Peer Reviewed Article Vol.11(1) March 2009

Investigating electronic records management and compliance with regulatory requirements in a South African university

M.E. Kyobe *
Department of Information Systems
University of Cape Town
Cape Town , South Africa
Michael.kyobe@uct.ac.za

P. Molai
Department of Information Systems
University of Cape Town
Cape Town , South Africa
palmol2001@yahoo.com

T. Salie
Department of Information Systems
University of Cape Town
Cape Town , South Africa
taariqsalie@gmail.com

This study investigated the extent to which academics and students at a leading University in South Africa managed electronic records in accordance with good practices and regulatory requirements. Literature on electronic records management (ERM) and regulatory compliance was synthesised to create a framework for effective records management. A survey was then conducted to test this framework with 17 academics, 97 students and two technical staff from five faculties. The results revealed several incidents of poor records management and lack of compliance with regulations. Many academics and students were unaware of legislative requirements and penalties. They did not backup or archive records regularly and where this was done, there were no standard procedures followed, which resulted in the adoption of distinct approaches to record keeping. Furthermore, appropriate programmes for educating users on ERM did not exist and academics had not established collaborative initiatives with other non-academics (e.g. internal auditors and legal experts) to ensure effective ERM. It was also surprising to find that non-computing academics and students managed system security risks better than their computing counterparts. Useful recommendations and the way forward are provided.

Key words: Electronic records management, regulatory compliance, academics, students, South Africa

Received 3 December 2008; accepted March 2009

Contents

1 Introduction

Electronic records management has become an essential business activity and an element of compliance with regulation in many countries. In academic institutions, students and academics are increasingly creating and accessing electronic documents, course materials, on-line assessments, e-mails and research databases. Studies indicate, however, that poor electronic records management is on the rise in South Africa and this could lead to costly legal liabilities (Michalson and Hughes 2005:2−3; *Image and Data Manager* 2006:1), inability to share information, wastage of storage space and poor governance (JISC 2004:1; Maguire 2005:151). Little is yet known about the management of electronic records and compliance with electronic communication regulations by academics and students in South Africa. This study investigated the extent to which academics and students at a leading university in South Africa managed electronic records in accordance with good practices and regulatory requirements.

In the following sections, a review of literature on records management and regulatory compliance are given. A framework to evaluate the effectiveness of records management is presented followed by the research design. The analysis of the data is then presented and the findings are discussed. Finally, conclusions are drawn and recommendations made.

top

2 Literature review

Electronic records management may be defined as that part of records management that deals with records in electronic form. According to Johnston and Bowen (2005:132) this includes 'the creation, use, maintenance and disposal of electronically created records for the purposes of providing evidence of business activities'. A rchivists emphasise that the term 'record' does not simply refer to a collection of data, but to a product or an event. It is a specific type of information reflecting and providing evidence of business processes or individual activities (Bantin 2001:18).

There has been considerable debate about the development of the records management discipline. While some argue that the discipline is under-developed and lacks its own theoretical basis, recent studies provide evidence to suggest the existence of a body of theoretical knowledge consisting of document authentication theories, archival-based theories (e.g. those on permanent storage, inactive storage and disposal), information science principles (e.g. principles of retrieval, maintenance, active storage and indexing) and information communication and technology-based (ICT-based) practices for handling intangible records, physical control and data transformation (Darlington, Finney and Pearce 2003:1−3; Yusof and Chell, 2002:55). Some of these theoretical foundations are reviewed below.

2.1 Diplomatics theory – 16 th century

Diplomatics is the discipline which studies the genesis, forms and transmission of archival documents and their relationship with the facts represented in them and with the creator, in order to identify, evaluate and communicate their true nature (Cowan and Pember 2007:4, Duranti 1989:7; Underwood n.d.:54). According to Duranti (1989:12), the term diplomatics was adapted from the Latin word *res diplomatica*, which refers to the critical analysis of forms of diplomas (e.g. a deed issued by a sovereign authority, or documents), in order to distinguish genuine documents from forgeries. Duranti (1989:12) states that until the sixth century, there were no criteria for the identification of forgeries and legislators had limited interest in the issue because of this commonly accepted legal principle at the time: 'authenticity is not an intrinsic character of documents but is accorded to them by the fact of their preservation in a designated place, a temple, public office, treasury or archives'. This principle was abused as people eventually began to present forgeries to designated records office to lend them authentic. Practical rules were therefore introduced to recognise documents. For instance, fundamental rules for textual criticism were established in 1680s by Jean Mabillon (Duranti (1989:12). These involved categorisation and examination of documents for their material, ink, language, script, punctuation, abbreviations, formulas, subscriptions, seals, special signs, chancery notes, etc. This marked the birth date of diplomatics and palaeography (the study of writing and documents from the past).

2.2 Life cycle model

This theory is based on the premise that it is possible to divide the life of a record into distinct stages. The first phase of the life cycle would involve the creation or receipt, classification, use, maintenance and disposition of these records through destruction or transfer to archives. The second phase involves the archival of the records, for example description of the records in inventories, finding aids, preservation of the records and use by researchers, scholars or the public (Atherton 1985:44−48). This approach has been useful in promoting a sense of order. It tries to define what a record is, what happens to it during the process and who will manage the record during each stage.

However, since intervention in this model is only triggered by the age and use of records resulting in physical relocation, this approach may not be ideal in an electronic environment where data storage media and reading mechanisms change frequently and the priority is usually to capture records with all their attributes and evidence at the point of creation (Mcleod, Hare and Johare 2004:2−3). These authors argue for intervention at the systems design stage to guarantee appropriate record creation and capture.

2.3 Continuum theory − records management as a continuous process

The records continuum model focuses on the management of records as a continuous proce ss. It sees the need to manage records from the perspective of activities (rather than stages). This may be guided by questions such as: what records need to be captured to provide evidence of an activity; what systems and rules need to ensure records are captured and maintained; how long should the records be kept to meet business and other requirements; how they should be stored; and who should have access to them (Sletten 1999:28−29).

2.4 Partnership theory

Critics of the life cycle model have argued that it makes the role of archivists secondary to that of records managers. Atherton (1985:47−49), another advocate of the continuum model, argues that effective management of records requires ongoing cooperative interaction between the records manager and archivist. This view is also supported by Bantin (1999:2−3), who recommends a team approach whereby archivists form partnerships with decision support personnel, systems analysts and internal auditors in ensuring the creation and maintenance of accurate and authentic records.

2.5 Integrated theory

The integrated framework (Xiaomi 2003:28−29) combines the concepts of lifecycle model, records continuum and good practices. This model looks at management of records as an archival business geared towards customer satisfaction, cost-effective management and best value. Five levels of integration are recommended in the record keeping processes: common culture (common understanding and expectation among creators, users, custodians and administrators); common standards; information sharing; coordination; and collaboration.

top

3 Management of electronic records in academic institutions

Some major challenges in managing electronic records in academia relate to the nature of the records kept and used, where they are located, policy issues, accountability and responsibility of users, and compliance with rules and regulations.

3.1 Problem of dispersed records

Information is a key business resource for universities (Bailey 2007:5; Thornhill 2008) It aids competitiveness in higher institutions (Web portals, competition, lectures on-line, research, etc). Even administrative activities are now done electronically using applications such as Peoplesoft or Systems, Applications and Products in Data Processing (SAP) software. The fact that university transactions now transcend geographic borders (e.g. involving international students, business and research partners) has, however, created serious records management problems (Bailey 2007:5). Records are found on shared network drives, local drives, research databases, institution e-mail and external Web servers. Today many academics, administrative staff and students by-pass the institution systems and use externally hosted systems such as Google, Facebook and Yahoo. Such dispersed records make location, classification, sharing of information and enforcement of compliance much more difficult. Location of information and its classification (e.g. understanding what it is and whether it is subject to an obligation) have become critical aspects in litigations.

3.2 Non-linear, transient and fragile information

In addition, Web documents are non-linear (i.e. hyperlinked), transient and fragile (easily updated, moved or deleted). Lecture notes, courses and information about these courses change every year or semester. If these changes are not properly managed, they result in several generations of active documents which often confuse users (MERIT Report 2003:3).

3.3 Security

Information security issues (e.g. access to information, cyber-crime, privacy, virus attacks, and commercial data mining) are of major concern in academia today (Myler and Broadbent 2006:7−8). According to Wamukoya and Mutula (2005:74), poor security and confidentiality controls have been identified as major factors contributing to the failure of capturing and preservation of electronic records in eastern and southern African institutions of education. Chinyemba and Ngulube (2005:14) found that 89% of the academics surveyed at the University of KwaZulu-Natal did not adequately protect and secure their electronic records. Jones and Soltren (2005:25) found that 58% of the students surveyed were not concerned at all about risks to privacy on social network systems.

3.4 Policy development

Policy development has been emphasised by many authors as key to good records management (Kahn 2004:3−4). Such a policy would clearly set out the organisation's expectations regarding retention, individual roles and responsibilities, ownership, control, classification of different categories of content and privacy (Myler and Broadbent 2006:3). The failure to capture and preserve electronic records in eastern and southern African institutions of higher education have been attributed to lack of policies and procedures, among other factors (Wamukoya and Mutula 2005:74). Norris (2003:3−9) reports that not many higher education institutions in the United Kingdom had well defined and active e-mail archiving policies in place. In fact findings from Duke University show that lack of defined policies resulted in different capabilities and different levels of e-mail management, backup, security and privacy usage among faculties (Tibbo and Pyatt 2006:3−4). Similar problems have been reported at Loughborough University (Norris 2003:3−9) and at the University of KwaZulu-Natalu (Chinyemba and Ngulube 2005:13−16).

3.5 Responsibility and accountability

Once policies have been established the roles and responsibility of each individual in the organisation needs to be clearly set out and efforts must be made to ensure that everyone involved understands their roles and responsibilities thoroughly (Myler and Broadbent 2006:7−8). For instance, a n individual using e-mail would be expected to identify and categorise e-mail records of value, apply consistently relevant contextual information and metadata, and ensure their integrity. The institution on the other hand has the responsibility of providing guidance on categories of e-mail to be retained and retention schedules, provide viable mechanisms for archiving of records, training and support to staff and students (Norris 2003:3−9). SANS 15801 also emphasises the duty of care whereby consideration needs to be given to how people do their jobs, how authority is delegated and the separation of responsibilities to reduce collusion and potential fraud.

3.6 Compliance with records management policies and regulations

There is increasing pressure on organisations to ensure that their electronic records meet legislative requirements of authenticity, reliability and originality (Myler and Broadbent 2006:2). Section 25 (Part 1, chapter 3) of the *South African Electronics Communication and Transactions (ECT) Act* (South Africa Government 2002) clearly regulates document retention, retrieval of critical data and unsolicited communications. Lack of compliance with university policies and state laws is on the rise. There are many cases where members of online social networks have been involved in inappropriate acts, for example posting of obscene photos, disclosure of personal details of others and use of abusive language (Chalfant 2005:1; Thelwall 2008:1). Students have been accused of ignoring or violating the terms and conditions for using Internet and laboratory facilities while incidents of surveillance of students' work (by institutions) without their consent and commercial data mining of student profiles have also been reported (Greenop 2007:1; Jones and Soltren 2005:25−29). These violations may have serious social and legal implications for individuals and educational institutions.

Literature suggests several factors influencing regulatory compliance, for instance economic factors such as potential legal/illegal gains and cost of compliance. When the cost of compliance is high or perceived to exceed potential liabilities, compliance fails (Mayne 2006:1). If regulated entities lack cognitive capabilities, understanding or ability to address environmental influences (psychological factors), compliance may fail (Grossman and Zealke 2005:4−5). Sociological factors such as social influence, moral values, trust and perceived legitimacy of the regulation may also impede compliance (Grossman and Zealke 2005:4−5). Industry factors such as professional standards, ethics and good practice can enhance compliance. Technological factors such as possession of IT skills, IT resources, content and information overload also influence compliance (Kyobe 2009:41−47).

Therefore, as the IT environment becomes more complex and dispersed, and as the regulations governing records become increasingly more stringent, the researchers contend that there is need to maintain confidence and trustworthiness in electronic records (e.g. security, authenticity, integrity and usability), proper policy development, accountability and compliance with regulations.

top

4 Towards a framework for effective electronic records management in higher education

Various approaches have been adopted by professionals to address the challenges posed by electronic records. One of these is the InterPAREs project which has been conducted since early 2000 (Preston 2007:9−10). This project aims to ensure that digitally produced records are created in accurate and reliable form and also reserved in authentic form. It is based on the older archival science of diplomatics, whereby the true nature of records is determined by analysing their genesis, forms and transmission and their relation to the facts and their creator (Duranti 1998:52).

There are also various international professional frameworks that provide guidance on how organisations can implement good practices of records management, for example ISO 17799, which provide comprehensive information management, ISO 15489 for classification and documentation, ISO 15816 (2002) for access controls and security management, metadata standards (ISO 23081) and regulations such as the *ECT Act*, 2002.

While most of these frameworks emphasise good practices, few however examine the legal and ethical issues involved in records management. Electronic records have evidentiary value, therefore they must be properly managed (Henriksen and Andersen 2008: 40−41). Case law has shown that the consequences of untimely destruction of electronically stored information can have dire consequences for any organisation (e.g. Enron scandal). The *Sarbanes-Oxley Act* of United States (SOX) also makes corporate executives accountable for certifying the accuracy of their organisation records. The big bucket and small bucket theories of record retention emphasise the importance of evaluating the organisational specific legal, regulatory and compliance environments before record retention decisions are made (Harris 2008:1−4). This is strongly supported by Henriksen and Andersen (2008:40−41) and Kendall and Mirza (2006:2−3), and can be achieved by working in partnership with counsels, regulators, auditors and compliance functions. A framework for effective records management consisting of these two important aspects (i.e. good practices and compliance with regulations) is proposed in the following section.

top

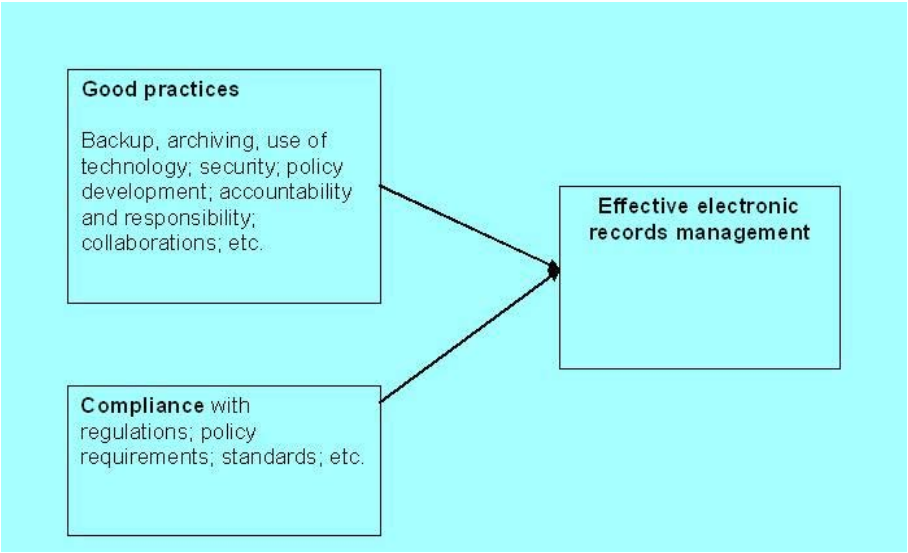
5 Proposed model

Figure 1 below presents the model for effective records management in higher education. The authors argue that effective records management entails not only adoption of good practices but also ensuring compliance with organisational policies and national regulations on the use of electronic media and facilities. The first element of the model therefore measures the extent to which good practices have been adopted while the second element looks at compliance with university policies and national regulations relating to ERM. Good practices involve (for instance) the development of a common backup and archiving culture and ensure the processes are conducted in a systematic manner. Those handling electronic records should understand their responsibilities, be accountable for their actions, collaborate with other stakeholders responsible for records management and be aware of security requirements. In addition, if the institution's ERM system is to be effective, it is imperative that learners and academics understand and comply with the policies and national regulations governing the use of electronic media. Deliberate or accidental destruction

of electronic records, spread of viruses, unauthorised access to personal records and other electronic records, copyright abuse, etc. could have dire consequences for those involved and for the institution.

The effectiveness of records management in the present study was measured by the extent to which good practices were adopted and policy, regulatory and other requirements adhered to by academics and students (JISC 2004:1; Maguire 2005:150−157).

Figure 1 Proposed model of effective records management



top

6 Research methodology and data collection

The aim of this study was to determine whether academics and students manage electronic records effectively. The researchers employed multiple techniques to capture data (i.e. a survey, interviews and observations). This ensured triangulation and also verification of the findings (Yin 1994). A questionnaire was used as the primary instrument for the collection of data from academics and students. Interviews were held with some academics and Information and Communication Technology Services (ICTS) staff who rendered IT services to the university, and student activities in the laboratory were also observed.

6.1 Reliability and validity testing

Reliability and validity tests were conducted to ensure the accuracy of the methods and data collected. The questionnaire was piloted withtwo academics and eigiht students. Corrections were made to some questions to ensure clarity and relevance. The questionnaire was also reviewed by the university's ethics committee and necessary amendments were made. Questions were mainly adapted from previous studies to ensured construct validity (Chinyemba and Ngulube 2005:13−16; Seow, Chennupati and Foo 2005:44−51). Factor analysis was also conducted to determine the extent to which items loaded on their relevant constructs.

6.2 Data gathering

Most of the data were captured using a 5-point Likert scale (where 1 indicated 'strongly disagree' and 5 'strongly agree'. A few questions required a 'yes' or 'no' answer while others allowed the respondent to express his or her opinion in the space provided. The first part of the questionnaire collected demographic information about respondents (e.g. occupation, department, faculty and field of study). The second part of the questionnaire measured the model constructs as indicated in Table 1 below. A list of interview questions was also compiled which covered functional, security and other matters relating to the use of computer laboratories, policy development and training. Some follow up interviews were conducted with academics to clarify issues raised in the survey.

Table 1 Items used to measure the constructs presented in Figure 1

Item	Good practice: Backup, archiving, use of technology
MER1	How often do you backup e-mails? (1=never; 2=infrequently; 3=monthly;4=weekly; 5=daily)
MER2	How often do you backup other electronic documents (e.g. essays, theses, notes)? (1=never; 2=infrequently; 3=monthly; 4=weekly; 5=daily)
MER3	Where do you backup materials (e.g. G-drive; C-

	drive; Flush disks)?
MER4	How often do you archive electronic documents? (1=never; 2=once a year; 3=twice a year; 4=quarterly; 5=monthly)
MER5	Do you use programs (tools) to organise or extract e-mail?
	Good practice: Security
SEC1	How often do you change your password(s)? (1=never; 2=once a year; 3=twice a year; 4=quarterly; 5=monthly)
SEC2	How often do you share your password with someone else? (1=never; 2=rarely; 3=occasionally; 4=often; 5=very often)
SEC3	What antivirus software do you use?
SEC4	How often do you open unsolicited e-mail? (1=never; 2=rarely; 3=occasionally; 4=often; 5=very often)
SEC5	How often do you scan downloaded material from the Internet for viruses or authenticity? (1=never; 2=rarely; 3=occasionally; 4=often; 5=very often)
SEC6	Do you understand security terminology like SSL, Public key encryption, Trojan?
SEC7	How often do you leave your computer unattended? (1=never; 2=rarely; 3=occasionally; 4=often; 5=very often)
	Good practice: Policies, procedures, responsibility and accountability
PAP1	I am familiar with policies regarding e-mail usage at the university (1=strongly disagree; 2=disagree; 3=uncertain; 4=agree; 5=strongly disagree)
PAP2	I feel the penalties for non-compliance with the university's laboratory policies are fair (1=strongly disagree; 2=disagree; 3=uncertain; 4=agree; 5=strongly disagree)
PAP3	When was the last time you received training on proper usage of the laboratory (IT facilities) at this university? (1=never; 2=more than a year ago; 3=last year; 4=last semester; 5=last month)
PAP4	When was the last time you received training on proper management of electronic records (e.g. training on backup, archiving, disposal or security)? (1=never; 2=more than a year ago; 3=last year; 4=last semester; 5=last month)
RAR1	I know my responsibilities as an e-mail/Internet user at the university (1=strongly disagree; 2=disagree; 3=uncertain; 4=agree; 5=strongly disagree)
RAR2	If you are familiar with your responsibilities as an e-mail/Internet user, how often do you fail to comply with the university rules on e-mail/Internet usage? (1=very often; 2=often; 3=occasionally; 4=rarely; 5=never)

	Compliance with regulation/legislation/policies **(psychological and sociological factors)**
AOL1	Are you aware of the South African *ECT Act* of 2002?
AOL2	Are you aware of the penalties for non-compliance to this *ECT Act*?
AOL3	If you are aware (understand) the penalties of this *ECT Act*; are they fair? (1=strongly disagree; 2=disagree; 3=uncertain; 4=agree; 5=strongly disagree)
	Effectiveness of ERM
EFF1	Extent to which good practices have been adopted
EFF2	Extent to which regulatory and policy requirements have been complied with

6.3 Sampling

Responses consisted of academics, ICTS staff and students from five university faculties (Commerce, Engineering, Humanities, Science and Law). Literature suggests that computing and non-computing students differ in their ethical behaviours and coping strategies (Belanger, Lewis, Kasper, Smith and Harrington 2007 :192−195). This combination of respondents would therefore allow for effective comparison of behaviours. A total of 112 responses were received of which eight were rejected due to incomplete responses. The remaining 104 responses consisted of 97 from students and 17 from academics. All respondents in this study possessed computing skills although the levels differed depending on the major programme pursued or taught.

top

7 Results, data analysis and discussion

7.1 Description of the research sample

Table 2 shows that most student responses were from the Humanities faculty (42%). Of the students from the Commerce faculty, 15 majored in Information Systems (IS) while, in the case of the Science faculty, 10 majored in computer science courses. Of the 17 academics, nine were from IS and Computer Science (referred to as IS/IT academics or academics in the computing field) while the rest were from other disciplines (non-IS/IT academics or academics in the non-computing fields).

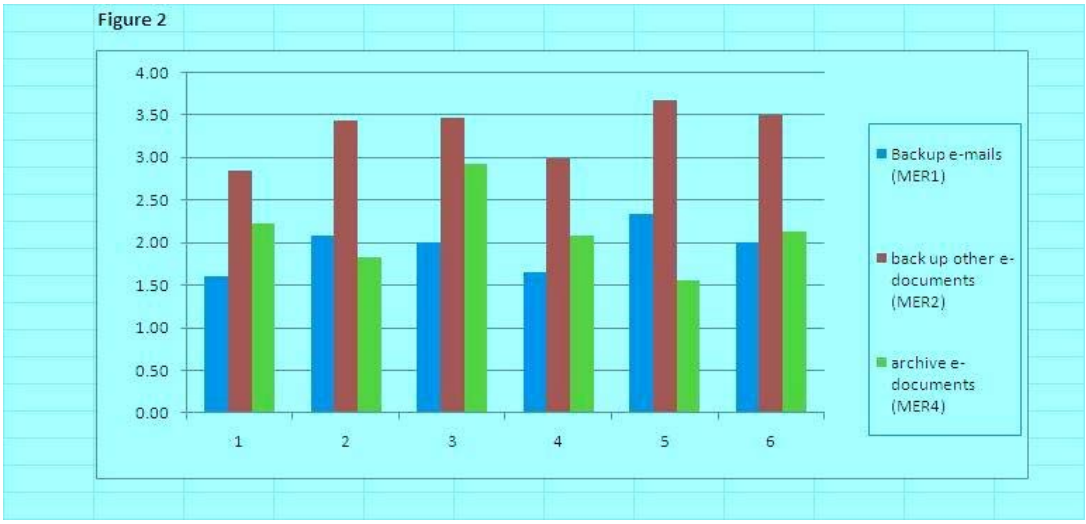
Table 2 Description of the research sample

	Students (*N*=97)	**Academics (*N*=17)**
Faculty	**%**	**%**
Humanities	42	17
Commerce	27	35
Science	24	22
Law	4	17
Engineering	3	9

7.2 Backup, archiving and use of technology to organise or extract records

Figure 2 represents the mean scores by students and academics on the items that measured the extent to which backup and archiving of records was done.

Figure 2 Backup and archiving of records by students and academics



Key:

1=All students (*n*=97)
2=All academics (*n*=17)
3=Students taking IS and Computer science (IS/IT students or computing students, *n*=15)
4=Students not taking IS or Computer science (non IS/IT students or non-computing students, *n*=82)
5=IS and computer science academics (IS/IT academics, *n*=9)
6=Other academics (non-IS/IT academics)

Figure 2 shows that on average both academics and students 'never' or 'infrequently' made backups (MER1 and MER2) and archived (MER4) their data. Further analysis of the responses showed that the few respondents that did backup and archived records were from the the IS and computer science departments. Academics and students in non-computing departments therefore did not seem to engage in these practices.

Furthermore, Table 3 below shows that, for most academics, backup was done on hard disks (C) and shared drives (G) (see MER3, Table 3) while students mainly used memory sticks (USB disks). Very few respondents indicated that they used software tools to extract mail or manage their records (see MER5, Table 3). It was also revealed in the interviews and discussions with respondents that the decision to backup or delete records was mainly influenced by factors such as availability of disk space, personal judgement and administrative responsibilities rather than established procedures or retention schedules. While sensitive electronic records (e.g. memos on decisions taken, responsibilities allocated, tests and examination results) were usually password controlled, records about the data stored (metadata) were never maintained. Users therefore developed their own approaches to record keeping which were sometimes insecure. Similar problems was also observed by Tibbo and Pyatt (2006:6−8).

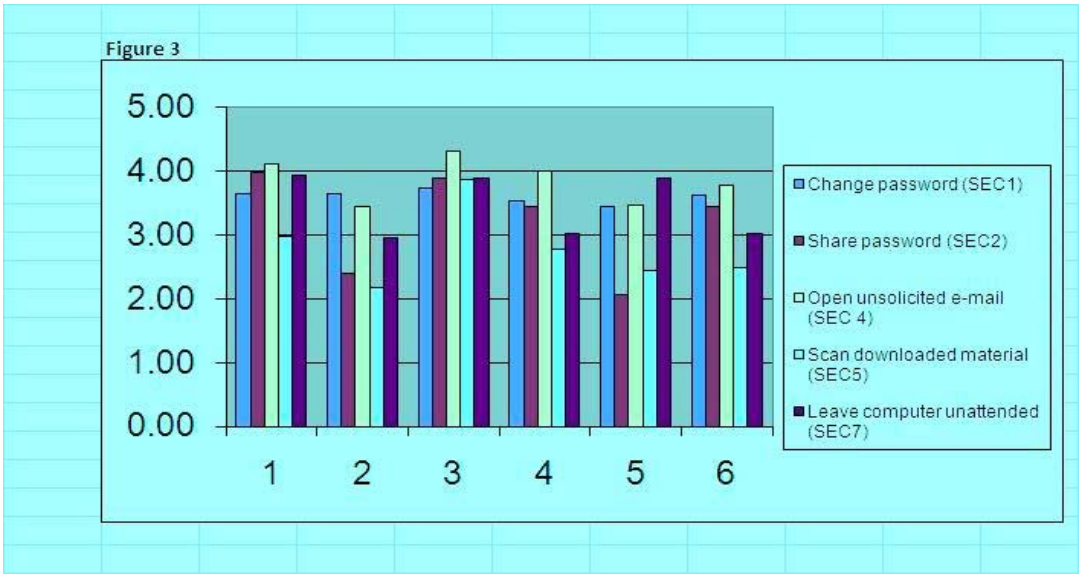
Table 3 Backup location and use of programs to organise or extract e-documents

	Item/response	**Academics**	**Students**
Where do you back up materials? (MER 3)	Hard disk	13	59
	Server	7	16
	Other (USB)	12	97
	Use two or more	8	16
Do you use programs to organise/extract e-mails? (MER5)	YES	7	23
	NO	10	74

7.3 Security

Figure 3 shows that students and academics usually changed their password quarterly (SEC1 is close to 4; score of 4=quarterly). Figure 3 also shows that academics did not allow unathorised use of passwords (SEC2=2,40, response 2) while students sometimes did (SEC2=3,99, response 1). Students also opened unsolicited mail (SEC4=4,12, response 1) and ocassionally left their computers unattended (SEC 5=2,99, response 1) more than academics did (2,17, response 2). The authors also found that the most commonly used anti-virus software was McAfee. Most respondents knew this software, possibly because it was the one installed on the university's network system.

Figure 3 Security practices



Key:

1=All students (*n*=97)
2=All academics (*n*=17)
3=Students taking IS and Computer science (IS/IT students or computing students, *n*=15)
4=Students not taking IS or Computer science (non IS/IT students or non-computing students, *n*=82)
5=IS and computer science academics (IS/IT academics, *n*=9)
6=Other academics (non-IS/IT academics)

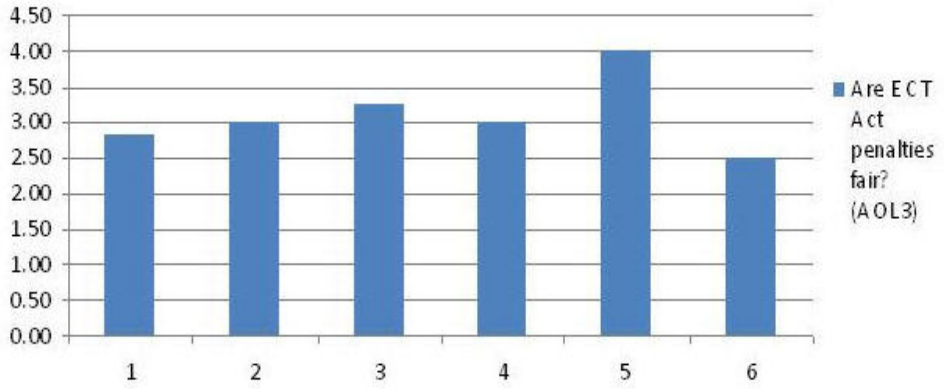
Non-computing students seemed to use their passwords and computers more responsibly, and in accordance with the rules (SEC2=3,45, SEC7=3,03 respectively), than their computing counterparts (3,89 and 3,89 respectively). This is suprising since computing students are expected to have a better understanding of ethics and security risks. Such behaviour may perhaps be attributed to differences in student characterisitics, demographics, culture and disciplines. Gan and Koh (2006:2−3) identify a number of forces that explain the lack of ethical standards. These include giving more emphasis to analytical methods than ethical principles in business programmes. Belanger *et al.* (2007:192−195) examined the coping strategies of computing and non-computing students. Coping strategies are the cognitive and behavioural tactics employed by individuals to work with real or perceived problems such as stress. Computing students were found to adopt the denial or avoidance strategy. They were more emotionally focused, diminishing the importance of the situation and persuading themselves that the problem is not as important as it may appear to be. Non-computing students were more problem focused, accepted the existence of the stressful situation and revised their expectations to change the situation. This 'change the situation' coping strategy was directly linked to academic success for non-computing students but not for computing students.

Non-computing students were also found to differ significantly in terms of age, hours per week volunteering, hours per week studying outside of class and hours per week working at a paying job. Computing students were found to be somewhat older than non-computing students, spend more time using a computer for non-academic activities, spend more time volunteering, work more hours at a paying job and study outside of class. They concluded that computing students are usually very busy people, doing more activities overall than non-computing students and as such face more stressful experiences, which influence their decision to abide by the rules or regulations (Belanger *et al.* 2007:192−195).

7.4 Compliance with legislation and perceptions of penalties

Figure 4 indicates that most students and some academics were not certain about the fairness of the penalties of the *ECT Act* (see response 1 and 2). Only academics in the computing departments seemed to have found these penalties to be fair (see response 5).

Figure 4 Compliance with regulations – fairness of *ECT Act* penalties



Key:

1=All students (*n*=97)
2=All academics (*n*=17)
3=Students taking IS and Computer science (IS/IT students or computing students, *n*=15)
4=Students not taking IS or Computer science (non IS/IT students or non-computing students, *n*=82)
5=IS and computer science academics (IS/IT academics, *n*=9)
6=Other academics (non-IS/IT academics)

Further analysis shows that most students were unaware of the *ECT Act* (Table 4) and did not know the penalties for non-compliance with this regulation. For academics, it was surprising to see that many knew the requirements of the Act but not the penalties involved.

Table 4 Awareness of the *ECT Act* and penalties for non-compliance

	Item/response	**Academics**	**Students**
Are you aware of the *ECT Act*? AOL1	YES	9	20
	NO	8	77
Are you aware of the penalties for non-compliance with the *ECT Act*? AOL2	YES	5	18
	NO	12	79

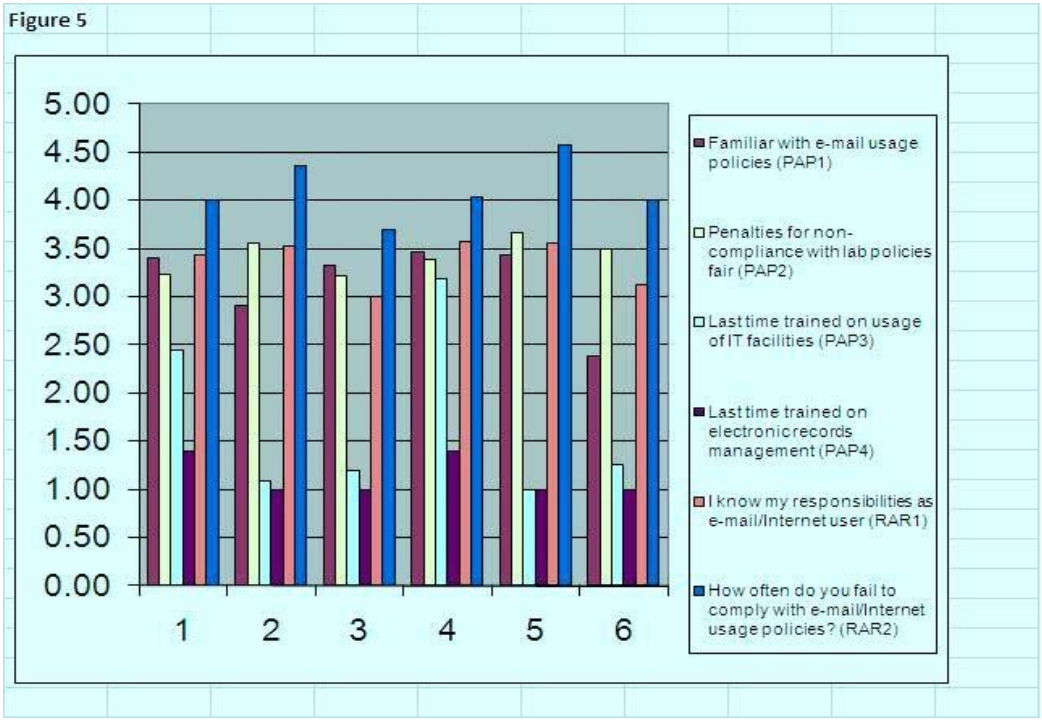
This finding suggests that most users of the university system were unaware of the requirements of the Act governing handling of electronic records and of the implications or liabilities involved. Suprisingly, of the 20 students who indicated awareness of the *ECT Act*, 74% were non-computing students. This could be attributed to the inclusion of law students taking E-Commerce law in their course. Computing students did not learn much about legal aspects of IT in their undergraduate programme. Integration of legal and security aspects at this level is strongly recommended.

7.5 Policies, procedures, responsibility and accountability

Policies and procedures

Figure 5 shows that most students and academics (see responses 1 and 2) were unfamiliar with e-mail usage policies (PAP1=3,40 and 2,91 respectively), were uncertain as to whether the penalties for non-compliance were fair or not (PAP2=3,32 and 3,50 respectively. Training on laboratory usage (PAP3=2,44 and 1,09) was basically conducted once a year while training on proper document management did not seem to have ever been conducted at this institution (PAP4=1,43 and 1,00). Most of the academics interviewed indicated that they had never received training on proper records management since they joined the University. Training and communication have been emphasised in previous studies as imperative for ensuring effective electronic management (Norris 2003:3−9). Lack of policy and guidance in the way electronic records were managed by individuals exposed the university to business loss and legal action. This is a major concern now that academics and students have developed their own distinct approaches to record keeping.

Figure 5 Policies, procedures, responsibility and accountability



Key:

1=All students (*n*=97)
2=All academics (*n*=17)
3=Students taking IS and Computer science (IS/IT students or computing students, *n*=15)
4=Students not taking IS or Computer science (non IS/IT students or non-computing students, *n*=82)
5=IS and computer science academics (IS/IT academics, *n*=9)
6=Other academics (non-IS/IT academics)

Non-computing students (see response 4) were particularly uncertain about e-mail policies and fairness of the penalties for violation of laboratory rules (PAP1=3,46; PAP2=3,38). Students were possibly more aware of laboratory usage rules than academics, simply because they had to accept a copy of these rules before they could log on to a network computer. Also, the presence of laboratory administrators monitoring the laboratories could influence them to obey the rules. However, even with these in place, students still violated the rules. Prior, Rogerson and Fairweather (2002:22) cite the work of Harrington (1996), showing that the effect of codes of ethics on computer abuse, judgement and intentions of IS personnel was very small. They argue that management cannot control people's behaviours solely through a code of ethics.

Responsibility and accountability

Figure 5 (response 1 and 2) indicates that students were more uncertain about their e-mail responsibilities (RAR1=3,44) than academics (RAR1=3,52). When compared with their computing counterparts (RAR1=3,00, response 3), non-computing students seemed to be slightly more certain of these responsibilities (RAR1=3,57, response 4). All respondents (academics and students) indicated that they rarely failed to comply with rules although some of the evidence reported in previous sections suggests otherwise.

The above results reveal that both academics and students had problems with electronic document management, security and understanding of policies, procedures and responsibilities. They also show that studying or having knowledge of IT did not necessarily guarantee adherence to good practices in electronic records management.

7.6 Knowledge of IT security terminology

This section determined the extent to which respondents understood some of the terminology used in a computing environment. The result gives some indication of the levels of awareness of the existing security challenges and the measures or good practices that could be implemented to address these problems. Table 5 reveals that all academics and almost all students in the computing departments were aware of these terms. While non-computing respondents were aware of the threats to their systems or data (e.g. Trojan and worms), they seemed to have limited knowledge of the measures that could be implemented to prevent these threats or attacks.

Table 5 Understanding of information technology/security terminology (SEC 6)

Term	Academics		Students	
	IS/IT (YES)	Non-IS/IT (YES)	IS/IT (YES)	Non-IS/IT (YES)
SSL	100%	13%	80%	9%
Public key	100%	38%	80%	15%

Trojan	100%	75%	93%	52%
Worm	100%	13%	93%	52%
Key-logger	100%	33%	47%	15%

7.7 Factor analysis

To determine the underlying factors explaining the constructs, factor analysis was performed using the varimax normalised rotation method. A factor is a combination of variables that expresses the common element that cut across the combined variables. The results are represented in Table 6 below. Only factor loadings higher than or equal to 0,50 were considered relevant in the present study (Gilbert , Veloutsou, Goode and Moutinho 2004: 381). A factor loading is the correlation of a variable with a factor.

Table 6 Factor analysis (significant loadings >= 0.50 are shown in bold)

	Factor 1	**Factor 2**	**Factor 3**	**Factor 4**
Backup e-mails (MER1)	0.076	**0.659**	-0.027	0.022
Backup other e-documents (MER2)	0.153	**0.725**	0.195	-0.137
Archive e-documents (MER4)	-0.391	**0.634**	0.061	0.262
Change password (SEC1)	-0.054	0.364	-0.206	0.357
Share password (SEC2)	0.051	0.236	**0.597**	0.038
Open unsolicited mail (SEC4)	-0.089	-0.221	0.237	-0.173
Leave computer unattended (SEC7)	-0.024	-0.053	**0.647**	0.460
Fairness of the *ECT Act* penalties (AOL3)	0.054	0.124	0.355	**0.512**
Familiar with university e-mail usage policies (PAP1)	**0.732**	0.088	-0.097	0.096
Fairness of the penalties for non-compliance with laboratory policies (PAP2)	**0.723**	-0.143	0.068	0.187
Last time trained on usage of IT facilities (PAP3)	-0.085	0.146	-0.122	**-0.793**
Last time trained on management of electronic records (PAP4)	-0.095	-0.246	0.202	**-0.503**
I know my responsibilities as an e-mail/Internet user (RAR1)	**0.702**	0.131	0.179	-0.118
Fail to comply with the University's e-mail/Internet usage policies (RAR2)	0.188	0.075	**0.746**	-0.144

As indicated in Table 6, except for MER3 (location of backup data), all three items measuring the first construct (backup, archiving and use of technology) loaded onto the same factor, thereby confirming the validity of these items. MER2 (backup other documents, e.g. essays and notes) explains this construct the best (0,725). Possibly, this is so because these documents are big, cannot be read easily on line and are used throughout the course period. For the second construct (security), SEC1 (frequency of password change) failed to load on any of the factors significantly. However, SEC2 (unauthorised use of passwords) and SEC7 (leaving computers unattended) loaded on Factor 3. RAR2 (how often you fail to comply with the University rules on e-mail/Internet usage) also loaded on this factor and appear to explain it the best. This suggests, therefore, that where there was compliance with the rules, possibilities of inappropriate use of computing resources might be minimised.

With regard to the construct 'policies, procedures, responsibility and accountability', PAP1 (familiarity with e-mail usage policies), PAP2 (familiarity with laboratory policies) and RAR1 (knowledge of responsibilities as an e-mail/Internet user) loaded significantly and highly onto factor 1. PAP3 (last time the respondent was trained on proper usage of laboratory), PAP4 (last time the respondent was trained on proper management of electronic records) and AOL3 (fairness of the penalties of the *ECT Act*) loaded, however, onto a different factor (factor 4). This suggests, therefore, that provision of training on rules, regulations and good practices might have been influenced by perception of fairness of the regulations.

Other measures of compliance with registration, policy requirements and rules were AOL1 – awareness of the *ECT Act* and AOL2 – awareness of penalties. The results (Table 4) indicate that most students were unaware of the *ECT Act* and, as expected, they did not understand the liabilities involved.

top

8 Effectiveness of electronic records management

The effectiveness of record management was measured by the extent to which good practices (EFF1) and regulatory requirements (EFF2) were adhered to. Figures 2, 3 and 5 show that the average scores of all students and academics (see responses 1 and 2) were generally below 3,50 (except for security − see Figure 3). Therefore there appears to be limited backup and archiving of records, inappropriate use of technology, poor security measures and lack of proper training on regulatory requirements and

policies. It was also revealed that few respondents were aware or understood the requirements of the *ECT Act* and related penalties for non-compliance with this Act. These findings confirm our suspicion that academics and students did not manage their electronic records effectively.

top

9 Conclusion and recommendations

This study provides useful insight into the way students and academics manage their electronic records. The findings clearly reveal a number of incidents where both academics and students have not managed their electronic records effectively. There is therefore great need to raise awareness of electronic records management and the responsibilities of students and academics in this process. Much can be achieved through proper education and regular training covering technical, legal and ethical issues. It is imperative that a new course in electronic records management targeting first-year students be introduced. Future research can investigate the structure of this course and its requirements.

The Computer Services unit of the university has the responsibility to provide clear policies regarding electronic records management and this process should involve all stakeholders, including student representatives. Policies should not only focus on technical issues such as bandwidth, hardware and storage space. Much focus on good practices, ethical issues, training and compliance with legislations is essential. Lack of proper policies and failure to communicate these effectively to the university community may render the institution and individuals liable for breach of legislative requirements (e.g. *ECT Act*, 2002).

The finding that non-computing students (non-IS/IT) managed security of electronic records better than their computing counterparts and were more knowledgeable about legal issues causes much concern. This study did not, however, collect information on, for example age, gender and culture, which could possibly provide more insight into the causes of such behaviour. Future studies should examine this problem.

There is also a need for computer services to work in partnership with other departments that engage or have special skills in records management. Discussions with academics and ICTS respondents revealed a lack of collaborative initiative in records management with non-academic units such as library services, legal and audit sections. Bantin (2001:5) argues that this is necessary since all these units have common goals in creating, managing and securing records. This study did not involve library staff and internal auditors, therefore future studies should capture the views of these stakeholders.

The framework developed in this study and the questionnaire used allow for more comprehensive assessment of the adoption of good practices and compliance with regulations. Universities can use this framework to guide future evaluations of academic and student practices and to identify areas for policy improvement.

top

10 Limitations

Only five university faculties were sampled. This excluded representation of the faculties of Health Sciences, Centre for Higher Education Development (CHED) and Graduate School of Business in the sample. The sample size was also small, therefore caution should be taken when generalising the findings. Secondly, information about actual statistics on laboratory usage, laboratory offences and technical audit trails could not be obtained to verify some of the claims made by students.

top

11 References

Atherton, J. 1985. From life cycle to continuum. Some thoughts on the records management-archives relationship. Archivaria 21 :43–51.

Bailey, S. 2007. Beyond compliance? The future of records management. [Online]. Available WWW: http://www.cilip.org.uk/publications/updatemagazine/archive/archive2007/september/beyondcompliance.htm (Accessed 14 March 2006).

Bantin, P.C. 1999. Collaborative models for system design, ECURE 1999: Preservation and access for electronic college and university records. Meza, AZ. [Online]. Available WWW: http://www.asu.edu/ecure/1999/bantin/bantin.ppt (Accessed 18 March 2006).

Bantin, P.C. 2001. The Indiana University electronic records project: lessons learned. *Information Management Journal* 35(1):16-24.

Belanger, F., Lewis, T., Kasper, G., Smith, W. and Harrington, K. 2007. Are computing students different? An analysis of coping strategies and emotional intelligence. *IEEE Transactions on Education* 50(3):188−195.

Chalfant, D. 2005. Facebook postings, photos incriminate dorm party goers. *The Northerner* 11/02/05. [Online]. Available WWW: http://www.thenortherner.com/media/paper527/news/2005/11/02/News/Facebook.Postings.Photos.Incriminate.Dorm.PartyGoers-1042037.shtml (Accessed 10 June 2007).

Chinyemba, A. and Ngulube, P. 2005. Managing records at higher education institutions : a case study of the University of KwaZulu-Natal, Pietermaritzburg Campus. *South African Journal of Information Management* 7 (1). [Online]. Available WWW: http://www.sajim.co.za/peer86.7nr1.asp. (Accessed 10 October 2008).

Cowan, R. and Pember, M. 2007. Promoting records management and archieves research in Australia. *Informaa Quarterly* 23 (4):32−36.

Darlington, J., Finney, A. and Pearce, A. 2003. Domesday redux: the rescue of the BBC Domesday Project vidodiscs. *Ariadne* [Online] Available WWW: http://www.ariadne.ac.uk/issue36/tna/ [Accessed 4 September 2006].

Duranti, L. 1989. Diplomatics: new uses for an old science.*Archivaria* 28(1):7−27.

Duranti, L. 1998. *Diplomatics: new uses for an old science*. Lanham Md.: Scarecrow Pre ss.

Gilbert, G.R., Veloutsou, C., Goode M.M.H. and Moutinho, L. 2004. Measuring customer satisfaction in the fast food industry: a cross-national approach. *Journal of Services Marketing* 18(5):371−383.

Gan, L. and Koh, H. 2006. An empirical study of software piracy among tertiary institutions in Singapore. *Information & Management* 43(5):640−649.

Greenop, M. 2007. Facebook – the CIA conspiracy. *Nzherald.co.nz*. [Online]. Available WWW: http://www.nzherald.co.nz/section/story.cfm?c_id=5&objectid=10456534&ref=emailfriend (Accessed 14 February 2008).

Grossman, D. and Zaelke, D. 2005. An introduction to theories of why states and firms do (and do not) comply with law. I*NECE*. [Online]. Available WWW: www.inece.org/conference/7/vol1/index.html(Accessed 24 April 2006).

Harrington, S. 1996. The effect of codes of ethics and personal denial of responsibility on computer abuse judgements and intentions. *MIS Quarterly* 20(3):257−278.

Harris, K.L. 2008. Adopting retention schedules to electronic records. The big bucket theory. *ARMA*. [Online]. Available WWW: http://www.armautah.org/documents/AdaptingRetentionSchedulestoElectronicRecords.pdf (Accessed 24 September 2008).

Henriksen, H.Z. and Andersen, K. 2008. Electronic records management systems implementation in the Pakistani local government. *Records Management Journal* 18(1):40−52.

Image and Data Manager. 2006. Poor email management cost US dollars 20-million. [Online]. Available WWW: http://www.idm.net.au (accessed 20 November 2006).

JISC. 2004. Developing an institutional records management programme. [Online]. Available WWW: http://www.jisc.ac.uk/media/documents/publications/recordsmanbriefing.pdf (Accessed 7 September 2007).

Johnston, P. and Bowen D. 2005. The benefits of electronic records management systems: a general review of published and some unpublished cases. *Records Management Journal* 15(3):131−140.

Jones, H. and Soltren, J. 2005. Facebook; threats to privacy. [Online]. Available WWW: http://ocw.mit.edu/.../facebook.pdf (Accessed 10 October 2007).

Kahn, R.A. 2004. Records management & compliance: making the connection. *Information Management Journal* 38(3):28−36.

Kendall, M. and Mirza, A. 2006. Framework for university records management. University of Birmingham, Information services. [Online]. Available WWW: http://www.isprojects.bham.ac.uk/RecordsManagement/RMpolicyV11.pdf (Access 22 May 2006).

Kyobe, M.E. 2009. Factors influencing SME compliance with government regulation on use of IT. *Journal of Global Information Management* 17(2):30−59.

Maguire, R. 2005. Lessons learned from implementing an electronic records management system. *Records Management Journal* 15(3):150−157.

Mayne, M. 2006. How are businesses facing up to the compliance challenge? *SC Magazine Australia*. [Online]. Available WWW: http://www.scmagazine.com.au/feature/how-are-businesses-facing-up-to-the-compliance-challenge.aspx (Accessed 30 November 2006).

Mcleod, J., Hare, C. and Johare, R. 2004. Education and training for records management in the electronic environment – the (re) search for an appropriate model. *Information Research* 9(3).

MERIT Report. 2003. Managing electronic records in teaching. JISC, Brunel University. [Online]. Available WWW: http://www.jisc.ac.uk/uploaded_documents/FinalReport11_03.doc (Accessed 20 July 2006).

Michalson, L. and Hughes, B. 2005. Guide to the *ECT Act*. Michalsons [Online]. Available WWW: http://www.michalson.com (Accessed 12 April 2007).

Myler, E. and Broadbent, G. 2006. ISO 17799: standard for security. *Information Management Journal* 40(6):43−52.

Norris, M. 2003. Records management and e-mail. [Online]. Available WWW: http://www.dcc.ac.uk/events/ec-2006/EC_email-arch-rep.pdf (Accessed 7 September 2007).

Preston, R. 2007. InterPARES 1& 2 overview: objectives, methodolgy and outcomes (1999−2007). InterPARES Project. [Online] Available WWW: http://www.interpares.org/display_file.cfm?doc=ip1-2_preston_longrec_2007.pdf (Accessed 12 March 2007).

Prior, M., Rogerson, S. and Fairweather, B. 2002. The ethical attitudes of information systems professionals: outcomes of an initial survey. *Telematics and Informatics* 19(1):21−36.

SANS 15801 [Online]. Available WWW: http//www.mostert.co.za/publications.htm (Accessed 15 May 2008).

Seow, B., Chennupati, K. and Foo, S. 2005. Management of e-mails as official records in Singapore: a case study. *Records Management Journal* 15(1):43−57.

Sletten, L. 1999. Lesson from down under: records management in Australia. Information Management Journal 33(1):26−33.
South Africa Government. 2002. Electronic Communications and Transactions Act of 2002. *Government Gazette* 446(23708). [Online]. Available WWW: http://www.info.gov.za/gazette/acts/2002/a25-02.pdf (Accessed 4 April 2007).

Thelwall, M. 2008. Fk yea I swear: cursing and gender in a corpus of MySpace pages. *Corpora*, 3(1). [Online]. Available WWW: http://www.scit.wlv.ac.uk/~cm1993/papers/MySpaceSwearing_online.doc (Accessed 20 March 2008).

Thornhill, K. 2008. Records management at the University of Lethbridge. [Online]. Available WWW: http://www.uleth.ca/lib/archives/records_Management/display.asp?PageID=227 (Accessed 12 December 2008).

Tibbo, H.R. and Pyatt, T. 2006. Email management, electronic records, and beyond. [Online]. Available WWW: http://www.ils.unc.edu/digitaldesktop (Accessed 7 September 2007).

Underwood, W. n.d. A formal method for analyzing the authenticity properties of procedures for preserving digital records. Georgia Tech Research Institute. [Online]. Available WWW: http://www.iis.sinica.edu.tw/APEC02/program/William.Underwood.doc (Accessed 7 February 2009).

Wamukoya, J. and Mutula, S.M. 2005. Capacity-building requirements for e-records management: the case in east and southern Africa. *Records Management Journal* 15(2):71−79.

Xiaomi, A. 2003. An integrated approach to records management. *The Information Management Journal* 37(4):24−31.

Yin, R.K. 1994. *Case study research: design and methods*. Thousand Oaks, California: SAGE Publications.

Yusof, Z.M. and Chell, R.W. 2002. Towards a theoretical construct for records management. *Records Management Journal* 12 (2):55−64.

ISSN 1560-683X

Published by InterWord Communications for Department of Information and Knowledge Management, University of Johannesburg