Records management and Irish law

Martin Bradley, Archives Consulting Services Ltd

Traditionally the approach towards record-keeping in Ireland has been to keep everything just in case it might be needed for some future, unspecified, requirement. Given the bewildering array of legislation that makes passing reference to record-keeping requirements and responsibilities, from the Organisation of Working Time Act 1997 to the Harbours Act of the same year; from the Criminal Justice Act 1994 to the Electronic Commerce Act 2000, and the lack of any clear Government guidance on the issue, it is entirely understandable that this culture of hoarding has been seen as the best way to proceed. That was until the advent of the Data Protection (Amendment) Act 2003, which has forced a new way of looking at the way people keep records; not only are they breaking the law by keeping everything indefinitely, but individuals are personally liable for penalties up to 5 €100,000 under Section 25 of the Act.

Under the 2003 extension to Data Protection legislation, there was a number of key changes. First, the Act was extended to apply to manual records that are held in an organised filing system (and before anyone asks, pleading that the files are disorganised can't be used as a defence: if it is on a file, then it's part of a filing system). Second, the extension states that appropriate security measures must be taken against unauthorised access to, or unauthorised alteration, disclosure or destruction of, data, and again includes manual records. Third, and possibly most importantly, it states that "data shall not be kept for longer than is necessary" for the original purpose it was collected.

Focusing on point three above, the Web site of the Data Protection Commissioner offers some practical advice: "You should pay particular attention to old information about former customers or clients, which might have been necessary to hold in the past for a particular purpose, but which you do not need to hold any longer. If you would like to retain information about customers to help you provide a better service to them in the future, you must obtain the customers' consent in advance. The same applies to paper records. Good housekeeping would also dictate that you regularly review the need to retain records." This clearly has serious implications for many law firms. The Commissioner further asks three simple questions:

- Is there a defined policy on retention periods for all items of personal data kept?
- Are there clerical and computer procedures in place to implement such a policy?
- Is information about old customers routinely purged from your systems?

I recently spoke at a seminar in the IFSC with **Tom Maguire**, the Deputy Data Protection Commissioner, who summed the issue up quite nicely by saying "as long as you have a records management policy, you won't get into trouble with us; if you don't have one, then this is an issue of concern."

So what does this all boil down to in practical terms? To put it simply, it is no longer acceptable to have a basement containing files on all your customers, past and present, to have ad-hoc arrangements for retrieving and tracking files, or to keep everything indefinitely. How do you ensure that you are not breaking the law? Have a records management policy.

The term 'records management' is still a slightly alien one to most Irish businesses, as it is often confused with document management, knowledge management, information management and any other number of management-speak buzzwords. The situation isn't helped by a variety of companies describing their product or service as records management solutions when they clearly aren't. Off-site storage, scanning, microfilm, document management software and e-mail archiving software can all be parts of a successful records management programme, but none of them is sufficient on its own to ensure legal compliance or, for that matter, administrative efficiency. No, records management boils down to slightly more old-fashioned and unpopular concepts like setting policies and procedures in place, training staff and constant monitoring of systems. Records management cannot be purchased in a box. As a recent records management training brochure produced by CMOD put it: Old rules are still good rules.

Good records management brings with it a number of benefits beyond compliance with legislation, and it certainly should not be viewed as a burdensome exercise that has to be implemented solely for that purpose. A recent study by the University of California at Berkeley came up with the following statistics:

- Offices worldwide used 43% more paper in 2002 than they did in 1999
- The average organisation makes 19 copies of each document, loses 1 out of every 20 documents, and office workers can each spend 400 hours per year looking for lost files
- Between 1% and 5% of all documents are misfiled
- When e-mail is introduced into an office, the percentage of printed documents increases by 40%.

So where did it all go wrong? The 1980s' promise of the paperless office has a lot to answer for. As these statistics show, the more technology that is introduced into an office the more paper records are generated, which would be fine if they

minimal delay. Several companies went under after 9/11 as they had no backups of their key business information

- It enables legal destruction of listed records. Quite simply it is not safe to shred anything unless there is a stated policy that, for the classification of records in question, they are destroyed after x years in line with legal and administrative requirements. If records are destroyed in an ad-hoc manner without a proper audit trail, someone can still be expected to produce these records, and penalised for not having them.

Creating a records management policy need not be a gargantuan undertaking, and there are 4 simple steps to putting the proper procedures in place. Elements of this process can be time-consuming, so many businesses hire in outside help from professional archivists rather than sacrifice staff time, but much can also be accomplished in-house.

- Survey and list all files, electronic and manual. Until the company knows what it has it is impossible to make any decisions about what to keep
- Create a file taxonomy. This is essentially a family tree of the records, normally broken down by department or business function to enable the records to be grouped together and decisions made about how long they are retained on a file series basis, rather than by individual files
- Decide on retention periods. Once a taxonomy is in place, it is possible to assign retention periods to the various series of files created by the business and ensure that they are only held for the correct length of time according to legal and administrative requirements. At this stage, a decision should be made on which are the key series of records that must be held permanently as archives
- Index and reference records. It is essential that the records be found when necessary, so many businesses take the opportunity of retro-actively assigning reference numbers to all their files and linking these to a database in order to find files. This is also the time to put systems in place that ensure that a newly-created record is automatically assigned a reference number to track it throughout its lifecycle.

On completion of this exercise, a number of Irish businesses are moving towards ISO 15489 certification. ISO 15489 is the International Records Management standard, and certification ensures that a business's records management meets that standard. This is useful both from the point of view of internal audit and in assuring its customers, and the regulatory authorities, that records management is taken seriously and has attained a high standard. If the choice is to bring in outside expertise, it pays to talk to people with actual ISO 15489 certifications under their belt: it is very easy to say a company conforms to best practice, but another thing altogether to have the proof. It is clear that ISO 15489 will soon become a benchmark for Irish business (think ISO 9000), and the legal profession in Ireland should certainly look towards certification to ensure that at the very least the requirements of the Data Protection Act are met. ■

Integrating records management requirements into Financial Management Information Systems

The International Records Management Trust (<http://www.irmt.org>) is working with the UK Department for International Development (DFID) on a project to investigate how records management standards and good practices can be integrated into financial information management systems to reduce the misuse, mismanagement or loss of the electronic financial records created in these systems, and to strengthen control of paper-based inputs.

Financial management is at the heart of anti-corruption and transparency efforts, and one of the most fundamental ways that governments are held accountable for their actions is by providing evidence, in the form of financial records, of how public funds have been spent and managed.

Records management standards and good practices, notably the *International Standard on Records Management* (ISO 15489), are available to guide the management of records as evidence. Within the past decade, standards and practices have also emerged for the lifecycle management of electronic records. However, most financial management information systems are implemented without consideration of these standards.

This means that one of the most critical systems for supporting government services and accountability is operating at significant risk due to the lack of systematic processes and controls for the capture, organisation, preservation and long-term accessibility of electronic records. At the same time, inadequate attention has been given to the issues involved in managing paper-based records as a critical part of financial information management systems. As a result, the systems tend to be incomplete and difficult to audit.

This project seeks to provide solutions to these issues by developing model policy statements, management frameworks, functional systems specifications and implementation guidelines for incorporating sound records management principles, processes and controls into financial information management systems. This will be done through an iterative analysis of standards and good practice against the results of field studies and field testing.

More details on the project can be provided by contacting the Trust by e-mail at <info@irmt.org>.

About the author

Martin Bradley has been a professional archivist and international records management consultant since 1997. Since May 2005, he has also been the Executive Director of Archives Consulting Services Ltd, providing consultancy throughout Ireland and the UK. Martin can be contacted at tel: 00 353 87 286 2274; e-mail: <info@archivesconsult.com> or Web: <http://www.archivesconsult.com>.

were kept in any kind of organised fashion. However the confident predictions of the technology industry that paper was a thing of the past, combined with an array of software products sold on the understanding that they did the filing for you, meant that proper records management was suddenly viewed as archaic and unnecessary. That is until the problems started. High-profile instances of Government departments being unable to lay their hands on files have led to costly reactive measures, including hiring teams of unfortunates to back-catalogue warehouses full of files that, if their original filing integrity had been maintained, would have been easily accessible.

When we talk about records management now, however, the situation is more complicated, as there are classes of records that are created and stored in exclusively electronic media. The real danger is that employees view these forms of communication as being personal, whereas they are in fact business transactions. They can be easily traced to the issuing organisation, so a very clear policy must be in place for these services to ensure that nothing libellous or containing sensitive business information about a company or its clients is inadvertently passed on.

E-mail is a key area here. Many people are quite ruthless at maintaining an empty in-box, whereas others tend to only delete information when quotas are breached. In both cases, key company records could be destroyed. If companies recognise the importance of e-mail in this context, they tend to keep everything just in case. The issuing of guidelines on which e-mail constitutes a business record and mechanisms to file them accordingly will help ensure obligations are met, while minimising unnecessary storage costs. E-mails, SMS and Messenger have all been the subject of legal discovery. There is no doubt that e-mail, messaging and SMS have opened up a can of worms for many organisations. For instance, many firms involved in share-trading have had to freeze their employees out from Instant Messaging products such as Yahoo/MS Messenger for fear of sensitive information being leaked. Key findings of a recent US study carried showed that

- most businesses do not preserve e-mail and instant messages in an archiving system; instead they rely on simple tape backups to preserve content from their messaging systems
- current practices in most businesses make it very difficult to recover old e-mail during legal discovery, during a regulatory agency's audit or simply when a user is looking for old content. However, during the past 3 years, the IT departments of nearly 3 in 4 businesses surveyed have been required to search through backup tapes in response to a formal legal, HR or other request. Most organisations have no policies or systems in place to prevent users from deleting messaging system content that is important for the business to retain on a long-term basis
- Less than 50% of businesses have an e-mail retention policy in place, despite the fact that virtually all businesses use e-mail for business applications.

So what steps can anyone take in order to increase efficiency, save storage space and ensure legal compliance? The first thing is to understand the difference between a record and a document. ISO 15489, the *International Records Management Standard*, defines a record as "Information created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business". The key to organising records (both electronic and manual) is being able to identify these key pieces of information and ensure they are properly looked after, while extraneous material (normally around 40% of what is kept by an average business) is disposed of. Once this concept is understood, it is time to produce a records management policy.

A records management policy has 6 key functions:

- It assigns responsibility for ensuring that records are properly kept to staff at all levels. It also explains to staff that records created during company time are not their personal property
- It applies to all records, electronic and manual
- It identifies records at creation, and follows their lifecycle from creation to ultimate archiving or destruction. If someone knows that an e-mail or letter they create will be considered a record, it is easier to ensure it is saved/filed in the right place. I often use the example that an e-mail from the HR Department saying "All lunch allowances are cancelled" is a record, whereas one saying "Where are you going for lunch?" is not. The first one should be saved appropriately, and the other deleted
- It sets out retention periods. A retention period is basically the length of time that a record is kept in an office, how long it is maintained as a non-current record in off-site storage and then whether it is destroyed or maintained permanently after a set period of time. This element is really the key issue for any records management policy, and is the cornerstone of compliance with legal requirements
- It ensures security and business continuity. As we have seen, security is a key element of the Data Protection (Amendment) Act 2003, and it is important to ensure that information in both electronic and manual filing systems is seen only by those who have a need to see it, and perhaps more importantly that it cannot be modified without an audit trail. It also ensures that the business key records are identified and a copy of them kept off-site so that, in the event of a disaster, the company can be back up and doing business with

Insurance firm fined for data protection offence

A travel and insurance agency has pleaded guilty and been fined by Nottingham Magistrates for offences under the Data Protection Act.

The charges were brought by the Information Commissioner's Office (ICO) against the Director and the Company Secretary of Ram Finance and Insurance Services Ltd. for failing to notify as data controllers who used a computer to process personal information. Yohanna Yaro and Rosella Yaro were each fined £300 and ordered to pay £300 costs. They were written to on four occasions since 2004, and failed to respond. They also received a telephone call and a visit from an ICO investigator.

The company, which no longer trades, was given a three year conditional discharge.