McGill

McGill University Archives

www.archives.mcgill.ca

Prepared by:
David Kemper
Archivist, Electronic Records

Date:
June 2005

Version No.:
1.1

McGill University Archives

digitalpermanence: Transfer and Access Protocols (electronic records)

Executive Summary

A wide range of McGill University functions is conducted electronically. The student application and registration process is among the range of activities now achieved either through enterprise resource planning systems (i.e. Banner), email, electronic documents, or web-based services.

In order to fulfill the McGill University Archives' (MUA) recordkeeping responsibilities, as well as provide researchers access to institutional electronic records, the MUA requires a comprehensive set of procedures or protocols that will ensure the acquisition, management, preservation, enduring access to and security of McGill University's electronic records.

The MUA's ***digitalpermanence*** initiative proposes a series of collaborative and strategic activities aimed at the long-term management and preservation of McGill University's institutional electronic records inside a ***digitalpermanence*** repository, a proposed secure storage area operating within McGill's information technology infrastructure.

This discussion document introduces electronic records protocols (as part of the ***digitalpermanence*** project) to a general audience, as well as to specialists in the fields of records management, archives, and information technology. This document outlines procedures for transferring and managing electronic records, including making them accessible to researchers, in the absence of an electronic document and records management system (EDRMS). The document will also however note the benefits that a records/document management application can bring to facilitate these protocols.

Version 1.1
June 2005

Protocols

digitalpermanence protocols are the proposed foundational elements to support the MUA's approach to managing electronic records.

1) Transfer: Process by which institutional electronic records are transferred from McGill departments, faculties and offices to the MUA;

2) Intellectual Controls/Processing: Series of intellectual control processes beginning with accessioning in-coming institutional electronic records, appraisal/application of the *McGill University Records Retention Schedule (MURRS)*, arrangement and description (or scheduling as part of the ongoing A/D backlog);

3) Preservation: Processes for migration of electronic records, depending on their retention schedule and/or long-term preservation strategy, from native file formats to a longer-term file format (such as XHTML or XML); and to research methods for electronic records preservation, ensuring their accessibility, authenticity and reliability throughout their retention period. Additionally, to prepare reference copies of e-records for research access;

4) Access: Processes for a convenient, secure means of disseminating electronic records to allow researchers access to electronic records stored in the ***digitalpermanence*** repository; and to acquire the necessary computer hardware and software to view these electronic records.

Document History

Version	Date	Author	Notes
Draft (0.1)	November 2004	David Kemper	Discussed with Johanne Pelletier and Gordon Burr
Draft (0.2)	January 2005	David Kemper	Discussed with Johanne Pelletier. Revised format and content arrangement.
Draft (0.3)	January 25, 2004	David Kemper	Discussed with Gordon Burr, Jerry Fielden, and Aaron Spreng. Corrected grammatical errors and clarified content.
Draft (0.4)	February 2, 2005	David Kemper	Added **e-records appraisal** sub-component to **Transfer protocol** (under consideration).
Draft (0.5)	March 8, 2005	David Kemper	Added to transfer protocol section on secure deletion.
Draft (0.6)	March 14, 2005	David Kemper	Edits made to overall document. Edits to protocols, focusing on interim solutions and EDRMS capabilities.
Draft (0.7)	March 21, 2005	David Kemper and Johanne Pelletier	Revisions to protocols and clarifications. Added appendix section.
Draft (0.8)	May 4, 2005	David Kemper and Johanne Pelletier	Further revisions to protocols and text clarifications. Introduced an interim access protocol.
Draft (0.9)	May 17, 2005	David Kemper and Johanne Pelletier	Minor textual edits, formatting changes.
Release 1.0	May 30, 2005	David Kemper and Johanne Pelletier	Minor changes.
Release 1.1	June 10, 2005	David Kemper and Johanne Pelletier	Interim Project Report (June 2005) update section added

1. Transfer

This stage is where McGill University units arrange for the transfer/delivery of institutional electronic records to the MUA (under the authority of the *McGill University Records Retention Schedule MURRS*). While the transfer protocol shall remain an important component, the precise methods used to transfer electronic records will change as technology evolves.

The goal of the transfer protocol is to safely and securely transfer electronic records from McGill units to the MUA's ***digitalpermanence*** repository for long-term preservation or permanent storage. The MUA envisions the ***digitalpermanence*** repository—either a single storage area or a set of storage servers—to operate within McGill's information technology infrastructure.

The ideal solution would organize and manage electronic documents throughout their business lifecycle, from document creation to document retention or destruction, classifying them and then transferring them to the ***digitalpermanence*** repository. This would involve the implementation of an electronic document and records management system (EDRMS). The transfer solution, therefore, would form part of the records/document management system.

However, pending the examination and implementation of an EDRMS, the MUA proposes procedures to achieve the goals of the protocols that make use of current campus resources.

Transfer elements:

1. **preliminary appraisal/assessment**
2. **preparation of e-records for transfer**
3. **records delivery and testing**
4. **secure deletion**

Transfer → preliminary appraisal/assessment

Prior to the actual transfer of electronic records to the MUA, the electronic records will have been assessed by the MUA's professional staff to ensure that the transfer complies with *MURRS* (i.e. that unnecessary files will not form part of the eventual data transfer).

If a preliminary assessment is not possible, the transfer must still comply with procedures for transferring records to the MUA. These procedures are available on the MUA website at the following URL: http://www.archives.mcgill.ca/recmanage/recguide.htm.

Transfer → preparation of e-records for transfer

All electronic records transfers to the MUA will require units to submit, along with their electronic records, the following information:

- **File listing** (statement in the form of an electronic or printed spreadsheet listing the files delivered).
- **File formats** (statement identifying file format(s) to be found, e.g. Word documents, PDF documents);
- **File and Folder structure** (statement explaining how the files and folders are organized, e.g. Folder "Senate" contains Senate Minute Files);
- **File context** (statement explaining how these files relate to the unit's daily business, including date ranges and basic finding aid information: e.g. "These project reports correspond to our Imaging of Personnel Records project, 2003-2004");

As technology permits, the MUA will require that text documents be converted to XML (or XHTML) prior to delivery.[1] If the conversion of text documents to XML (or XHTML) prior to deliver is not possible, the MUA may have to embark on a batch XML (or XHTML) conversion of MS Word or other MS Office-type documents (or other office productivity software) for preservation purposes.

It should be noted that the latest version of Microsoft Office, Microsoft Office 2003, has the ability to convert Word documents and Excel spreadsheets to XML.[2]

Transfer → records delivery and testing

The MUA will request that units contact and schedule a delivery date with the MUA (or, alternatively, the University Archives could develop a delivery schedule for units to follow). Once a delivery date has been set, the delivery of electronic records will proceed.

There are 2 transfer methods currently available and within the University's and MUA's means:

1) Deliver electronic records on physical media such as CD-R or DVD or tape. This method is convenient as most McGill staff members are familiar with CD-DVD writing software, but it will require extra storage space to accommodate a growing collection of CDs and DVDs. At this stage, the physical media transfer method will most likely be used by McGill units.

2) Secure file transfer protocol (FTP) to transfer electronic records from McGill units directly to the MUA. This transfer method can take advantage of the power of secure file transfer technology (e.g. SSH Secure Shell).

3) Alternatively, the implementation of an electronic document and records management system would be another method for transferring electronic records sent from McGill units directly to the MUA's ***digitalpermanence*** repository.

In any case, the integrity and authenticity of the electronic records must be assured while in transit and once deposited to the MUA. In other words, the submission of any electronic records to the MUA must be performed by authorized staff using only an approved file transfer mechanism.

Once the electronic records have been transferred to the MUA's ***digitalpermanence*** repository, they will be temporarily stored in quarantine for testing to ensure that they are accessible and virus-free. Once testing is complete, the MUA will notify the depositing McGill unit that it is now safe to delete the files.

Transfer → secure deletion

McGill units transferring electronic records to the MUA should keep a copy of their electronic records locally until notified that it is safe to securely delete the electronic records on their end.

It is important that, when deleting electronic records found on various media formats (hard disk, optical, etc), McGill units use a secure deletion method, one that ensures that all data is erased once a transfer has been successfully made to the MUA. There are several small- and medium-sized companies, as well

[1] It should be noted that Library and Archives Canada (LAC) recommends that Office-type documents, or files in which both content and format are important, be converted to XHTML (a reformulation of HTML 4) using a client-server software package called **HTML Transit Central**. Meanwhile, LAC recommends that databases and spreadsheets, or files in which data is more important than format, be converted to XML. The LAC hosts an Information Management website <http://www.collectionscanada.ca/information-management/0612/061204_e.html>.

[2] Microsoft Corporation, <http://www.microsoft.com/office/editions/prodinfo/technologies/xml.mspx>

as large enterprise companies, that offer such secure deletion solutions. The sources below on secure deletion offer more information on techniques, company names and products.

Sources Consulted
U.K. National Archives. “Electronic records management: Guidelines for management, appraisal and preservation of electronic records.” October 12, 2004.
<http://www.nationalarchives.gov.uk/electronicrecords/advice/guidelines.htm>

Library and Archives Canada. “Information Management Services: Guidelines for File Types, Interchange Formats and Information Standards.” October 12, 2004. <http://www.collectionscanada.ca/information-management/0612/061204_e.html>

A full list of small-scale **secure deletion** software solutions is available here: <www.brown.edu/Facilities/CIS/Doc/dararmv.html>
Meanwhile, there are also enterprise-wide software solutions, including Decru CryptoShred 2.0 software <www.netapp.com/ftp/decru-fileshredding.pdf>

2. Intellectual Controls/Processing

Intellectual controls/ processing describes the range of intellectual control procedures used by the MUA as applied to electronic records transfers. While arrangement and description functions are traditionally a key component in a range of intellectual controls procedures they are not specifically addressed by this document.

The goal of this section is to process in-coming electronic records, thereby allowing them to be identified and systematically managed according to retention rules, properly preserved, and accessible to researchers in the long-term, and to deposit them inside a virus-free/virus-protected secure digital repository—the ***digitalpermanence*** repository.

The implementation of an electronic document and records management system would alter the manner in which electronic records are accessioned. Depending on the technology used, the EDRMS could perform some preliminary intellectual control functions automatically by appending select metadata (i.e. contextual information about the document) to the electronic records at the moment of document creation. This automatic or near-automatic process would greatly enhance the overall processing protocol.

Processing elements:

1. **accession/intellectual controls**
2. ***digitalpermanence* repository storage**

Processing → accession/intellectual controls

Combining both current and developing accessioning practices (e.g. the draft e-records access register form **Electronic Records Accession Form** or ERAF, see appendix), the MUA will process in-coming electronic records, assigning them an accession number and retention period, as well as indicating their provenance, name of depositor, and a brief content description. The processing protocol should also take note of the explicit electronic properties of the electronic records, such as:

- **System Properties** (i.e. operating system used by depositor and MUA)
- **File Properties** (i.e. file format, file extension, file format ownership, file preservation category and strategy)
- **File Details** (i.e. application used to open file during accessioning, if PDF, more info on PDF producer tool and PDF version, for instance)

The **Electronic Records Accession Form** could be either electronic (saved as ASCII text or XML) or paper and filed alongside the current paper accession registry. A more efficient method could involve the development of a template-based **Electronic Records Accession Form** that processing staff would use to input accessioning data and save it in a secure database.

The goal of collecting this information is to provide MUA staff with enough information about the electronic record so that they may determine the computing environment that created the electronic record and, if necessary, re-create that environment or find a suitable emulated environment to access the electronic record in the future.

Processing → *digitalpermanence* repository storage

Once the delivered electronic records are tested, which occurs during the transfer protocol, and then accessioned, the electronic records are ready to be stored inside the ***digitalpermanence*** repository.

The stored electronic records are given a virtual shelf number. This information should also be noted on the Electronic Records Accession Form. For example:

***digitalpermanence* repository Location Path**
(i.e. path and location of e-record once deposited inside the ***digitalpermanence*** repository, similar to a shelf number):

dp:\\{YEAR}\{ACCESSION NUMBER}\{RG}\{electronic records here}

3. Preservation

This stage is where electronic records, once securely deposited inside the ***digitalpermanence*** repository, are cloned and converted into both a reference and preservation copy and routinely tested over their retention period to ensure their accessibility and readability.

This stage is also the research and development (R&D) component of ***digitalpermanence***, where records managers and archivists collaborate with information technologists and computer scientists to research and develop strategies and mechanisms to preserve electronic records throughout their retention period.

The goal of the preservation protocol is two-fold: to take electronic records and covert them into a reference copy (for research access) and a preservation copy (for long-term or permanent retention purposes); and to research and develop strategies and mechanisms to ensure the long-term accessibility and readability of institutional electronic records.

For the MUA, the ideal scenario to achieve these goals would be a batch processing utility that can convert frequently used office system documents, such as Word, Excel as well as Outlook Email, into an accessible but secure reference copy (e.g. PDF), which would be accessible to researchers, in addition to a striped-down and simplified preservation copy (e.g. XHTML or XML), which would preserve the essential components of the document (content, formatting, etc).

Preservation elements:

1. **e-records clone and conversion**
2. **e-records digital preservation**

Preservation → e-records clone and conversion

Among the key reasons for preserving records is to make them available to researchers. In the course of being used, electronic records may be accidentally (or purposefully) manipulated or altered. In order to avoid such a scenario, and to still enable researchers access to electronic records, it will be necessary to clone (i.e. duplicate) and convert electronic records to an accessible but secure format such as PDF.[3]

Furthermore, this first preservation element will require the conversion of electronic records to a preservation copy, either to XHTML or XML, both recommended choices because of their standards-based and open-source architecture. As file formats evolve, however, there may be changes made to the choice of preservation file format. In 5, 10, 50 years, file formats will undergo radical changes, so an on-going preservation strategy must form part of ***digitalpermanence***.

In order to keep track of electronic records requiring long-term preservation (amid a large volume of other electronic records inside the ***digitalpermanence*** repository), there needs be a system (possibly an EDRMS) that will flag, either manually or automatically, those electronic records whose retention periods are marked in years (or permanent) so as to alert future archivists that such electronic records, though they may be in a preservation format such as XHTML or XML, will need on-going testing to ensure that they are still readable and accessible with future technologies and software. If necessary, those flagged electronic records, after consultation, should be migrated to another, more stable file format.

Preservation → e-records digital preservation

[3] The U.K. National Archives is planning on converting PostScript, TIFF and SGML files (generally, most text and image-based documents) to PDF as their presentational format of choice.

Electronic records are fragile dependent on the software and hardware environments in which they were created. In response, ***digitalpermanence*** will proactively seek methods to ensure readability and accessibility of electronic records through research on new and emerging file formats.

This will require collaboration between records managers and archivists (who will supply the expertise in identifying what e-records should be preserved long-term and what requirements and standards best fulfill recordkeeping and archival needs) and information technologists (who will supply the software and hardware expertise to work towards the long-term readability and accessibility of electronic records).

Electronic records archivists and information technologists have begun examining these long-term preservation issues and have posted detailed file format longevity information. The following are a few examples.

Library and Archives Canada has created an online set of guidelines for computer file types.[4] Meanwhile, the Massachusetts Institute of Technology (MIT) and its DSpace Institutional Repository technology, while not specifically a digital preservation tool, has compiled a list of supported, known, and unsupported file formats.[5] Finally, the United Kingdom's National Archives has a comprehensive file format database called PRONOM,[6] a free online resource, continually updated, that provides file format description, version, support information, and so on.

Overall, these resources can help in determining what file formats are currently the most supported or stable. The MUA's approach in dealing with file formats was spawned from the electronic records inventory conducted in 2004, when our survey of campus departments, faculties and offices revealed a clear snapshot of software applications used on campus. The majority of administrative software used on campus is produced by Microsoft. From email (MS Exchange) to office applications (MS Office), the use of Microsoft products, thanks mostly to the standardization of software purchases, was very common. While there are other applications in use on campus, such as software from Apple, Adobe, and Corel, the majority of administrative units use Microsoft products.

From this standpoint, the MUA will monitor changes to Microsoft Exchange and Microsoft Office software, making sure that their file formats (i.e. pst, doc, xls, ppt, mdb) remain accessible in the short-term and, above all, can be migrated to a preservation format for long-term preservation.

[4] LAC website <http://www.collectionscanada.ca/information-management/0612/061204_e.html>
[5] DSpace File Format Support reference <http://www.library.rochester.edu/index.cfm?PAGE=1360>
[6] UK National Archives PRONOM file format reference <http://www.nationalarchives.gov.uk/pronom/>

4. Access

This stage is where accessioned and deposited institutional electronic records are made available to researchers. There are a variety of electronic records that will be made accessible: enterprise data (Student, Finance, HR), business emails, and departmental/office system electronic documents.

The goal of the access protocol is to ensure that electronic records are available to staff, students, and researchers under the policies of the MUA. The goal is straightforward; however, it will require that all 3 previous protocols (transfer, processing, and preservation) be built upon a system that can bring organization and structure to the myriad of electronic records to be acquired.

Currently, the MUA believes that an electronic document and records management system can more effectively and efficiently organize and structure electronic documents than a case-by-case, one electronic document at a time scenario. Furthermore, when electronic records are organized, structured, and given contextual information, they become more easily managed and in turn more accessible to research interests.

In short, a solid classification of electronic records, provided by an EDRMS, will allow administrative control over and access to electronic records stored in the ***digitalpermanence*** repository through the university's emerging campus-wide access infrastructure (e.g. university portal).

Access Protocol: A System Proposal

The access protocol proposes a sophisticated search and retrieval mechanism, somewhat similar to an integrated library system, where, instead of books and journals, electronic records are stored inside a database (the proposed basis of the ***digitalpermanence*** repository), which, in turn, can be searched by researchers at workstations located at the MUA that grant them controlled access to institutional electronic records.

One vision of the access protocol is to imagine a researcher sitting at a workstation at the MUA, facing a search interface (Web-based or other) which has the ability to search and retrieve the electronic records stored inside the ***digitalpermanence*** repository.

Once the researcher inputs a few terms or keywords in the search field, the search engine searches the ***digitalpermanence*** repository, seeking out the electronic records via their metadata (added during the processing protocol or, ideally, by an EDRMS at the moment of document creation), and the most relevant results are then displayed. Once access controls are initiated, the user may access the results by clicking on an item (identified by a clickable hyperlink). The researcher would click on the hyperlink—it may be a link to a Word document, an email message, a Banner report, etc—and view a reference copy version (i.e. PDF) of the electronic record.

In order to achieve the goal of electronic records transfers and access, the ***digitalpermanence*** repository would be a highly structured and organized digital repository, founded on a robust and scalable database, with its own controlled vocabulary and records management metadata, and a web-based or system-based data input (administrative) tool and a simple and advanced search interface (user).

Interim Access

In the mean time, while such a theoretical system is considered, the MUA proposes to provide access to electronic records using common record request and retrieval methods.

The MUA has several electronic records in its inventory, all on CD-ROMs, most containing institutional records and others business emails. The content of the CD-ROMs was appraised and accessioned, following MUA records management procedures (along with the draft Electronic Records Accession Form outlined in this discussion document). With intellectual controls in place, the CD-ROMs were stored away.

Several internal requests have been made for theses electronic records, and each have been responded to by following MUA procedures: accession file examined, location determined, and the appropriate CD-ROM retrieved. However, because we are dealing with a very small volume of CD-ROMs, the search and retrieval of the requested electronic files was achieved in very rapid time. The request and retrieval method was sufficient, and the technology to access the electronic files was available.

However, the MUA recognizes that this small-scale scenario will not remain the norm for very long as more electronic records are created and transferred to the MUA for recordkeeping purposes. There will clearly be a need to transform electronic records request and retrieval methods and modernize the technologies used to access the electronic files. This early stage, therefore, represents a useful period whereby the MUA can familiarize itself with retrieving electronic records and subsequently determine with more clarity the design of a proposed ***digitalpermanence*** repository.

Sources Consulted

"Digital Preservation at the National Archives"
<http://www.nationalarchives.gov.uk/preservation/digitalarchive/pdf/dpattna.pdf>

"New Digital Archive at the National Archives"
<http://www.nationalarchives.gov.uk/preservation/digitalarchive/pdf/project_background.pdf>

"Preserving the Digital Heritage: building a digital archive for UK Government Records"
<http://www.nationalarchives.gov.uk/preservation/digitalarchive/pdf/brown.pdf>

Interim Solutions

The MUA is working on solutions to manage electronic records until and pending the possible implementation of a formal electronic document and records management system. In the interim, however, the MUA must address the continuing development, use, and ongoing management of digital records assets on campus.

The goal of these interim solutions is two-fold: to manage electronic records using modified records management techniques; and to gain a better understanding of the dynamic nature of electronic records as their presence increases on campus.

Interim Solutions > Managing Emails Pilot Testing

The MUA received business emails from two sources: a former McGill University Archives employee, whose emails we had access to and were subsequently archived using Microsoft Outlook's Auto-Archive feature, and a retiring professor, whose emails were submitted to the MUA on a CD-ROM. These emails records were Microsoft PST data files.

Once the PST data files were imported into a Microsoft Outlook Client, the emails were appraised by reviewing their content and categorizing them into a classification scheme. For instance, the emails were classified under: administrative/business (or at times confidential) emails, research-oriented emails, and personal emails.

The next step required that the emails be converted to both a reference copy (for research purposes) and preservation copy (for preservation purposes).

The MUA purchased a piece of software called ABC Amber Outlook Converter (a 30-day trial version is available at http://www.processtext.com/abcoutlk.html), which has the ability to batch convert emails found in PST data files into HTML, XML, PDF, TIFF file formats, among others.

Our test involved converting emails in the "Sent Items" folder to HTML. The software converted the emails into the chosen file format relatively quickly. The conversion results were good. The software converted all the email messages found in the folder, created HTML files named after the emails' subject line (this can be customized), and placed them inside a user created folder on the hard disk. Any email attachments were placed in a single, separate folder called "_attach." It should be noted that file attachments were not converted. The software converts emails only.

Access to these newly created HTML files was easy: using Windows Explorer, one browses to the file location, double-clicks on a HTML file, and views them as one would normally view a HTML file inside a web browser. The content and contextual information about the email (To, From, Subject, Date & Time) were preserved as well as links to any email attachments.

At this stage, ABC Amber Outlook Converter, while impressive, is useful only in converting a moderate volume of emails from a single PST date file, such as the amount the MUA procured. However, large-scale and ongoing email conversion would require a larger more robust system. Nevertheless, the software proves that such email conversion utilities exist and work well, and therefore further advancements can be made in this area.

Web Archiving

The McGill University Web System, McGill's official presence on the Web developed and maintained by the Web Services Group (WSG), is the online source for information regarding McGill University. As such, the McGill Web System represents a valuable digital asset to the MUA, for it is evidence of McGill University's institutional and historical "Web" record.

However, due to the dynamic and interactive nature of the McGill Web System, common acquisition methods (such as grabbing static web pages) need to be replaced with a solution that can acquire both the static Web System elements as well as the behind-the-scenes data-driven content. The web archiving test pilot will seek the development of a special tool to capture the many databases that operate ‘behind-the-scenes’ which distribute content to the entire Web System. Moreover, and most importantly, the tool will allow the MUA to quickly re-build the Web System snapshot into a fully-functioning website, therefore allowing researchers the ability to browse the Web System as though it were still “live.”

To achieve this complex solution, the MUA is working with the Web Service Group (WSG) to develop a specialized web snapshot software tool tentatively called the McGill Web System Snapshot Tool.

Conclusion: Next Steps

After accomplishing several important steps toward managing electronic records—a campus-wide electronic records inventory, the creation of new electronic records series and retention rules—the University Archives' ***digitalpermanence*** looks ahead to the second half of 2005 to establish and present its records management and archival strategy for the university's electronic records.

Among the next steps, the following are worth highlighting:

- Continue to advise McGill units about the value and importance of managing electronic records, encouraging the adoption of email and file classification best practices;
- Revise *MURRS* (McGill University Records Retention Schedule) to reflect results ascertained through the electronic records campus-wide survey;
- Pursue pilot testing projects—that is, email acquisitions and conversion and web archiving;
- Prepare and present records management and archival requirements for an electronic document and records management system that will ensure the proper management of institutional electronic records;
- Establish an electronic document and records management working group to investigate and evaluate electronic document and records management software solutions.

Created by David Kemper
McGill University Archives
www.archives.mcgill.ca

Update: **Interim Report June 2005**

A series of project-based work continues as an extension of the MUA's ***digitalpermanence*** project initiated in 2003/04.

McGill Web System Snapshot Tool: As part of a joint initiative with the Web Services Group (WSG), the MUA has contracted the creation of a *McGill Web System Snapshot Tool.* Previous pilot tests of available website capture utilities revealed weaknesses in the ability to capture the McGill Web System's complex, dynamically-generated web pages. This project envisions a utility devised to capture the McGill Web System and web content databases in XHTML and XML, respectively (for the purpose of preservation), and provide added functionality to the WSG in its web publishing work.

Document Management (Office-Systems): At the close of Phase I, a plan was approved for the selection/identification of a document management (DM) solution for University Offices (to be jointly chaired by Johanne Pelletier and Gary Bernstein). While this remains a priority, resources have been temporarily deferred to provide support/advisory services to campus reformatting projects, with a view to continued discussions around DM solutions arising from these.

Retention Rules – Electronic Records: Revisions to *MURRS (McGill University Records Retention Schedule)* reflecting results of the electronic records surveys conducted in 2004/05 are in development and will be pending approval by the University's Legal Services Office and the Provincial Government.

Outreach to University Offices: During the 2004/05 academic year each of McGill University's faculties received an information session on record-keeping responsibilities, *MURRS* and the ***digitalpermanence*** project – included in these sessions was a review of McGill University's Scanning Standard and related best practices for office records pending the selection of a document management solution.

MUA Terms of Reference: The MUA's revised *Terms of Reference* was approved by the Executive Committee (Board of Governors) in January 2005. Among the revisions is language reflecting the MUA's role in e-records management, and its continuing role in private acquisitions (excerpt follows):

> *The mission of the McGill University Archives (MUA) is to promote good governance, and accountability, through the protection of the University's documentary heritage and records/information assets, in all formats, by combined archives and records management services.*

Staffing: Short-term contracts with three Records Analysts for the purposes of the e-records survey ended in January 2005 – at the close of the contracts a new Archivist/Records Analyst joined the staff full-time (Mr. Aaron Spreng). Mr. David Kemper continues as a member of the MUA staff as Archivist, Electronic Records.

Appendix

Electronic Records Accession Form

Definition
The Electronic Records Accession Form (ERAF) is designed to provide electronic records archivists with information concerning electronic records—in other words, a description of the file format(s) found on digital media transferred to the University Archives.

Much as the Archives Accession Register provides an intellectual and physical description of a record, the ERAF will provide a digital description of electronic records by identifying such items as operating system, file format, file extension, and related applications.

The Electronic Records Accession Form should complement the Archives Accession Register.

The ERAF will either be a paper file or an electronic file (ASCII text file), depending on what medium is most feasible, and as such could be located either within the Accession Register File (paper) or on the digital media itself as a text README file on the root level entitled, for example, 04-056-README. An electronic ERAF file can be used when electronic files are migrated from a hard disk or server and backed-up to CD-ROM or DVD-ROM. A README file can be placed alongside the electronic files.

Procedure
In order to ensure the readability of an electronic record in, say, five to ten years, the ERAF must identify all pertinent information related to the electronic file in question.

Using a sampling method for each type of file format found, we should identify the following:

A. System Environment

1. **Identify Operating System (OS) used by Depositor:** This information, which may be made more easily attainable if the Depositor depositing electronic files is required to submit this information, can help a future archivist assess the system environment in which the electronic file was created.

   e.g. Microsoft Windows 98 SE
   Microsoft Windows XP
   Mac OS 10

2. **Identify Operating System (OS) used at the time of accessioning:** This information, which can be found by right-clicking the My Computer desktop icon, selecting Properties and then the General tab, allows future archivists to compare system environments, determine whether or not a file remains functional inside another operating system environment, and, if necessary, recreate that OS environment.

   e.g. Microsoft Windows 2000 SP 4

B. File Properties

1. **Identify file format (full name and file extension):** In the Windows Explorer, right-click on a file, from the menu choose Properties, and then select the General tab.

   e.g. Portable Document Format (.pdf)
   Microsoft Word Document (.doc)
   Microsoft PowerPoint Presentation (.ppt)
   Tagged Image File Format (.tiff)

2. **Identify total number of above files:** Count the number of files or navigate Windows Explorer to root level, right-click on main folder (or highlight all files and right-click) and select Properties. Quote the number provided by Windows.

3. **Identify file creation dates (YYYY/MM/DD):** In the Windows Explorer, right-click on a file, from the menu choose Properties, and then select the General tab to generate an approximate date range when files were created.

4. **Identify file format ownership (full name):** Either look at the file format or do an online search to identify company owning the file format, if any. (Some file formats are without corporate ownership).

   e.g. Adobe Systems, Inc.
   Microsoft Corporation
   open source (URL, if downloadable from the Web)

C. File Details

1. **Identify application used to create file:** This information, found by right-clicking file, selecting Properties, and then the Summary tab or, failing that, asking the Depositor for this information,

would detail the software name and version used to create the file, and create a 'benchmark' from which to proceed in cases of migration or emulation of the file format.

e.g. Microsoft Word 2002
HP PrecisionScan/Adobe Photoshop 7.0.1
Windows Encoder

2. **Identify application used to open file at the time of accessioning (name/version):** File formats usually have an association with a specific application that will open it. By identifying the application used during accessioning, future archivists can determine the functionality of the file, whether it works or not.

e.g. Microsoft Word 2002
Adobe Photoshop 7.0.1
Windows Media Player 9.0

PDF File Details

a. **When accessioning a PDF file, with file open in Acrobat Reader, select Document Properties from the File menu (or press Ctrl-D)**

b. **Identify creator (Application) and producer (PDF producer) as well as PDF version:** Since PDF files are files converted from another format, it is important to identify what created the original file (creator), what converted the file to PDF (producer), and what version of the PDF converter.

c. **Identify security features/restrictions, if any:** Make note of restrictions such as opening, printing, editing as well as encryption features.

MacDonald Campus: Final Exams
Faculty of Agriculture and Environmental Sciences
Fall 2001/Winter 2002/Fall 2002/ Winter 2003

Electronic Records Accession Form			
Accession Number:	**XX-XXX**	RG/MG Number:	**XXXX c. xxx**
Date Received:	**2004/03/16**		
A. System Environment			
Operating System used by Depositor:	**Not known**		
Operating System used by MUA:	**Windows 2000 SP 4**		
B. File Properties			
File Format:	**Portable Document Format (.pdf)**		
Total Number of Above Files:	**62 PDF files**		
File Creation Dates:	**October 25, 2003 – November 23, 2003**		
File Format Owner:	**Adobe Systems Incorporated**		
C. File Details			
Application used to open file:	**Adobe Acrobat Reader 6.0**		
If file format is PDF, identify the following			
Creator Application:	**Acrobat 5.0 Image Conversion Plug-in for Windows**		
PDF Producer:	**Acrobat 5.0 Image Conversion Plug-in for Windows**		
PDF Version:	**1.4 (Acrobat 5.x)**		
Security/Restrictions			
Open (password-protected):	**No**		
Edit:	**No**		
Print:	**No**		
Encryption:	**No**		
Other:			
Received By:	**David Kemper**		
dp repository location:	**2005\XX-XXX\RGXX**		
Remarks:			

McGill University Archives: Reports
***digitalpermanence* Project**
January 2003—March 2003

Electronic Records Accession Form			
Accession Number:	**XX-XXX**	RG/MG Number:	**11 c. xx**
Date Received:	**2004/03/23**		
A. System Environment			
Operating System used by Depositor:	**Windows 2000 SP 4**		
Operating System used by MUA:	**Windows 2000 SP 4**		
B. File Properties			
File Format:	**Microsoft Word Document (.doc)**		
Total Number of Above Files:	**2**		
File Creation Dates:	**March 19, 2004**		
File Format Owner:	**Microsoft Corporation**		
C. File Details			
Application used to create file:	**Microsoft Word 10.0**		
Application used to open file:	**Microsoft Word 10.0**		
If file format is PDF, identify the following			
Creator Application:			
PDF Producer:			
PDF Version:			
Security/Restrictions for the following			
Open (password-protected):			
Edit:			
Print:			
Encryption:			
Other:			
Received By:	**David Kemper**		

dp repository location:	**2005\XX-XXX\RGXX**
Remarks:	