation.

- b. Course materials reproduced and or prepared by the department originating the WBLS course. RDA #659

Retention: Retain until superceded and then destroy/delete.

WBLs Administrative Information: RDA # 1085

WBLs administrative information maintained by a WBLs user in connection the development and presentation of academic courses such as permission forms, copyright agreements, and other formal approvals or agreements.

Retention: Retain 5 years from the date the course concluded.

Documents used in the development of this guideline:

ARMS Bulletin #3

Board of Regents Policy on Use of Information Technology Resources

UW System Financial and Administrative Policy - Copyrightable Instruction Materials Ownership, Use and Control (GAPP 27)

Archives and Records Management Services

Main Office

B134 Memorial Library

728 State Street

Madison, WI 53706-1494

Phone: (608) 262-5629

Fax: (608) 265-2754

Recmgmt@library.wisc.edu

www.library.wisc.edu/libraries/Archives/

©1999, Board of Regents, University of Wisconsin-Madison
ARMS is a periodical bulletin from the University of Wisconsin-Madison's Archives and Records Management Services.