

Freedom of Information & Data Protection Legislation

Implications for Libraries

Report to CONUL

January 2005

CONUL Sub-Committee on Copyright and
Regulatory Matters

Introduction

Remit of the Sub-Committee on Copyright and Regulatory Matters

The CONUL Sub-Committee on Copyright and Regulatory Matters was established to address legislative and other aspects of the regulatory framework through research and assess the implications for CONUL member libraries. In July 2002 the Sub-Committee presented a briefing paper on the Copyright and Related Rights Act 2000 to CONUL.

In March 2004 CONUL directed the Sub-Committee to investigate issues for member libraries in relation to compliance with Freedom of Information and Data Protection legislation, and to submit a report.

The remit of the group consisted of four strands:

- an overview of the relevant legislation, emphasising the statutory implications for CONUL libraries
- a survey of current practice
- an outline of policies and practices necessary to ensure compliance
- recommendations.

CONUL Sub-Committee on Copyright and
Regulatory Matters

Convenor

Margaret Flood, TCD

Members

Marie Burke, UCD

Miriam Corcoran, DCU

Monica Crump, NUI Galway

Yvonne Desmond, DIT

Maire Domhnat Kirakowska, UCC

Elizabeth Murphy, NUI Maynooth

Paul Murphy, RCSI

Colette O'Flaherty, NLI

Gobnait O'Riordan, UL

Contents

Introduction	iii
Executive Summary, Conclusions & Recommendations	1
Part A - Legislative Framework	
1. The Data Protection Acts	4
2. Freedom of Information Acts	10
Part B - Policies and Practice	
3. Records Management	13
4. Data Protection Legislation – Checklists of Issues for Library Staff	21
Appendices	
I. Survey of current practice in CONUL libraries in relation to FOI and Data Protection legislation	33
II. Records Retention Schedule	35
III. Bibliography	42
IV. Freedom of Information and Data Protection Legislation: Guidelines for Library Staff	43

Executive Summary, Conclusion & Recommendations

Executive Summary

This Report is intended as an introduction to the responsibilities of CONUL libraries as institutions and library staff as officers of those institutions to ensure compliance with the provisions of the Freedom of Information Acts 1997 and 2003 and the Data Protection Acts 1988 and 2003.

Part A addresses the legislative framework. Part B focuses upon policy and practice, with particular emphasis upon core Records Management requirements. Taking particular account of the findings set out at Appendix I to this Report, the Sub-Committee's conclusions and recommendations focus upon staff awareness, the introduction of systems and procedures and, in particular, staff training.

Part A – Legislative Framework

1. Data Protection Acts 1988 and 2003

The Data Protection Acts 1988 and 2003 specify the conditions, rules and permitted handling and uses of personal data held by all public and private corporate bodies.

This section of the Report sets out the following:

- the key points of relevance in the legislation **(1.2 and 1.3)**
- a summary of definitions embedded in the Acts **(1.4)**
- the main data protection rules and conditions **(1.5)**
- the rights of data subjects **(1.6 to 1.10)**
- responsibilities of data controllers **(1.11 to 1.12; 1.14)**
- the role of the Data Protection Commissioner. **(1.13)**

Data Protection legislation has an immediate and continuing impact upon libraries. **(1.15)**

2. Freedom of Information Act 1997 and Freedom of Information (Amendment) Act 2003

The Freedom of Information Act 1997 (or FOI Act) provides members of the public with statutory rights of access to official information held by public bodies. The 2003 (Amendment) Act broadened the range of material exempted from release, provided for new fee arrangements and scales and introduced certain provisions relating to records of family members and dependants.

This section of the Report sets out the following:

- the key points of relevance in the legislation **(2.2 and 2.5)**
- the definition of 'record' and an overview of rights of access **(2.3)**
- an overview of the FOI process. **(2.6 to 2.10)**

The FOI Acts have implications for how libraries conduct their activities. **(2.6)**

Part B – Policies and Practices

3. Records Management

Records Management is the formal application of systematic controls to the creation, use, maintenance and/or disposal of records. Section 3 of this Report provides guidance on the following

- developing a Records Management policy **(3.2)**
- core components of a Records Management policy **(3.3)**
- implementing a Records Management policy. **(3.4)**

The implications of poor Records Management policy are set out **(3.5)**, as are the implications for libraries **(3.6)**, with recommendations for CONUL libraries **(3.7)**.

4. Data Protection and Freedom of Information legislation – Checklist of issues for library staff

Section 4 contains checklists, which are intended to give some practical guidelines and examples to encourage the development and maintenance of good systems and practices in libraries, and are drawn from a number of sources. **(4.1)**

- Checklist of issues for setting up a Records Management system **(4.2)**
- Checklist of issues for a Records Management policy **(4.3)**
- Checklist of issues for staff working at service desks **(4.4)**
- Sample questions and answers **(4.5)**
- Checklist of issues for staff about their own rights **(4.6)**
- Checklist of issues for staff holding files that might include comments or opinions about individuals **(4.7)**
- Checklist of best practice for Records Management **(4.8)**

Appendices

Four appendices contain the following:

- I** Survey of Current Practice in CONUL Libraries in relation to FOI and Data Protection Legislation
- II** Records Retention Schedule
- III** Bibliography
- IV** Freedom of Information and Data Protection Legislation: Guidelines for Library Staff

Conclusion

The FOI Act 1997 and the FOI (Amendment) Act 2003 have increased the public's right of access to the information created and maintained by all public institutions. These, taken with the Data Protection Acts 1988 and 2003, constitute the most demanding in a series of initiatives by Government and other regulatory bodies to improve corporate governance in the public sector and to become more publicly accountable.

FOI legislation regulates the public sector and the responsibility for compliance rests at corporate level. For CONUL libraries the immediate level of responsibility varies from the National Library, which is fully responsible in its own right for ensuring that it meets the requirements of the Act, to the College of Surgeons, which, as a private institution, is not subject to the legislation. The

majority of CONUL libraries are part of larger institutions and it is with the parent organisation that the major responsibility for compliance rests.

Under Data Protection legislation staff at every level of the institution have responsibilities and obligations. Staff in all CONUL libraries collect, hold or process data as part of their employment. Consequently, they are affected on a day-to-day basis by the Data Protection legislation, as every employee is responsible for ensuring that data is held and processed in compliance with the statutory provisions. For this reason, there is a specific obligation on the library to ensure that appropriate training and systems are in place.

The results of the Sub-Committee's survey (Appendix I) indicate that there is currently a very mixed level of awareness among the staff of CONUL libraries of their individual responsibilities and obligations.

The demands on record-keeping practices in all institutions have increased as a result of the requirements of both Data Protection and FOI legislation. Efficient records management is increasingly being recognised as a strategic necessity for all institutions to enable them to comply with legal and regulatory obligations.

These points form the basis of the Sub-Committee's recommendations.

Recommendations

1. That in order to promote awareness and facilitate discussion, CONUL agree to release Appendix IV, as an information document for all CONUL library staff.
2. That CONUL will develop and promote procedures and systems to ensure compliance with the relevant legislation by
 - a. ensuring the widespread dissemination of this report to relevant officers and appropriate bodies at organisational level and beyond, for comment and consideration;
 - b. facilitating the establishment of a framework that libraries can use to develop and embed procedures;
 - c. arranging for a shared training programme, based upon the procedural framework, to be devised and put in all CONUL libraries.
3. That CONUL members adopt best practice in Records Management (RM) by
 - a. each Library implementing a Records Management Policy in line with the recommendations
 - b. agree standard retention schedules for library specific records in line with the University's Record Management Policy and in consultation with the University Archivist.

CONUL Sub-Committee on Copyright and Regulatory Matters

Convenor

Margaret Flood, TCD

Members

Marie Burke, UCD

Miriam Corcoran, DCU

Monica Crump, NUI Galway

Yvonne Desmond, DIT

Maire Domhnat Kirakowska, UCC

Elizabeth Murphy, NUI Maynooth

Paul Murphy, RCSI

Colette O'Flaherty, NLI

Gobnait O'Riordan, UL

Part A – The Legislative Framework

1. The Data Protection Acts 1988 and 2003

1.1. Introduction

Irish data protection legislation establishes certain rights for individuals over data which contains personal information about themselves and the legislation regulates use of such data in many ways. The Data Protection Acts originated as implementations of the 1981 Strasbourg Convention on the processing of data and they are primarily concerned with personal data that is data about living, identifiable individuals. Several EU directives have since been introduced and transposed into national law, namely Directive 95/46/EC, Directive 2002/58/EC (and now repeated Directive 97/66/EC). Certain rights are established for individuals with respect to how their personal data is gathered and handled and how such data may be processed and used by the data holders. The legislation specifies conditions, rules and permitted handling and uses of such data on the part of data holders and it imposes a range of related obligations, including disclosure.

The legislation is now wide ranging insofar as it effectively applies to all personal data held in all media from print to digital. The legislation applies to personal data held by organisations or individuals. There are some limited exclusions, primarily relating to legal, criminal and security considerations.

1.2. The Data Protection Act of 1988

- the 1988 Act established the principle of the protection of privacy of individuals with respect to personal data held in automated form
- defined individual rights of access to, and review of, personal data held by public and corporate bodies
- established a Data Protection Commissioner to enforce the rights established
- instituted a registration procedure for corporate data holders
- introduced provisions regulating data gathering, data holding and data dissemination
- specified the requisite enforcement and legal frameworks.

1.3. The Data Protection (Amendment) Act, 2003

The 2003 Act amended the 1988 Act in a number of significant ways:

- extended definitions so as to broaden the scope of the legislation, for example:
 - “data” was extended to mean both automated data and manual data
 - covers all data from July 2003 and will cover all prior data from 2007
 - “processing” was redefined in very broad terms embracing all information collecting, storage, access and use stages
 - manual data includes data in “relevant filing systems” i.e. any retrieval system structured by reference to individuals

- improved the rights granted to individuals to access data, to object to data holding or use and to block certain uses
- enlarged the range of responsibilities for data holders in gathering, maintaining, processing and protecting all data containing personal information
- new registration rules broaden the application of the Act considerably by including all but very small or restricted data holders
- new powers and functions are granted to the Data Protection Commissioner and codes of practice may have statutory effect.

The two Acts are cited and construed as one, The Data Protection Acts 1988 and 2003.

1.4. Definitions

Certain terms have particular meaning in the legislation and these definitions establish the essential concepts. The following are some important definitions embedded in the Acts (1988 S.1 (1)):

Data means information in a form, which can be processed. Since 2003 it includes both automated data and manual data. However, the application of certain parts of the Act to existing manual data is deferred until October 2007.

Automated data means, broadly speaking, any information on computer, or information recorded with the intention of putting it on computer.

Manual data means information that is kept as part of a relevant filing system, or with the intention that it should form part of a relevant filing system (see “*Relevant Filing System*”)

Relevant filing system means any set of information that, while not computerised, is structured by reference to individuals, or by reference to criteria relating to individuals, so that specific information relating to a particular individual is readily accessible.

Personal data means data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller (see “*Data Controller*”).

Processing means performing any operation or set of operations on data, including:

- obtaining, recording or keeping the data
- collecting, organising, storing, altering or adapting the data
- retrieving, consulting or using the data
- disclosing the data by transmitting, disseminating or otherwise
- making it available
- aligning, combining, blocking, erasing or destroying the data.

Data Subject is an individual who is the subject of personal data (*any library user, any library employee*).

Data Controller is a person who, either alone or with others, controls the contents and use of personal data – any library staff member who can collect, store, process, edit or delete

any personal data about any living person is a data controller. See the Data Commissioners' document - *A Guide for Data Controllers*.

Data Processor is a person who processes personal information on behalf of a data controller.

Sensitive personal data relates to specific categories of data which are defined as data relating to a person's racial origin; political opinions or religious or other beliefs; physical or mental health; sexual life; criminal convictions or the alleged commission of an offence; trade union membership.

1.5. Main data protection rules & conditions

(1988 & 2003, Section 2 (1)–(7) & S.2A–C)

Under these sections, data controllers are obliged to:

1.5.1. Obtain and process information fairly

- the data subject must be made aware of the purpose in collecting the data, the identity of the data controller and the persons to whom the data may be disclosed and any other information which it is reasonable to think may be fair.
- the data subject either must have given consent to the processing of the data or the processing must be necessary for a number of specified legal or contractual reasons. In the case of 'sensitive personal data' such consent must be given explicitly.

1.5.2. Keep it only for one or more specified, explicit and lawful purposes

- data subjects should know why data is collected
- the data controller must be explicitly aware of the various sets of data and the specific purpose of each.

1.5.3. Use and disclose it only in ways compatible with these purposes

- subject to specific limited exceptions, disclosure of data must be consistent with the purposes for which it was collected.

1.5.4. Keep it safe and secure

- appropriate security measures must be taken against unauthorised access to, or alteration, or disclosure or destruction of the data
- the levels of appropriate security are proportionate to the harm that might result from an unauthorised disclosure.

1.5.5. Keep it accurate, complete and up-to-date

- compliance requires that all procedures ensure the highest possible levels of accuracy

- subject to periodic review and audit

1.5.6. Ensure that it is adequate, relevant and not excessive

- requires that only the minimum amount of personal data is held
- requires that the data controller establish what are the specific criteria to meet this requirement.

1.5.7. Retain it for no longer than is necessary for the purpose or purposes

- requires a defined policy on retention for all items of personal data kept
- procedures in place to implement such policies.

The above three rules apply to all personal computer-held data and to all personal manual data created from the 1 July 2003. However, for manual records created before 1 July, 2003, the obligations are

- to keep data accurate, complete and up-to-date
- to ensure that they are adequate, relevant and not excessive
- to retain them no longer than is necessary for the purpose or purposes will only apply from 24 October, 2007

Until that date the following procedures will apply to personal manual data created before 1 July, 2003:

- provide a copy of his/her personal data to any individual on request (see below)
- correct, erase or destroy any manual personal data that are incomplete or inaccurate
- destroy any personal manual data that are incompatible with legitimate purposes for which it was collected.

1.6. “Fair Processing” provisions (S.2D) entitle a data subject to:

- a copy of the personal data held by the data controller
- know the source and purpose of the data
- the identity of those to whom you disclose the data
- the data subject must comply with specific conditions in making such requests
- the data subject has the right to have inaccurate data erased or rectified
- the data controller is required to reply to requests within specified time periods
- prescribed fees may be charged to the data subject
- the data subject has the right to complain to the Data Protection Commissioner.

1.7. Subject’s right to establish existence of personal data (S.3)

Upon enquiry, data controllers are obliged to fully inform the subject of all relevant data held within 21 days.

1.8. Subject’s right of access (S.4)

These provisions include that - on foot of an application by a data subject - the data controller must inform the data subject whether his or her personal data is processed by or on behalf of the data controller and, if so

- provide a copy of personal data
- describe in writing the categories of data and the purpose of the processing
- state the source of the data
- state the persons to whom the data would be disclosed
- inform the data subject of the logic involved in any automated decision
- the data subject must comply with specific conditions in making such requests
- the data controller is required to reply to requests within 40 days
- prescribed fees may be charged to the data subject
- the data subject has the right to complain to the Data Protection Commissioner.
- See the Data Commissioners' document - *A Guide to Your Rights*.

However a data controller is not required to give access to personal data relating to other individuals unless they have consented.

1.9. Restrictions on right of access (S.5)

- restricted rights of access apply in specified tax, criminal, regulatory, legal and certain other situations.
- restricted rights of access also apply where undisclosed personal data is specifically gathered for statistical purposes and these restrictions also apply to backup data.

1.10. Rights to rectification or erasure data (S.6)

- where there has been a breach of the data protection rules a data controller must correct or erase personal data on receipt of a written request from a data subject and must comply within 40 days.

1.11. Duty of care by data controllers (S.7)

- specifies duty of care with respect to accuracy and other conditions.

1.12. Disclosure of personal data in certain cases (S.8)

- The restrictions on the processing of personal data do not apply in specified criminal, legal and security and other, contexts, (such as if disclosure were required urgently to prevent injury or damage to someone's health) under Section 8 of the Act.

1.13. Data Protection Commissioner

The Office of the Data Protection Commissioner is established under the 1988 Act to perform the designated functions of enforcement (S.10). The Commissioner may investigate any of the provisions of the Acts either directly or on foot of complaints. The Commissioner is empowered to

require data controllers to furnish any required information within a specified time. If contraventions are found, the Commissioner may serve an enforcement notice to the data controller(s) to ensure required compliance. Non-compliance with enforcement notices constitutes an offence in law. There is provision for an appeals procedure.

The Commissioner is obliged to encourage trade and representative associations, and related bodies, to prepare appropriate codes of practice which, if approved as being in conformance with the legislation, may in turn be deemed to be statutory instruments.

Under Section 11, the Commissioner may prohibit the transfer of personal data outside the European Economic Area.

1.14. Registration

Sections 16–20 of the 1988 Act required all designated data controllers to register with the Commissioner. Registration is at the institutional level: on the current register, there is one entry for each of the universities and colleges. These Sections were reviewed in the 2003 legislation and the scope broadened to include virtually all but the smallest data holders. Registration and renewal fees are payable. It is an offence not to be registered.

1.15. Implications for libraries

Universities and their libraries, holding significant volumes of personal data, are required to implement the applicable conditions of the legislation through appropriate policies, procedures and systems. Co-ordination of Data Protection policies must be centrally organised within institutions. Data Protection legislation has an immediate and continuing impact upon libraries as library staff continually process data about students and staff of their institutions. The duty of compliance resides at all levels within libraries and with each library staff member with access to any personal data. For instance, the legislation prohibits the revelation of either registration or loan information to any third party; all personnel related records within libraries are also included. Libraries are obliged to respond promptly and appropriately to requests for disclosure and are subject to investigation by the Data Protection Commissioner. Appropriate systems and training must be in place in all functional areas to ensure compliance.

Bibliography

Guidance documents on the Acts available from the website of the Data Protection Commissioner <http://www.dataprivacy.ie/index.htm> [accessed 2.7.04]:

- Texts of the Acts, European Union Directives and Statutory Instruments
- Composite text in one of both the 1988 and 2003 Acts
 - <http://www.dataprivacy.ie/images/CompendiumAct.pdf>
- Data Protection (Amendment) Act, 2003 - A Summary Guide
- Data Protection Acts, 1988 and 2003 - A Guide for Data Controllers
- Data Protection Acts, 1988 and 2003 - A Guide to Your Rights
- Self-assessment checklists for data controllers

The Acts and Statutory instruments are also available on the Irish Statute Book site <http://www.irishstatutebook.ie/>

2. Freedom of Information Act 1997 and Freedom of Information (Amendment) 2003

2.1. Introduction

The Freedom of Information Act 1997 came into being to provide a statutory right for members of the public to access official information held by public bodies. The Act was first implemented in Government Departments in 1998 and applied to third level educational institutions from October 2001. These Acts in conjunction with the Data Protection Acts 1988 & 2003 ensure that the rights of individuals are protected, that records are accurate and that access to information is made as simple as possible.

2.2. Freedom of Information Act 1997

Essentially the Act establishes 3 statutory rights

- right to access information held by public bodies
- right to have personal information in a record amended where it is incomplete, incorrect or misleading,
- right to obtain reasons for decisions affecting the person.

The Act also established the independent Office of the Information Commissioner to enforce the legislation including the role of reviewing decisions made by public bodies under the legislation.

2.2.1. Section 15 and Section 16

The most immediate impact of the Act was the legal obligation imposed on public bodies to provide S.15 and S.16 manuals. These must clearly describe the way the body is organised, its functions, the services it provides to the public and how these can be accessed. The kinds of decisions they makes and how they are arrived at, the types of records held and a procedure for accessing them and the internal rules, procedures, guidelines used in the decision making process. It must also describe how decisions made by the body can be reviewed and what avenue of appeal exists.

The purpose of these manuals is to help the public to decide what kind of information the body holds and how they can access it. S.15(3) clearly states that bodies must have regards to the needs of the public when compiling the manuals so for example heavy use of jargon would be seen as contrary to the provision of these sections. These manuals are required to be published, but the 2003 Amendment Act introduced a minimum publication requirement via electronic means. Initially many were produced in hard copy but increasingly they can be found on the Web. A revised version should be prepared every 3 years and as soon as possible after any significant change.

2.3. Records and right of access

2.3.1. What is a record? (S.2)

As defined by the 1997 & 2003 Acts a record" includes any memorandum, book, plan, map, drawing, diagram, pictorial or graphic work or other document, any photograph, film or recording (whether of sound or images or both), any form in which data (within the meaning of the [Data Protection Act, 1988](#)) are held, any other form (including machine-readable form) or thing in which information is held or stored manually, mechanically or electronically and anything that is a part or a copy, in any form, of any of the foregoing or is a

combination of two or more of the foregoing and a copy, in any form, of a record shall be deemed, for the purposes of this Act, to have been created at the same time as the record;”.

2.3.2. What records can be requested?

1. Records created after the commencement of the Act in April 1998 (i.e. 21 April 1998)
2. All personal records and records containing personal information irrespective of when created
3. Any other record deemed necessary to the understanding of a current record
4. Personnel records of staff in public bodies after 1995. Earlier records may be accessed if they are being used in a way that may adversely affect the interests of the staff member involved.

Given the wide-ranging definition of what constitutes a record it is wisest to assume that all records held by an Institution fall under the Act unless they are subject to the stated exemptions. Examples of such exemptions are information obtained in confidence (S.26), commercially sensitive information (S.27), information that would prejudice the functions or performance of a public body or adversely affect its negotiation process (S21), records concerned with the deliberations of public bodies (S.20). Records containing the personal information of other people (s28) and Section 30 protect research and development before it comes into the public domain.

Each request is dealt with on a case by case basis. When an institution refuses to release information it must make a cogent argument that to do so will cause it harm or injury and public interest tests, contained in several of the exemptions, must be satisfied.

2.4. The Process

The Act clearly lays out how a request is to be made in Section 3 7 and emphasises the duty of the public body to assist the person (a requester) making the request. S.8(4) states the motive of a requester cannot be taken into account but the Information Commissioner has decreed that S.8(4) allowed for the motive of a requester to be taken into account if a request is “frivolous or vexatious”.

Public bodies have appointed FOI Officers and designated decision makers for the relevant areas of their organisations.

The Act details the time limits to be applied. An internal review must be requested within 4 weeks of notification to the requester of the initial decision with a decision issued by the public body within 3 weeks of receipt of such request. An external review to the Information Commissioner must be sought within 6 months. His/her decisions are binding but can be appealed. to the High Court on a point of law.

2.5. Freedom of Information (Amendment) Act, 2003

The basic purpose of this Amendment was to increase the level of protection afforded to key areas of government activity, and parliamentary matters as well as to make a series of small amendments to improve the workings of the Act. The scope of some exemptions was increased. Following the Amendment Act an upfront fee of €15 was imposed for requests for non-personal information, €75 for internal review and €150 for review by the Information Commissioner.

S.17 and S.18 were amended to give the right to parents, guardians and next of kin to amend records of their children or relatives and to be given the reasons for decisions affecting such children or relatives.

2.6. Implications for Libraries

The Freedom of Information Acts 1997 and of 2003 have implications for how libraries conduct their activities. To allow Libraries to respond in the necessary timescales set down in the Act there is a need for each library to have a records management system, which permits easy and efficient retrieval of information. There should be a policy on records keeping stipulating what records shall be kept and for how long and ideally, one member of library staff should be given responsibility for this area. The reasons for any decisions should be clearly documented with reference to the appropriate policies that might apply to the decision making process. Care should be taken to ensure that any information kept is accurate, factual and relevant to the matter in hand. Records should be simply written, free from jargon, personal comment or speculation and should be signed and dated where possible. All draft copies should be removed and only the final record kept.

As information brokers it is the responsibility of each member of library staff to be aware of the rights and obligations conferred on the public by these Acts and to be sufficiently aware and trained to assist any member of the public with an FOI request.

Bibliography

Short Guide to Freedom of Information Act 1997 : Dept of Finance, Freedom of Information Central Policy Unit

<http://www.foi.gov.ie/>

Office of the Information Commissioner (both text and guides)

<http://www.oic.gov.ie/>

Comhairle Justice: Citizens Information. Freedom of information: your rights

<http://www.cidb.ie/live.nsf/0/8025636c004d1a8d80256778003f3fa2?OpenDocument>

Part B – Policies and Practice

3. Records Management

3.1. Introduction

Records management is the formal application of systematic controls to the creation, use, maintenance and/or disposal of records. The international standard for records management developed by the International Organisation for Standardisation (ISO) defines records as "information created, received, and maintained as evidence and information by an organization or person, in pursuance of legal obligations or in the transaction of business" (ISO 15489, clause 3.15, 2001). It also states that the role of records management is to support the continuing conduct of business, to comply with the regulatory environment, and to provide the necessary accountability, organizations should create and maintain authentic, reliable and useable records, and protect the integrity of those records for as long as required.

Apart from the benefits of increased organisational efficiency, records management, as a formal process, has been driven by legislation that seeks to increase public accountability, most notably the Freedom of Information Acts 1997 and 2003 and the Data Protection Acts 1988 and 2003 (FOI & DP Acts) discussed in Part A above. In her 2003 annual report, the Information Commissioner states that "Good records management practice is critical from an FOI perspective..." and also alludes to the provisions of the DP Acts. (http://www.oic.gov.ie/report03/221e_20a.htm)

Although these Acts do not legally require a records management policy, the FOI Acts legislate for access to information and the DP Acts state very specifically how information is to be created, maintained, stored and retained/disposed.

3.2. Developing a Records Management Policy

A records management policy identifies how records are used within an organisation. It acknowledges and identifies, at a general level, the records that need to be created and maintained to support core business functions, to satisfy legal requirements and to meet stakeholder expectations. It also identifies requirements such as form, content, retention, disposal and access. These requirements need to be identified with regard to the organisation's exposure to risk if records are not effectively created or managed.

The objectives and intended outcomes of a records management policy need to be identified during the initial stages of policy development. The target audience, that is, all staff within the organisation, needs to be identified and involved in this process to address any existing issues they may have and to foster their support and adoption of the final product.

The role of records within an organisation will be affected by the organisation's regulatory environment. A records management policy needs to identify any legislation that affects the records administered by the organisation, such as the FOI and DP Acts. The regulatory environment also includes voluntary standards or codes of practice with which the organisation has chosen to comply.

The existing records management environment of the organisation also needs to be understood in order to develop a relevant and practicable policy. This includes identifying strengths and weaknesses, and how records management is currently supported and controlled within the

organisation. This will involve evaluating existing policies, practices and procedures to decide whether they will be integrated within the new policy, or replaced.

As a framework, a records management policy needs to be simple and concise. The policy does not need to include any detailed advice on operational procedures or tools (such as classification schemes or disposal schedules). However, such products will need to be developed to support the policy. The policy document needs to be easy to understand, and present its directives and responsibilities in a clear and simple manner. It must contain accurate, relevant and up-to-date information.

A records management policy framework may be delivered through a variety of disparate documents. However, the creation of a single comprehensive organisational policy statement is a more effective way of controlling and communicating a strong records management culture.

3.3. Core Components of a Records Management Policy

3.3.1. Purpose

This statement defines the aims of a records management policy. For example:

The purpose of this policy is to establish a framework for the creation and management of records within this organisation. This organisation is committed to establishing and maintaining records management practices that meet its business needs, accountability requirements and stakeholder expectations.

3.3.2. Policy statement

This statement outlines the organisation's commitment to records management. It needs to define the records management policy as the framework for the organisation's records and their management processes. It could also provide a brief background on records, records management and the regulatory environment of the organisation. Any other important influences or interests specific to the management of records within the organisation could also be outlined here. For example:

This organisation's records are its corporate memory, and as such are a vital asset for ongoing operations, providing valuable evidence of business activities and transactions.

This organisation is committed to implementing best records management practices and systems to ensure the creation, maintenance and protection of accurate and reliable records. All practices concerning records management within this organisation are to be in accordance with this policy and its supporting procedures.

3.3.3. Scope

This statement identifies and defines who and what the policy applies to. For example:

This policy applies to all staff within this organisation.

This policy applies to all aspects of organisational business, all records created during business transactions, and all business applications used to create records regardless of format.

This policy applies to all areas and locations of work within this organisation.

This policy provides the overall framework for any future records management policies, practices or procedures.

3.3.4. Legislation and standards

This statement identifies the regulatory environment, as it affects records management within the organisation. It also acknowledges any voluntary standards, codes of practice or guidelines that the organisation has chosen to adopt. For example:

This organisation will develop records management systems that capture and maintain records with appropriate evidential characteristics in accordance with its obligations under the following pieces of legislation:

- Data Protection Acts, 1988 & 2003
- Employment Equality Act, 1998
- Freedom of Information Acts, 1997 & 2003
- Organisation of Working Time Act, 1997
- Safety, Health and Welfare at Work Act, 1989
- Safety, Health and Welfare at Work (General Applications) Regulations, 1993
- Unfair Dismissal Acts, 1977 & 1993.

This list is not exhaustive. An increasing body of legislation presenting retention periods for records means that the above list will be extended.

This organisation is committed to best practice in records management, and will develop records management systems consistent with the ISO 15489, the international standard for records management.

3.3.5. Records management systems

This statement identifies the records management systems of the organisation and mandates their exclusive use to promote compliance amongst staff. However, this information needs to remain general, so that the policy will remain relevant even if specific records management systems are superseded during its projected life. This statement could also outline the key records management processes undertaken by the identified systems. Existing operational policies or procedural guidelines that control any of these processes can be linked here to the policy framework. For example:

This organisation's primary records management system is an electronic records management system. All paper-based records received in the organisation from [*specify date*] are captured within this system through digital imaging.

This organisation's records management systems are dedicated to the creation and maintenance of authentic, reliable and usable records for as long as they are required to effectively and efficiently support business functions and activities.

The records management systems will manage the following processes:

- creation or receipt of records
- accuracy, relevance, integrity and authenticity of records
- security of records
- access to records
- retention/disposal of records

3.3.6. Responsibilities

This statement outlines the various records management responsibilities within the organisation, assigning them to an individual, level and/or area within the organisation. Despite specific accountabilities, it also identifies that all staff are accountable for records management. For example:

The President/Director is responsible for the authorisation of the records management policy. The President must oversee the management of this policy within this organisation.

Senior administrators/officers are responsible for the management of this policy through resource allocation, and other management support.

The Records Manager is responsible for overseeing the design, implementation, and maintenance of this records management policy, as well as monitoring compliance.

The system administrators are responsible for maintaining the technology for this organisation's records management systems.

Departmental/office managers are responsible for supporting and monitoring staff records management practices as defined by this policy.

All staff are responsible for complying with the records management processes and procedures as defined by this policy.

3.3.8. Monitor and review

This statement sets a date for review. It may also be used to set up monitoring and review procedures, such as an audit committee. For example:

This policy is scheduled for review in [*specify date*]. This review will be conducted by an internal audit committee established by senior management.

3.3.8. Authorisation

This statement authorises the policy with an appropriate signature and date. For example:

This policy has been approved by:
[Name of President/Director], [Date]
[Signature]

3.3.9. Definitions

This statement is a list of definitions to clarify certain terms used within the policy. For example:

Records means any information, in any format, created, received, and/or maintained by officers or employees in the course of their duties on behalf of the organisation.

Active Records means records that are required and referred to constantly for current use, and that need to be retained and maintained in office space and equipment close to users.

Semi-active Records means records that are referred to infrequently and are not required constantly for current use. These are removed from office space to lower cost off-site storage until they are no longer needed.

Inactive Records means records for which the active and semi-active retention periods have lapsed and which are no longer required to carry out the functions for which they were created.

Archives are defined as records that include those with legal, operational, administrative, historical, scientific, cultural and social significance.

Records Management means the formal application of systematic controls to the creation, use, maintenance and/or disposal of records.

Records Retention Schedules means control documents that specify the periods of time, varying from a few months to permanency during which a record has to be maintained. This is determined by statute, legal, regulatory or business compliance, or where these do not apply, by a best assessment of risks involved in destruction against the costs of retention.

3.4. Implementing a Records Management Policy

A records management policy needs to be implemented as a distinct control mechanism in the organisation even if it has been developed alongside other records management products, such as detailed procedure manuals. This will help to ensure that staff clearly recognise the corporate mandate for records management in the organisation. Steps towards successful implementation include:

3.4.1. Promotion

A records management policy needs to be widely promoted to clearly inform staff of its contents and implications, and most importantly, to make staff aware of their responsibilities as defined within the policy. However, it is also vital to promote staff compliance with the policy. The responsibilities of all staff members can be made conditions of employment in job descriptions and performance management procedures. It may also be useful to highlight how poor records management may affect individual staff and the organisation through legal action or media exposure.

The support of senior management is vital when promoting policy. This needs to be made visible through clear authorisation of policy, allocation of appropriate resources, and subsequent monitoring of organisational compliance. This support could also be documented in the employment contracts of senior management, to mandate and create incentives for the effective management of good record management practices within the organisation.

3.4.2. Training

Staff who can effectively implement the directives of policy are critical to its success. Staff training is essential for this purpose, ensuring that staff do not merely understand their records management responsibilities but are able to carry them out.

3.4.3. Supplementary guidelines and procedures

To accompany the policy framework, supplementary guidelines and procedures will need to be developed within the organisation. See Appendix II (b) for an example of a Records Retention Schedule in place in a university learning resource centre.

3.4.4. Monitoring and review

The success of a records management policy depends on effective monitoring and review mechanisms, to ensure its proper and continued use and relevance. Ideally this would be undertaken at a set time after policy implementation, and continued on an ongoing basis. It would involve:

- evaluating the policy document for comprehensibility and relevance
- measuring policy impact and results against initial objectives

- looking for unforeseen effects
- surveying organisational awareness of policy and contents
- monitoring staff adoption and application of policy.

3.5. The implications of poor Records Management

The interrelationship between records management practice and public accountability is best demonstrated by some case histories. For example, in 2003, the Data Commissioner found that a company had breached the security requirements of the DP Acts as adequate safeguards regarding access to the data, which resulted in an individual's personal data being disclosed to a third party without consent, were not in place (Data Commissioner Annual Report 2003, p.35). In another case involving the publication of personal data relating to individuals making FOI requests in a personal capacity (as opposed to a professional or business capacity), the Data Commissioner advises that such practice "constitutes a disclosure under the Data Protection Acts 1988 and 2003" (Data Commissioner Annual Report 2003, p.45).

In her reviews in 2003, the Information Commissioner "came across two particular situations demonstrated the importance of a proper records management policy in relation to the destruction of records." (See the Annual Report of the Information Commissioner 2003 http://www.oic.gov/report03/221e_20a.htm). The same report documents a separate issue relating to records management, which arose in a review involving the Athlone Institute of Technology where the Commissioner found that the retention period for the relevant records had not been appropriate to meet the legislative requirements.

As demonstrated by these cited cases, poor records management can contribute to non-compliance. Non-compliance can incur heavy penalties, up to €100,000 in the case of the DP Acts. In addition, poor records management can also result in a lack of confidence in the organisation, not to mention the bad press that publicised legal cases can generate.

3.6. Implications for libraries

3.6.1. Institutional policy

Many of the CONUL libraries' parent institutions have already introduced records management policies as detailed in Appendix I - Survey. Any records management practices in the library would need to be informed by institutional guidelines or best practice (see Appendices I-IV for some guidance) where none exists.

3.6.2. Obtaining personal data indirectly

Under DP legislation, an organisation is obliged to inform individuals (data subject) from whom it is obtaining data, why it is required and if it will be disclosed to any third parties. In disclosing data to third parties, the data subject must be given the identity of the third party, the reason the data is required and any other information relevant to the specific circumstances. This is usually done at the time the data is collected and in third level institutions where students are concerned this would be at registration. This means that the data subject would need to be informed if his/her personal data is disclosed to the library and to what purpose it is required, etc. However, this would not include users who register directly with the library.

3.6.3. Third party disclosure

Under DP legislation, records must be kept secure and not made available to third parties without consent. Front-line staff are particularly vulnerable to breaching this law if they are not fully aware of the legislation. For example, a staff member at a Circulation Desk may be innocently asked by a user to disclose the name of the borrower of an item required by that user.

3.6.4. Currency of records

Under FOI and DP legislation individuals have a right to amend their own personal record and in addition, under DP legislation, records must be kept up-to-date. Most CONUL libraries obtain their student records from the central registration office so any update to common information made directly to the library would not be made to the central registration record. In addition, there may be a delay in supplying amendments from the central registration office to the library.

Under DP legislation, if the organisation fails to maintain accurate, complete and up-to-date data, it may be liable to an individual for damages under the duty of care provision applying to the handling of personal data.

3.6.5. Defaulters

Under FOI and DP legislation, individuals have the right to access their records and in addition, under DP legislation, records may only be retained for as long as is necessary to fulfil a specified purpose. Information regarding users will be provided to other sections of the institution as appropriate. As such, the library is responsible for the recording and maintenance of this information. Ideally, library regulations would include the full procedures for dealing with such issues, including the procedure for recording details.

3.6.6. Manual records

Certain parts of the Data Protection (Amendment) Act, 2003 will only apply to manual data (i.e. files which are part of a relevant filing system created prior to enactment i.e. July 2003) and from the 24 October 2007, such data will need to:

- be accurate, complete and up-to-date
- be adequate, relevant and not excessive
- be retained for no longer than is necessary for the specified purpose
- in the case of personal and sensitive personal data, comply with at least one of a number of extra conditions.

Although a lot of personal data held in libraries is now computerised, data such as staff records and inter-library loan forms will still be held manually. There may also be other files holding personal data that have not been updated since July 2003 such as correspondence, manual files pre-dating computerisation, etc.

3.7. Recommendations

It is recommended that CONUL libraries:

- adopt institutional retention schedules where appropriate and where no institutional retention schedule exists to deal with specific library-related records, seek advice from the records manager and contact other libraries to agree an appropriate schedule

- lobby the parent institution to introduce a records management policy where none exists and apply best practice in the interim
- comply with institutional guidelines and seek advice from the records manager when necessary where an institutional records management policy is in place
- have very clear guidelines for front-line staff
- ensure that the purpose to which data collected directly by the library is made known to the data subject at the time of collection
- ensure that any use, outside of normal administration, made of data received from another source, e.g. central registration office, is made known to the data subject
- who receive student records from the central registration office advise students to update their records via the central registration office
- who receive student records from the central registration office ensure any updates made by the central registration office are immediately effective in the library
- ensure information regarding defaulters is appropriately recorded, maintained and processed
- examine manual records created before July 2003 to ensure compliance with the DP Acts before 24 October 2007.

Bibliography

This statement is a list of resources for further information. It may include contact details of relevant staff within the organisation as well as reference material. For example:

- Archives Ireland - <http://www.archives.ie/rmanagement.htm>
- ISO 15489-1:2001 Information and documentation – records management – part 1: general. International Standards Organization.
- ISO/TR 15489-2:2001 Information and documentation – records management – part 1: guidelines. International Standards Organization.
- JISC infoNet - http://www.jiscinfonet.ac.uk/InfoKits/records-management/index_html
- Shepherd, Elizabeth & Geoffrey Yeo. Managing Records: a handbook of principles and practice. London: Facet Publishing, 2003.

4. Data Protection and Freedom of Information Legislation Checklists of Issues for Library Staff

4.1. Introduction

Part A of this document clearly outlines the legislative framework and associated implications arising from the Data Protection Acts 1988 and 2003 and from the Freedom of Information Acts 1997 and 2003.

Because all library staff are collecting, holding or processing personal data as a legitimate part of their daily employment, they are affected directly by the Data Protection legislation. Every member of library staff is responsible for ensuring that personal data is held and processed in accordance with the legislation and can be held personally liable. Equally, under Freedom of Information legislation, there is an obligation for libraries to have records management systems that are easily accessible and provide for the efficient and timely retrieval of information.

The checklists contained in this section are intended to give some practical guidelines and examples to encourage the development and maintenance of good systems and practices in our libraries. They are not intended to be exhaustive and should be read in conjunction with institutional and library guidelines and policies. Advice should also be sought from institutional Data Protection and Freedom of Information Officers and in matters of specific legal interpretation advice should be sought from the office of the Data Protection Commissioner at www.dataprivacy.ie

The checklists are based on the SCONUL produced document “¹Data Protection Issues: Checklists for Libraries” and on good practice examples received from a number of academic libraries and their institutional Data Protection and Freedom of Information offices. (See Data Protection Issues: Checklists for Libraries / prepared by Karen Senior for the Advisory Committee on Access to Information Systems and Services of SCONUL (Society of College, National and University Libraries)).

4.2. Checklist of issues for setting up a Records Management system

Libraries necessarily need to collect and retain information for a variety of purposes in the course of their business. Records are legitimately kept about both staff and library users.

Typical examples of records in each category include:

User Records	Staff Records	Administrative Records
<ul style="list-style-type: none"> ▪ Borrower records with associated personal data (addresses, phone numbers) ▪ Recalls ▪ Reservations ▪ Overdue and fines records ▪ Cash transactions ▪ Inter library loan records ▪ Photocopying requests ▪ Enquiry forms ▪ Room bookings ▪ Copyright data on requesters of theses ▪ External borrower records (reciprocal, corporate, graduate member, long term visitors, ALCID etc) ▪ Registration forms ▪ Access forms ▪ Disability records ▪ Passwords ▪ Incident/Accident reports and medical details ▪ Queries ▪ Suggestions ▪ Complaints ▪ Rule infringement records ▪ Correspondence ▪ Photographs of users 	<ul style="list-style-type: none"> ▪ Personnel files with addresses, phone numbers and other personal data. ▪ Salary details ▪ Expenses ▪ Applications ▪ CVs ▪ References ▪ Results of recruitment processes ▪ Probation records ▪ Annual leave and absence records ▪ Staff development and training records ▪ Time in lieu and overtime records ▪ Results of performance management processes ▪ Grievance/disciplinary information ▪ Correspondence ▪ Information about staff held on library/university websites including photographs 	<ul style="list-style-type: none"> ▪ Donations ▪ Budget allocations ▪ Accounts ▪ Supplier details ▪ Contractor details ▪ Order records ▪ Invoices ▪ Contracts ▪ Licences ▪ Results of tendering exercises ▪ Health and Safety records ▪ Security incidents ▪ Telephone log ▪ Diaries ▪ Minutes of meetings ▪ Correspondence

There are **8 guiding principles** or rules underpinning Irish Data Protection legislation and all must be considered when setting up any records system; manual or computerized and for any of the above data types.

1. Obtain and process information fairly

- At the time when the information is collected about individuals, are they made aware of all the uses for that information?
- Are individuals made aware of any disclosures of their data to third parties? This might include fines data to Registry or borrower data to alumni associations.
- Has consent been obtained from individuals for any secondary uses of their personal data?
- Are our records management systems and practices open and transparent?
- Has responsibility for the maintenance of all record types been clearly assigned?
- Has permission been obtained to keep, copy or use photographs of individuals?
- If your library uses CCTV surveillance, it is essential to have notices in place alerting users to the presence of the cameras Guidelines on the use of CCTV cameras is available from the Commissioner's website at (<http://www.dataprotection.ie/viewdoc.asp?m=m&fn=/documents/guidance/cctv.htm>)

2. Keep information only for one or more specified, explicit and lawful purpose

- Is the information being kept for a clear and stated purpose?
- Are the people about whom information is held clear about that purpose?
- Is the purpose included in the institutional register entry submitted to the Data Protection Commissioner? If you are using personal data for a purpose not listed on your register entry, you may be committing an offence. Your institutional Data Protection Officer will be able to assist you in this.

3. Use and disclose only in ways compatible with purpose

- Are there clear rules for access, processing and disclosure of information? The rules should cover:
 - *Who* is allowed access to the information
 - *Who* can process the information,
 - *How* the information is collected and stored
 - *How* long the information will be kept
 - *How* the information will be kept accurate and up-to-date
 - *To whom* the information will be disclosed and under what circumstances
- Ensure all staff are aware of the rules
- Ensure the rules are documented and readily available

4. Keep it safe and secure

- Record systems must not be set up in such a way that easily allows unauthorized access or disclosure of information.
- Store manual files in locked cabinets or drawers.

- Ensure relevant computer security mechanisms and procedures such as passwords, encryption, locked server rooms etc. are in place and are used.
 - Keep desks clear of papers containing personal data.
 - Keep computer screens clear of personal data, particularly those screens in public areas. Screens should be cleared after each transaction.
 - Lock offices and workstations when leaving them unattended.
 - Develop and review security provisions according to need.
 - Be cautious about putting personal information in e-mails. Where strict confidentiality is necessary e-mails should not normally be used, as they are at present less secure than paper mail.
 - Personal data records should not be transferred to home computers
 - Computers should not be redeployed or discarded without deleting personal data records appropriately. Advice should be sought from relevant computer services departments.
- 5. Keep it accurate, complete and up-to-date**
- Are records checked for accuracy?
 - Are procedures in place to ensure record systems are kept up-to-date?
- 6. Ensure that it is adequate, relevant and not excessive**
- Does the information kept serve our purpose effectively?
 - Is the information relevant and not excessive for our specified purpose?
 - Is the information duplicated elsewhere. It may be preferable to negotiate access to an existing system rather than create a duplicate.
- 7. Retain it for no longer than is necessary**
- Is there a clear statement on how long records will be retained?
 - Are staff clear about legal requirements to retain certain records for a certain period?
 - Are record systems regularly purged of data that is no longer required?
 - Is there a policy on deleting personal records as soon as the purpose for which the data was retained has been completed?
- 8. Give access to personal data to an individual on request**
- Are there clear procedures and guidelines for dealing with access requests from individuals?
 - Is a named individual responsible for handling access requests?
- 9. Respond appropriately to Freedom of Information requests**
- Are there clear procedures and guidelines for dealing with FOI requests from individuals?
 - Is a named individual responsible for handling FOI requests?

4.3. Checklist of issues for a Records Management policy

1. Does the institution have a records management policy?
2. Has the policy been authorized at an appropriate senior level?
3. Does the policy cover all records in all formats
4. Does the policy identify legislation, standards and codes of best practice to which the institution is subject?
5. Does the policy identify the institution's records management requirements?
6. Has the policy been promoted throughout the institution?
7. Is the policy addressed in the institution's operating procedures and manuals?
8. Is the policy known and understood by all staff?
9. Does the policy outline the various roles and responsibilities for staff who manage or perform records management processes throughout the institution?
10. Are records management responsibilities documented in job descriptions?
11. Have staff received the appropriate level of training to help them carry out the records management responsibilities outlined in the policy?
12. Is staff compliance with the policy monitored?
13. Is the policy reviewed at regular intervals?

4.4. Checklist of issues for staff working at service desks

As a general principle, data about library users should **never** be revealed to third parties either deliberately or accidentally. This includes, friends, parents, relatives, classmates, lecturers/tutors, landlords, Gardaí, etc.

1. If anyone asks for information about a library user, or anyone else, do not give it to him or her.
2. Do not even reveal whether the library has information about an individual.
3. Enquiries from the Gardaí should be referred to Security, Registry, HR or other named people in the institution. A procedure should be in place to deal with such enquiries.
4. Requests for information about loans, overdue, renewals, reservations etc. can be answered on production of an ID card, staff card or other identification. These should be checked carefully.
5. Telephone, written or email enquiries about loans etc. require the quotation of a library ID, often the barcode number. In some cases another unique identifier such as a PIN number may be required.
6. Treat all information about library users as private and secure.
7. Do not allow other users to deliberately or inadvertently see another user's personal information on a screen. Screens should be cleared after each transaction.
8. Dispose appropriately of any paper records such as correspondence regarding fines overdue etc. Appropriate disposal may include shredding or the use of confidential waste bins.
9. Where relevant, refer to library or institutional records retention schedules. Files should be purged or weeded regularly and should be deleted/destroyed when no longer required for the stated purpose.
10. Do not discuss library users, in person or on the phone, within the hearing of other library users.
11. Requests for loan history information in cases of plagiarism should be referred to a senior member of staff. Information may be released as appropriate.
12. If information is held about an individual, they have the right to inspect this data. Any request under right of access should be referred to the appropriate named person in the library or institution.
13. When adding a message to a user's borrower account on the library management team the message should be shown to the user and the reason for recording the message explained. (Infringement of library rule, fines message etc.)

4.5. Sample questions and answers

The following examples, which are not exhaustive, may help in dealing with some typical queries that may arise at issue and information desks in the library. Frequently the questions will seem reasonable and the requestor may not understand your refusal. It helps if the procedure and reason for it is explained.

Q.1 *Please can you tell me which books I have on loan?*

You can give this information provided the user shows you his/her current Library card.

If this request is made by someone who has forgotten his or her card, some other identification is required preferably with a photograph.

Q.2 *I am ringing (or emailing) to enquire what books I have on loan?*

This information can be given over the phone or by email once the user can give you their library ID number or barcode.

Q.3 *You may not have my correct address. Can you tell me what address you have?*

Addresses should not be divulged. Remember cards can be stolen. Instead ask for their library ID and then ask the user for their correct address. If the address is different do not disclose it. Refer the user to student records/registry to have their address amended.

Q.4 *Can I renew my books, I don't have my library card.*

As with Q.1, if the user has come to the desk in person you can renew books based on another acceptable form of ID.

Telephone or email requests to renew should not be done without a library ID number or barcode.

Q.5 *My friend has asked me to check what books they have on loan?*

You cannot do this. Borrower details should not be supplied to a third party – friend or relative. The exception to this rule may be where a user has a designated assistant in the case of illness or where there may be mobility issues.

Q.6 *I have requested a book and it is overdue. I think someone in my class might have it – can you tell me who it is?*

You cannot do this. Borrower details should not be supplied to a third party.

Q.7 *I have reserved a book but someone has reserved it before me – can you tell who it is?*

You cannot do this. Borrower details should not be supplied to a third party.

Q.6 A lecturer asks for information about who has a course book on loan

You cannot do this. Requests from lecturers can be hard to refuse but again borrower details should not be supplied to a third party.

Q.7 I am trying to trace an old friend who may be on your files. Could I have their address?

You cannot do this. Personal information should not be supplied to a third party.

Q.8 This is the Gardaí. We need to locate someone urgently and the only identification we have is their library card.

Firstly you need to verify that the call is legitimately from the Gardaí. Ask the caller for details of their name, phone number and Garda Station and refer the query to the appropriate person within the library or institution.

Q.9 I am trying to fill out an application form on your website and it is asking for my library ID number. I don't have it with me as I am at work – can you give it to me?

You cannot do this. The ID/barcode is a unique identifier and cannot be disclosed.

Q.10 I think my daughter/son/friend/partner is in the library – I need to find them urgently – can you tell me if they are there?

You cannot do this. Personal information should not be supplied to a third party. Also you do not know that they are who they say they are.

Q.11 I am preparing a video/photographic assignment. May I film/take photographs in the library?

Photographs and images are considered personal data. Inform the requestor that permission must be sought from the library. They must also ask permission of any person they wish to photograph or film.

Q.12 You are holding a copy of my thesis, can you tell me who has asked to see it?

You cannot do this. Borrower history information should not be disclosed to a third party even if the requestor is the author of the item borrowed.

4.6. Checklist of issues for staff about their own rights

1. Right of access

Under Section 4 of the Data Protection Acts, 1988 and 2003, you have a right to obtain a copy of any information relating to you kept on computer or in a structured manual filing system by your employer.

2. Institution's right to process employee data

As part of the contract of employment it is implied that employees have agreed for the institution to hold and process personal data about them for designated purposes. In turn as an employee you have the right for all data recorded about you to be correct, securely held and not held for longer than the purpose for which it was intended.

3. Right of rectification or erasure

If you find out that information held about you by your employer is inaccurate, you have the right to have it corrected or if the information is irrelevant or excessive for the purpose you have the right to have that information erased.

4. Notification of changes in personal data

Employees have a duty to inform the institution of any changes of name, address etc. to ensure the accuracy of information held.

5. Freedom from automated decision making

As an employee important decisions about you, such as rating your work performance or reliability, may not be made solely by computer automated means. As a general rule, there has to be human input into such decisions.

4.7. Checklist of issues for staff holding files that might include comments or opinions about individuals

Frequently in the course of library business, comments and opinions about individuals are recorded and retained. Examples would include comments about staff performance, comments on problems with individual users etc.

Under Freedom of Information or Data Protection legislation all such records are subject to disclosure upon request. Before deciding to retain and record such comments and in the interests of good practice a useful test is to ask yourself two questions:

1. Is the comment objective, fair, accurate and justifiable?
2. If I were to show this information to the individual concerned would I still be confident that the comment is objective, fair, accurate and justifiable?

4.8. Checklist of best practice for Records Management

Objective

- To ensure the creation and maintenance of authentic, reliable, complete and secure records that serve as evidence and support of past, present and future organisational activity.

Composition

- Compose in a clear, concise, factual and objective style
- Be aware of the responsibility to be accountable
- Record opinions in the context of the facts
- Avoid personal or anecdotal remarks
- Write manual notes and annotations legibly
- Date and sign all notes and documents
- Record attendees of meetings
- Record discussions that contribute to decisions
- Record decisions as soon as they are made
- Only record third-party comments with consent

Maintenance

- Use a communication medium appropriate to the subject matter
- Maintain documents that support decisions
- Destroy notes and drafts that have not contributed to decisions
- File records in a logical sequence
- Classify records in a structure that reflects the function of the office they serve
- Ensure storage and security of records are appropriate to the subject matter

Retention/Disposal

- Keep records for a specific purpose
- Retain records no longer than is required for the specified purpose
- Dispose of records in a manner appropriate to the subject matter

Appendices

- Appendix I Survey of Current Practice in CONUL Libraries in relation to FOI and Data Protection Legislation
- Appendix II Records Retention Schedule
- Appendix III Bibliography
- Appendix IV Freedom of Information and Data Protection Legislation: Guidelines for Library Staff

Appendix I. Survey of Current Practice in CONUL Libraries in relation to FOI & DP Legislations

No	Question	NUIM	RCSI	TCD	DCU	DIT	NUIG	UCC	NLI	UL	UCD
1	Does institution have a written DP policy	Yes	No	In progress	Yes	No	Yes	Yes	No	Yes	Yes
2	DP policy – do library staff know where to find	Yes	n/a	n/a	Some	n/a	No	Some	n/a	Mixed	Yes
3	DP – Is there a library staff member responsible	No	Deputy librarian	No	No	No	No	Librarian	Keeper (Systems)	Head of Administration	Deputy librarian
4	Level of library staff awareness of DP issues	Mixed	Very general	Reasonable awareness	High at issue and information desks	No	In the main yes	Vaguely	Mixed	Yes	Very mixed
5a	DP awareness training available – Institution	Yes	No	No	No	No	No	Yes	No	Not recently	Yes
5b	DP awareness training available – Library	Not yet	No	Informal only	Yes	No	No	No	n/a	Not recently	Informal only
6	Does institution have a written FOI policy	Yes	n/a	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
7	FOI policy – do library staff know where to find	Yes	n/a	Low levels of staff awareness	Yes	Yes	Some	Yes	Yes	Yes	Some
8	FOI – is there a library staff member responsible	No	n/a	Deputy librarian, Keeper of Manuscripts	No	No	Librarian	Librarian	Shared: Keeper (Administration) & Keeper (Systems)	Head of Administration	Deputy Librarian
9	Library staff awareness of FOI query procedures	Low but know where to find procedures	n/a	Low levels of staff awareness	Yes	Yes	No	No	Yes	Yes	Most
10a	FOI awareness training available – institution	Yes	n/a	Yes when legislation enacted. None since	No	No	Yes – not currently	Yes	Yes when legislation enacted and some follow-up for new decision makers.	Yes	Yes

Appendix I. Survey of Current Practice in CONUL Libraries in relation to FOI & DP Legislations

No	Question	NUIM	RCSI	TCD	DCU	DIT	NUIG	UCC	NLI	UL	UCD
10b	FOI awareness training available – Library	Not yet	n/a	No	Yes	No	No	No	N/a	No	No
11	Does institution have a written RM policy	Yes	No	Yes	No	No	No	Yes	No	Draft	Yes
12	Does RM policy identify responsibilities, legislation, codes of practice and retention schedules	In progress	n/a	No – work in progress	n/a	n/a	n/a	Yes	N/a	Yes	Yes
13	RM policy – do library staff know where to find	Yes	n/a	Very low level of staff awareness	n/a	n/a	n/a	Yes	N/a	Mixed	Low level of staff awareness
14	RM – is there a library staff member responsible	No	No	Librarian, Keeper of Manuscripts	No	No	No	Librarian	Keeper (Manuscripts)	No	Deputy Librarian
15	RM – guidelines for library staff	Institution policy used	No	No integrated policy	No	No	No	No	No	No	Nothing official
16a	RM awareness training available – institution	Yes	No	Only to departments involved in pilot project	No	No	No	Yes	No	No	Yes
16b	RM awareness training available – Library	Not yet	No	No	No	No	No	No	N/a	No	No

Appendix II (a): Checklist of library records (all formats)

Example from the University of Wolverhampton Learning Resources

Users	Staff	Administration
Registration forms (staff) Access forms Contact details Disabilities Medical details Passwords Courses Loan transactions Cash transactions Inter-library loan transactions Photocopying requests Service application forms Enquiry forms Equipment bookings Room bookings Overdue notices Recall notices Request available notices Invoices Delinquencies Complaints Suggestions Correspondence	Applications CVs References Training Probation and other reports Complaints Disciplinary Appraisal Performance management development reviews Staff development Correspondence Annual leave Sick leave Extra hours Time in lieu Absence Expenses	Bibliographical information in: Catalogues Other databases Photographs Donations Budget allocations Accounts Orders Invoices Supplier details Contractor details Contracts Licence agreements Maintenance agreements Health & Safety Security Incidents Telephone logs Diaries Minutes of meetings Correspondence

Appendix II (b): Records Retention Schedule example

Record Kept	Location Held	Retention Period	Responsibility for maintenance/deletion of records
Accident reports	Compton LC Dudley LC Health LCs HLC MS Team Telford LC Walsall LC	Permanent Permanent Permanent Permanent Permanent Permanent Permanent	SRA SRA RLs Operations Co-Ordinator MS Co-Ordinator SRA LC Manager
Addresses (LR staff)	MS Team	Permanent	MS Staff
Annual Leave (LR staff)	MS Team	2 years + current year	MS Staff
Application Forms	MS Team	1 year + current year	MS Co-ordinator
Appraisal Records	Compton LC Dudley LC Health LCs HLC LRSS MS Team Telford LC Walsall LC	1 year 1 year 1 year 1 year 2 years Permanent 1 year 1 year	Relevant Appraiser Relevant Appraiser Relevant Appraiser Relevant Appraiser Relevant Appraiser Director of Learning Centres Relevant Appraiser Relevant Appraiser
Athens Forms	Compton LC Dudley LC Health LCs LRSS Walsall LC	1 year 1 year 1 year 1 year 1 year	LC Manager RL/CMRA RLs LRSS Staff AIA
Book Exchange	Telford LC	2 years or until book sold	SRA
CCTV Videos	Compton LC Dudley LC Health LCs HLC Telford LC Walsall LC	1 month 1 month 1 month 1 month 1 month 1 month	SRA SRA RLs Operations Co-Ordinator SRA SRA
CCV Forms	MS Team	10 years	MS Co-Ordinator

Appendix II. Sample record retention schedule

Record Kept	Location Held	Retention Period	Responsibility for maintenance/deletion of records
Complaints	Compton LC Dudley LC Health LCs HLC LRSS MS Team Telford LC Walsall LC	2 years 2 years 2 years 2 years 2 years 6 years 2 years 2 years	LC Manager LC Manager RLs LC Manager HSM MS Co-ordinator LC Manager LC Manager
Computer Booking	Health LCs	1 month	RLs
Declaration of Interest	LRSS	Permanent	Finance Co-ordinator
Enquiries email folder	Health LCs LRSS - Distance Serv Walsall LC	Permanent 1 year 1 year	RLs Distance Serv Unit Leader AIA
Enrolment forms	Compton LC Dudley LC Health LCs HLC Telford LC Walsall LC	1 year Until entered on system 1 year Until entered on system 1 year 1 year	SRA SRA RLs Operations Co-ordinator SRA SRA
Equipment borrowing records	Health LCs Walsall LC	1 year 1 year	RLs CMRA
External Borrowers	Compton LC Dudley LC Health LCs HLC Telford LC Walsall LC	1 year Length of lending rights 1 year 1 year 1 year 1 year	SRA SRA RLs Operations Co-ordinator RL SRA
Extra Hours Forms	Health LCs LRSS MS Team	1 year 1 year 2 years	LC Manager LRSS Unit Leaders MS Staff
Final Overdue letter	Health LCs HLC	1 year 1 year	RLs SRA
Forms and Receipts of all PDQ payments	LRSS Distance Serv	6 years	LRSS Distance Serv Staff

Appendix II. Sample record retention schedule

Record Kept	Location Held	Retention Period	Responsibility for maintenance/deletion of records
Gate Alarm Records	Compton LC Dudley LC Health LCs HLC Telford LC Walsall LC	1 year 1 year 1 year 1 year 1 year 1 year	LC Manager/SRA SRA RLs Operations Co-Ordinator SRA SRA
Group study room bookings form	Walsall LC	1 year	AIA
ILL Records	Compton LC Dudley LC Health LCs HLC Telford LC Walsall LC	5 years 6 years 6 years + 1 day 6 years 5 years 7 years	ILL Assistant ILL Assistant RLs ILL Assistant ILL Assistant ILL Assistant
Incident Reports	Compton LC Dudley LC Health LCs HLC MS Team Telford LC Walsall LC	3 years 3 years 3 years 3 years 3 years 3 years 3 years	SRA SRA RLs Operations Co-Ordinator MS Co-Ordinator SRA LC Manager
Invoice Records (Includes request to invoice)	Compton LC Dudley Health LCs HLC LRSS Telford LC Walsall LC	Until invoice paid Until invoice paid 1 year/Until invoice paid Until invoice paid 6 years Until invoice paid Until conf recd inv paid	SRA SRA RLs SRA Finance Co-Ordinator SRA SRA
Mileage forms/Travel Expenses claims	Health LCs MS Team	1 year 2 years	LC Manager MS Staff
Mobile phone offender records	Health LCs Walsall LC	1 year 1 year	RLs AIA
Monthly Absence Returns (LR staff)	MS Team	5 years	MS staff
Overdues	Dudley LC Telford LC	Until dealt with Until record cleared	SRA SRA

Appendix II. Sample record retention schedule

Record Kept	Location Held	Retention Period	Responsibility for maintenance/deletion of records
Personal Files/Records (LR staff)	Health LCs LRSS MS Team Telford LC Walsall LC	Permanent Permanent Permanent Permanent Permanent	LC Manager HSM MS staff LC Manager LC Manager
Personnel lists (LR staff) /Staffing budget	MS Team	10 years	MS Co-Ordinator
Probation	Compton LC Dudley LC Health LCs HLC LRSS MS Team Telford LC Walsall LC	6 months 6 months 6 months 6 months 6 months Permanent 6 months 6 months	Relevant Supervisor Relevant Supervisor Relevant Supervisor Relevant Supervisor Relevant Supervisor Director of Learning Centres Relevant Supervisor Relevant Supervisor
Reciprocal Borrower Forms	Compton LC Dudley LC Health LCs HLC Telford LC Walsall LC	1 year 1 year 1 year 1 year 1 year 1 year	SRA SRA RLs Operations Co-Ordinator RL AIA
Reference requests	Health LCs LRSS MS Team Telford LC	Permanent 2 years 5 years 1 year	LC Manager & RLs HSM Director of Learning Centres RL
Refund/Reimbursement	LRSS	6 years	Finance Co-ordinator
Risk Assessment forms	Compton LC Dudley LC Health LCs HLC LRSS MS Team Telford LC Walsall LC	Permanent Permanent Permanent Permanent Permanent Permanent Permanent Permanent	LC Manager LC Manager LC Manager LC Manager HSM Director of Learning Centres LC Manager LC Manager

Appendix II. Sample record retention schedule

Record Kept	Location Held	Retention Period	Responsibility for maintenance/deletion of records
Sanction Records	Compton LC Dudley LC Health LCs HLC MS Team Telford LC Walsall LC	1 year 1 year 2 years 1 year 5 years 1 year 1 year	LC Manager SRA RLs LC Manager MS Co-ordinator LC Manager LC Manager
Sick Reports (LR staff)	MS Team	1 year + current year	MS Staff
Staff development	MS Team	Permanent	MS Staff
Student IT helper test records/forms	Dudley LC	2 months	CMRA
Student Request for Credit completed records	LRSS	Permanent	Finance Co-ordinator
Student Request for Invoice completed records	LRSS	Permanent	Finance Co-ordinator
Student/staff data on TALIS	LRSS	Students - Length of course + 6 mths, or until record clear. Staff 5 yrs or date of leaving (whichever soonest), or until record clear	LRSS Staff
Suggestion Forms	Compton LC Dudley LC Health LCs HLC Telford LC Walsall LC	1 year 1 year Permanent 2 years 1 year 2 years	LC Manager LC Manager LC Manager LC Manager LC Manager LC Manager
Suspension memos	HLC	5 years	Operations Co-Ordinator
Time sheets (LR staff)	Compton LC Dudley LC Health LCs HLC LRSS MS Team Telford LC Walsall LC	2 years 2 years 2 years 2 years 2 years 2 years 2 years 2 years	LC Manager LC Manager RLs LC Manager HSM MS Staff LC Manager LC Manager
Timesheets (Student helper)	Dudley LC MS Team	1 year 2 years	CMRA MS Staff
Timesheets (Unitemp)	MS Team	2 years	MS Staff

Appendix II. Sample record retention schedule

Record Kept	Location Held	Retention Period	Responsibility for maintenance/deletion of records
Transaction log of telephone calls	LRSS Distance Serv	6 months	LRSS Distance Serv Staff
Visitors sheets	Compton LC Dudley LC HLC Health LCs Telford LC Walsall LC	1 year 1 year 1 year 1 year 1 year 1 year	SRA SRA Operations Co-Ordinator RLs SRA SRA

Key

AIA - Academic Information Assistant
 ARL - Academic Resources Librarian
 CMRA - Computer Media Resources Adviser
 HLC - Harrison Learning Centre
 HSM - Hybrid Systems Manager
 ILL - Inter Library Loans
 LC - Learning Centre
 LR - Learning Resources
 LRSS - Learning Resources Support Services
 MS - Management Services, ML Block
 RL - Resources Librarian
 SRA - Senior Resources Assistant

University of Wolverhampton Learning Resources (Mary Heaney) in Senior, Karen. Data Protection Issues: checklists for Libraries. SCONUL, p.14-19.

(http://www.sconul.ac.uk/activities/info_systems/papers/dpa_checklist.doc)

Appendix III: Bibliography

Archives Ireland. Records Management <http://www.archives.ie/management.htm> (accessed 26/11/2004)

Comhairle: Citizens Information Database (1999) The Information Commissioner: Protecting your right to know <http://www.cidb.ie/live.nsf/0/8025636c004d1a8d80256778003f3fa2?OpenDocument> (accessed 26/11/2004).

Data Protection (Amendment) Act 2003
<http://www.oireachtas.ie/viewdoc.asp?fn=/documents/bills28/acts/2003/a603.pdf> (accessed 26/11/2004).

Data Protection Act 1988 <http://www.irishstatutebook.ie/ZZA25Y1988.html> (accessed 26/11/2004).

Data Protection Commissioner (2003) Data Protection (Amendment) Act, 2003: A Summary Guide. <http://www.dataprivacy.ie/images/New%20Act%20Summary-website%20version.pdf> (accessed 26/11/2004).

Data Protection Commissioner <http://www.dataprivacy.ie/index.htm>.

Data Protection Commissioner. Self-assessment checklists for data controllers
<http://www.dataprivacy.ie/3k.htm> (accessed 26/11/2004).

Data Protection Commissioner. Data Protection Acts, 1988 and 2003 – A Guide to your Rights
http://www.dataprivacy.ie/images/A%20Guide%20to%20Your%20Rights_web%20version.pdf (accessed 26/11/2004).

Department of Finance. Freedom of Information Act, 1997 - Short Guide
<http://www.finance.gov.ie/viewdoc.asp?fn=/documents/foi/foi2.htm> (accessed 26/11/2004).

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *Official Journal L 281*, 23/11/1995 P. 0031 - 0050

Fifteenth Annual Report of the Data Protection Commissioner, 2003.
http://www.dataprivacy.ie/images/annual_report_2003.pdf (accessed 26/11/2004).

Freedom of Information (Amendment) Act 2003
<http://www.oireachtas.ie/documents/bills28/acts/2003/a903.pdf> (accessed 26/11/2004).

Freedom of Information Act 1997 <http://www.gov.ie/bills28/acts/1997/a1397.pdf> (accessed 26/11/2004).

ISO 15489-1:2001. Information and Documentation – Records Management – Part 1: General. International Standards Organization.

ISO 15489-2:2001. Information and Documentation – Records Management – Part 2: Guidelines. International Standards Organization.

JISC infoNet. Records Management InfoKit. Joint Information Systems Committee.
http://www.jiscinfonet.ac.uk/InfoKits/records-management/index_html (accessed 26/11/2004).

Office of the Information Commissioner <http://www.oic.gov.ie> (accessed 26/11/2004).

Office of the Information Commissioner: Annual Report, 2003.
<http://www.oic.gov.ie/2612/OICAR03e.pdf> (accessed 26/11/2004).

Senior, Karen (2003) Data Protection Issues: checklists for Libraries. Advisory Committee on Access to Information Systems and Services of SCONUL.
http://www.sconul.ac.uk/activities/info_systems/papers/dpa_checklist.doc (accessed 26/11/2004).

Shepherd, Elizabeth & Yeo, Geoffrey (2002) Managing Records: a handbook of principles and practice. London: Facet Publishing. ISBN 1-85604-370-3.

Freedom of Information & Data Protection Legislation

Guidelines for Library Staff

CONUL Sub-Committee on Copyright and Regulatory
Matters

Convenor

Margaret Flood, TCD

Members

Marie Burke, UCD

Miriam Corcoran, DCU

Monica Crump, NUI Galway

Yvonne Desmond, DIT

Maire Domhnat Kirakowska, UCC

Elizabeth Murphy, NUI Maynooth

Paul Murphy, RCSI

Colette O'Flaherty, NLI

Gobnait O'Riordan, UL

Contents

Part A - Legislative Framework

- | | |
|--------------------------------|---|
| 1. The Data Protection Acts | 1 |
| 2. Freedom of Information Acts | 7 |

Part B - Policies and Practice

- | | |
|------------------------------------------------------------------------|----|
| 3. Records Management | 10 |
| 4. Data Protection Legislation – Checklist of Issues for Library Staff | 18 |

- | | |
|------------------------------|-----------|
| Appendix Bibliography | 29 |
|------------------------------|-----------|

Part A – The Legislative Framework

1. The Data Protection Acts 1988 and 2003

1.1. Introduction

Irish data protection legislation establishes certain rights for individuals over data which contains personal information about themselves and the legislation regulates use of such data in many ways. The Data Protection Acts originated as implementations of the 1981 Strasbourg Convention on the processing of data and they are primarily concerned with personal data that is data about living, identifiable individuals. Several EU directives have since been introduced and transposed into national law, namely Directive 95/45/EC, Directive 2002/58/EC (and now repeated Directive 97/66/EC). Certain rights are established for individuals with respect to how their personal data is gathered and handled and how such data may be processed and used by the data holders. The legislation specifies conditions, rules and permitted handling and uses of such data on the part of data holders and it imposes a range of related obligations, including disclosure.

The legislation is now wide ranging insofar as it effectively applies to all personal data held in all media from print to digital. The legislation applies to personal data held by organisations or individuals. There are some limited exclusions, primarily relating to legal, criminal and security considerations.

1.2. The Data Protection Act of 1988

- the 1988 Act established the principle of the protection of privacy of individuals with respect to personal data held in automated form
- defined individual rights of access to, and review of, personal data held by public and corporate bodies
- established a Data Protection Commissioner to enforce the rights established
- instituted a registration procedure for corporate data holders
- introduced provisions regulating data gathering, data holding and data dissemination
- specified the requisite enforcement and legal frameworks.

1.3. The Data Protection (Amendment) Act, 2003

The 2003 Act amended the 1988 Act in a number of significant ways

- extended definitions so as to broaden the scope of the legislation, for example:
- “data” was extended to mean both automated data and manual data
- covers all data from July 2003 and will cover all prior data from 2007
- “processing” was redefined in very broad terms embracing all information collecting, storage, access and use stages

- improved the rights granted to individuals to access data, to object to data holding or use and to block certain uses
- manual data includes data in “relevant filing systems” i.e. any retrieval system structured by reference to individuals
- enlarged the range of responsibilities for data holders in gathering, maintaining, processing and protecting all data containing personal information
- new registration rules broaden the application of the Act considerably by including all but very small or restricted data holders
- new powers and functions are granted to the Data Protection Commissioner and codes of practice may have statutory effect.

The two Acts are cited and construed as one, The Data Protection Acts 1988 and 2003.

1.4. Definitions

Certain terms have particular meaning in the legislation and these definitions establish the essential concepts. The following are some important definitions embedded in the Acts (1988 S. 1 (1)) :

Data means information in a form, which can be processed. Since 2003 it includes both automated data and manual data. However, the application of certain parts of the Act to existing manual data is deferred until October 2007.

Automated data means, broadly speaking, any information on computer, or information recorded with the intention of putting it on computer.

Manual data means information that is kept as part of a relevant filing system, or with the intention that it should form part of a relevant filing system (see “*Relevant Filing System*”)

Relevant filing system means any set of information that, while not computerised, is structured by reference to individuals, or by reference to criteria relating to individuals, so that specific information relating to a particular individual is readily accessible.

Personal data means data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller (see “*Data Controller*”).

Processing means performing any operation or set of operations on data, including:

- obtaining, recording or keeping the data
- collecting, organising, storing, altering or adapting the data
- retrieving, consulting or using the data
- disclosing the data by transmitting, disseminating or otherwise
- making it available
- aligning, combining, blocking, erasing or destroying the data.

Data Subject is an individual who is the subject of personal data (*any library user, any library employee*).

Data Controller is a person who, either alone or with others, controls the contents and use of personal data – any library staff member who can collect, store, process, edit or delete any personal data about any living person is a data controller. See the Data Commissioners' document - *A Guide For Data Controllers*.

Data Processor is a person who processes personal information on behalf of a data controller.

Sensitive personal data relates to specific categories of data which are defined as data relating to a person's racial origin; political opinions or religious or other beliefs; physical or mental health; sexual life; criminal convictions or the alleged commission of an offence; trade union membership.

1.5. Main data protection rules & conditions

(1988 & 2003, Section 2(1)–(7) & S.2 A-C)

Under these sections, data controllers are obliged to:

1.5.1. Obtain and process information fairly

- the data subject must be made aware of the purpose in collecting the data, the identity of the data controller and the persons to whom the data may be disclosed and any other information that it is reasonable to think may be fair
- the data subject either must have given consent to the processing of the data or the processing must be necessary for a number of specified legal or contractual reasons. In the case of sensitive personal data such consent must be given explicitly

1.5.2. Keep it only for one or more specified, explicit and lawful purposes

- data subjects should know why data is collected
- the data controller must be explicitly aware of the various sets of data and the specific purpose of each.

1.5.3. Use and disclose it only in ways compatible with these purposes

- subject to specific limited exceptions, disclosure of data must be consistent with the purposes for which it was collected.

1.5.4. Keep it safe and secure

- appropriate security measures must be taken against unauthorised access to, or alteration, or disclosure or destruction of the data
- the levels of appropriate security are proportionate to the harm that might result from an unauthorised disclosure.

1.5.5. Keep it accurate, complete and up-to-date

- compliance requires that all procedures ensure the highest possible levels of accuracy
- subject to periodic review and audit

1.5.6. Ensure that it is adequate, relevant and not excessive

- requires that only the minimum amount of personal data is held
- requires that the data controller establish what the specific criteria to meet this requirement are.

1.5.7. Retain it for no longer than is necessary for the purpose or purposes

- requires a defined policy on retention for all items of personal data kept
- procedures in place to implement such policies.

The above three rules apply to all personal computer-held data and to all personal manual data created from the 1 July 2003. However, for manual records created before 1 July, 2003, the obligations are

- to keep data accurate, complete and up-to-date
- to ensure that they are adequate, relevant and not excessive
- to retain them no longer than is necessary for the purpose or purposes will only apply from 24 October, 2007

Until that date the following procedures will apply to personal manual data created before 1 July, 2003:

- provide a copy of his/her personal data to any individual on request (see below)
- correct, erase or destroy any manual personal data that are incomplete or inaccurate
- destroy any personal manual data that are incompatible with legitimate purposes for which it was collected.

1.6. “Fair Processing” provisions (S.2D) entitle a data subject to:

- a copy of the personal data held by the data controller
- know the source and purpose of the data
- the identity of those to whom you disclose the data
- the data subject must comply with specific conditions in making such requests
- the data subject has the right to have inaccurate data erased or rectified
- the data controller is required to reply to requests within specified time periods
- prescribed fees may be charged to the data subject
- the data subject has the right to complain to the Data Protection Commissioner.

1.7. Subject’s right to establish existence of personal data (S.3)

Upon enquiry, data controllers are obliged to fully inform the subject of all relevant data held within 21 days.

1.8. Subject's right of access (S.4)

These provisions include that - on foot of an application by a data subject - the data controller must inform the data subject whether his or her personal data is processed by or on behalf of the data controller and, if so

- provide a copy of personal data
- describe in writing the categories of data and the purpose of the processing
- state the source of the data
- state the persons to whom the data would be disclosed
- inform the data subject of the logic involved in any automated decision
- the data subject must comply with specific conditions in making such requests
- the data controller is required to reply to requests within 40 days
- prescribed fees may be charged to the data subject
- the data subject has the right to complain to the Data Protection Commissioner.
- See the Data Commissioners' document - *A Guide to Your Rights*.

However a data controller is not required to give access to personal data relating to other individuals unless they have consented.

1.9. Restrictions on right of access (S.5)

- restricted rights of access apply in specified tax, criminal, regulatory, legal and certain other situations.
- restricted rights of access also apply where undisclosed personal data is specifically gathered for statistical purposes and these restrictions also apply to backup data.

1.10. Rights to rectification or erasure data (S.6)

- where there has been a breach of the data protection rules a data controller must correct or erase personal data on receipt of a written request from a data subject and must comply within 40 days.

1.11. Duty of care by data controllers (S.7)

- specifies duty of care with respect to accuracy and other conditions.

1.12. Disclosure of personal data in certain cases (S.8)

- The restrictions on the processing of personal data do not apply in specified criminal, legal and security contexts (such as if disclosure were required urgently to prevent injury or damage to someone's health) under Section 8 of the Act

1.13. Data Protection Commissioner

The Office of the Data Protection Commissioner is established under the 1988 Act to perform the designated functions of enforcement (S.10). The Commissioner may investigate any of the provisions of the Acts either directly or on foot of complaints. The Commissioner is empowered to require data controllers to furnish any required information within a specified time. If contraventions

are found, the Commissioner may serve an enforcement notice to the data controller(s) to ensure required compliance. Non-compliance with enforcement notices constitutes an offence in law. There is provision for an appeals procedure.

The Commissioner is obliged to encourage trade and representative associations, and related bodies, to prepare appropriate codes of practice which, if approved as being in conformance with the legislation, may in turn be deemed to be statutory instruments.

Under Section 11, the Commissioner may prohibit the transfer of personal data outside the European Economic Area.

1.14. Registration

Sections 16–20 of the 1988 Act required all designated data controllers to register with the Commissioner. Registration is at the institutional level: on the current register, there is one entry for each of the universities and colleges. These Sections were reviewed in the 2003 legislation and the scope broadened to include virtually all but the smallest data holders. Registration and renewal fees are payable. It is an offence not to be registered.

1.15. Implications for libraries

Universities and their libraries, holding significant volumes of personal data, are required to implement the applicable conditions of the legislation through appropriate policies, procedures and systems. Co-ordination of Data Protection policies must be centrally organised within institutions. Data Protection legislation has an immediate and continuing impact upon libraries as library staff continually process data about students and staff of their institutions. The duty of compliance resides at all levels within libraries and with each library staff member with access to any personal

data. For instance, the legislation prohibits the revelation of either registration or loan information to any third party; all personnel related records within libraries are also included. Libraries are obliged to respond promptly and appropriately to requests for disclosure and are subject to investigation by the Data Protection Commissioner. Appropriate systems and training must be in place in all functional areas to ensure compliance.

Bibliography

Guidance documents on the Acts available from the website of the Data Protection Commissioner <http://www.dataprivacy.ie/index.htm> [accessed 2.7.04] :

- Texts of the Acts, European Union Directives and Statutory Instruments
- Composite text in one of both the 1988 and 2003 Acts
 - <http://www.dataprivacy.ie/images/CompendiumAct.pdf>
- Data Protection (Amendment) Act, 2003 - A Summary Guide
- Data Protection Acts, 1988 and 2003 - A Guide for Data Controllers
- Data Protection Acts, 1988 and 2003 - A Guide to Your Rights
- Self-assessment checklists for data controllers

The Acts and Statutory instruments are also available on the Irish Statute Book site <http://www.irishstatutebook.ie/>

2. Freedom of Information Act 1997 and Freedom of Information (Amendment) 2003

2.1. Introduction

The Freedom of Information Act 1997 came into being to provide a statutory right for members of the public to access official information held by public bodies. The Act was first implemented in Government Departments in 1998 and applied to third level educational institutions from October 2001. These Acts in conjunction with the Data Protection Acts 1988 & 2003 ensure that the rights of individuals are protected, that records are accurate and that access to information is made as simple as possible.

2.2. Freedom of Information Act 1997

Essentially the Act establishes 3 statutory rights

- right to access information held by public bodies
- right to have personal information in a record amended where it is incomplete, incorrect or misleading
- right to obtain reasons for decisions affecting the person.

The Act also established the independent Office of the Information Commissioner to enforce the legislation including the role of reviewing decisions made by public bodies under the legislation.

2.2.1. Section 15 and Section 16

The most immediate impact of the Act was the legal obligation imposed on public bodies to provide S15 and S16 manuals. These must clearly describe the way the body is organised, its functions, the services it provides to the public and how these can be accessed. The kinds of decisions they makes and how they are arrived at, the types of records held and a procedure for accessing them and the internal rules, procedures, guidelines used in the decision making process. It must also describe how decisions made by the body can be reviewed and what avenue of appeal exists.

The purpose of these manuals is to help the public to decide what kind of information the body holds and how they can access it. S15(3) clearly states that bodies must have regards to the needs of the public when compiling the manuals so for example heavy use of jargon would be seen as contrary to the provision of these sections. These manuals are required to be published, but the 2003 Amendment Act introduced a minimum publication requirement via electronic means. Initially many were produced in hard copy but increasingly they can be found on the Web. A revised version should be prepared every 3 years and as soon as possible after any significant change.

2.3. Records and right of access.

2.3.1 What is a record? (S.2)

As defined by the 1997 & 2003 Acts a record" includes any memorandum, book, plan, map, drawing, diagram, pictorial or graphic work or other document, any photograph, film or recording (whether of sound or images or both), any form in which data (within the meaning of the [Data Protection Act, 1988](#)) are held, any other form (including machine-readable

form) or thing in which information is held or stored manually, mechanically or electronically and anything that is a part or a copy, in any form, of any of the foregoing or is a combination of two or more of the foregoing and a copy, in any form, of a record shall be deemed, for the purposes of this Act, to have been created at the same time as the record;”.

2.3.2. What records can be requested?

1. Records created after the commencement of the Act in April 1998 (i.e. 21 April 1998)
2. All personal records and records containing personal information irrespective of when created
3. Any other record deemed necessary to the understanding of a current record
4. Personnel records of staff in public bodies created after 1995. Earlier records may be accessed if they are being used in a way that may adversely affect the interests of the staff member involved.

Given the wide-ranging definition of what constitutes a record it is wisest to assume that all records held by an Institution fall under the Act unless they are subject to the stated exemptions. Examples of such exemptions are information obtained in confidence (S26), commercially sensitive information (S27), information that would prejudice the functions or performance of a public body or adversely affect its negotiation process (S21), records concerned with the deliberations of public bodies (S20). Records containing the personal information of other people (S28) and Section 30 protect research and development before it comes into the public domain.

When an institution refuses to release information it must make a cogent argument that to do so will cause it harm or injury and public interest tests contained in several of the exemptions, must be satisfied.

2.4. The Process

The Act clearly lays out how a request is to be made in Section 7 and emphasises the duty of the public body to assist the person (a requester) making the request. S3.4 states the motive of a requester cannot be taken into account but the Information Commissioner has decreed that S8 (4) allowed for the motive of a requestor to be taken into account if a request is “frivolous or vexatious”.

Public bodies have appointed FOI Officers and designated decision makers for the relevant areas of their organisations.

The Act details the time limits to be applied to a request. An internal review must take place within 4 weeks with a decision within 3 weeks of that review. An external review to the Information Commissioner must be sought within 6 months. His/her decisions are binding but can be appealed to the High Court on a point of law.

2.5. Freedom of Information (Amendment) Act, 2003

The basic purpose of this Amendment was to increase the level of protection afforded to key areas of government activity and parliamentary as well as to make a series of small amendments to improve the workings of the Act. The scope of some exemptions was increased. Following the Amendment Act an upfront fee of €15 was imposed for requests for non-personal information, €75 for internal review and €150 for review by the Information Commissioner.

S 17 and S 18 were amended to give the right to parents, guardians and next of kin to amend records of their children or relatives and to be given the reasons for decisions affecting such children or relatives.

While the imposition of a charge has led to a decrease in the number of FOI requests, they would now appear to be of a more serious nature.

2.6. Implications for Libraries

The Freedom of Information Acts 1997 and 2003 have implications for how libraries conduct their activities. To allow libraries to respond in the necessary timescales set down in the Act there is a need for each library to have a records management system, which permits easy and efficient retrieval of information. There should be a policy on records keeping stipulating what records shall be kept and for how long and ideally, one member of library staff should be given responsibility for this area. The reasons for any decisions should be clearly documented with reference to the appropriate policies that might apply to the decision making process. Care should be taken to ensure that any information kept is accurate, factual and relevant to the matter in hand. Records should be simply written, free from jargon, personal comment or speculation and should be signed and dated where possible. All draft copies should be removed and only the final record kept.

As information brokers it is the responsibility of each member of library staff to be aware of the rights and obligations conferred on the public by these Acts and to be sufficiently aware and trained to assist any member of the public with an FOI request.

Bibliography

Short Guide to Freedom of Information Act 1997 : Dept of Finance

<http://www.foi.gov.ie>

Office of the Information Commissioner (both text and guides)

<http://www.oic.gov.ie/>

Comhairle Justice: Citizens Information.

Freedom of information: your rights

<http://www.cidb.ie/live.nsf/0/8025636c004d1a8d80256778003f3fa2?OpenDocument>

Part B – Policies and Practice

3. Records Management

3.1. Introduction

Records management is the formal application of systematic controls to the creation, use, maintenance and/or disposal of records. The international standard for records management developed by the [International Organisation for Standardisation \(ISO\)](#) defines records as "information created, received, and maintained as evidence and information by an organization or person, in pursuance of legal obligations or in the transaction of business" (ISO 15489, clause 3.15, 2001). It also states that the role of records management is to support the continuing conduct of business, to comply with the regulatory environment, and to provide the necessary accountability, organizations should create and maintain authentic, reliable and useable records, and protect the integrity of those records for as long as required.

Apart from the benefits of increased organisational efficiency, records management, as a formal process, has been driven by legislation that seeks to increase public accountability, most notably the Freedom of Information Acts 1997 and 2003 and the Data Protection Acts 1988 and 2003 (FOI & DP Acts) discussed in Part A above. In her 2003 annual report, the Information Commissioner states that "Good records management practice is critical from an FOI perspective..." and also alludes to the provisions of the DP Acts (http://www.oic.gov.ie/report03/221e_20a.htm)

Although these Acts do not legally require a records management policy, the FOI Acts legislate for access to information and the DP Acts state very specifically how information is to be created, maintained, stored and retained/disposed.

3.2. Developing a Records Management Policy

A records management policy identifies how records are used within an organisation. It acknowledges and identifies, at a general level, the records that need to be created and maintained to support core business functions, to satisfy legal requirements and to meet stakeholder expectations. It also identifies requirements such as form, content, retention, disposal and access. These requirements need to be identified with regard to the organisation's exposure to risk if records are not effectively created or managed.

The objectives and intended outcomes of a records management policy need to be identified during the initial stages of policy development. The target audience, that is, all staff within the organisation, needs to be identified and involved in this process to address any existing issues they may have and to foster their support and adoption of the final product.

The role of records within an organisation will be affected by the organisation's regulatory environment. A records management policy needs to identify any legislation that affects the records administered by the organisation, such as the FOI and DP Acts. The regulatory environment also includes voluntary standards or codes of practice with which the organisation has chosen to comply.

The existing records management environment of the organisation also needs to be understood in order to develop a relevant and practicable policy. This includes identifying strengths and weaknesses, and how records management is currently supported and controlled within the organisation. This will involve evaluating existing policies, practices and procedures to decide whether they will be integrated within the new policy, or replaced.

As a framework, a records management policy needs to be simple and concise. The policy does not need to include any detailed advice on operational procedures or tools (such as classification schemes or disposal schedules). However, such products will need to be developed to support the policy. The policy document needs to be easy to understand, and present its directives and responsibilities in a clear and simple manner. It must contain accurate, relevant and up-to-date information.

A records management policy framework may be delivered through a variety of disparate documents. However, the creation of a single comprehensive organisational policy statement is a more effective way of controlling and communicating a strong records management culture.

3.3. Core Components of a Records Management Policy

3.3.1. Purpose

This statement defines the aims of a records management policy. For example:

The purpose of this policy is to establish a framework for the creation and management of records within this organisation. This organisation is committed to establishing and maintaining records management practices that meet its business needs, accountability requirements and stakeholder expectations.

3.3.2. Policy statement

This statement outlines the organisation's commitment to records management. It needs to define the records management policy as the framework for the organisation's records and their management processes. It could also provide a brief background on records, records management and the regulatory environment of the organisation. Any other important influences or interests specific to the management of records within the organisation could also be outlined here. For example:

This organisation's records are its corporate memory, and as such are a vital asset for ongoing operations, providing valuable evidence of business activities and transactions.

This organisation is committed to implementing best records management practices and systems to ensure the creation, maintenance and protection of accurate and reliable records. All practices concerning records management within this organisation are to be in accordance with this policy and its supporting procedures.

3.3.3. Scope

This statement identifies and defines who and what the policy applies to. For example:

This policy applies to all staff within this organisation.

This policy applies to all aspects of organisational business, all records created during business transactions, and all business applications used to create records regardless of format.

This policy applies to all areas and locations of work within this organisation.

This policy provides the overall framework for any future records management policies, practices or procedures.

3.3.4. Legislation and standards

This statement identifies the regulatory environment, as it affects records management within the organisation. It also acknowledges any voluntary standards, codes of practice or guidelines that the organisation has chosen to adopt. For example:

This organisation will develop records management systems that capture and maintain records with appropriate evidential characteristics in accordance with its obligations under the following pieces of legislation:

- Data Protection Acts, 1988 & 2003
- Employment Equality Act, 1998
- Freedom of Information Acts, 1997 & 2003
- Organisation of Working Time Act, 1997
- Safety, Health and Welfare at Work Act, 1989
- Safety, Health and Welfare at Work (General Applications) Regulations, 1993
- Unfair Dismissal Acts, 1977 & 1993.

This list is not exhaustive. An increasing body of legislation presenting retention periods for records means that the above list will be extended.

This organisation is committed to best practice in records management, and will develop records management systems consistent with the ISO 15489, the international standard for records management.

3.3.5. Records management systems

This statement identifies the records management systems of the organisation and mandates their exclusive use to promote compliance amongst staff. However, this information needs to remain general, so that the policy will remain relevant even if specific records management systems are superseded during its projected life. This statement could also outline the key records management processes undertaken by the identified systems. Existing operational policies or procedural guidelines that control any of these processes can be linked here to the policy framework. For example:

This organisation's primary records management system is an electronic records management system. All paper-based records received in the organisation from [*specify date*] are captured within this system through digital imaging.

This organisation's records management systems are dedicated to the creation and maintenance of authentic, reliable and usable records for as long as they are required to effectively and efficiently support business functions and activities.

The records management systems will manage the following processes:

- creation or receipt of records
- accuracy, relevance, integrity and authenticity of records
- security of records
- access to records
- retention/disposal of records

3.3.6. Responsibilities

This statement outlines the various records management responsibilities within the organisation, assigning them to an individual, level and/or area within the organisation. Despite specific accountabilities, it also identifies that all staff are accountable for records management. For example:

The President/Director is responsible for the authorisation of the records management policy. The President must oversee the management of this policy within this organisation.

Senior administrators/officers are responsible for the management of this policy through resource allocation, and other management support.

The Records Manager is responsible for overseeing the design, implementation, and maintenance of this records management policy, as well as monitoring compliance.

The system administrators are responsible for maintaining the technology for this organisation's records management systems.

Departmental/office managers are responsible for supporting and monitoring staff records management practices as defined by this policy.

All staff are responsible for complying with the records management processes and procedures as defined by this policy.

3.3.7. Monitor and review

This statement sets a date for review. It may also be used to set up monitoring and review procedures, such as an audit committee. For example:

This policy is scheduled for review in [*specify date*]. This review will be conducted by an internal audit committee established by senior management.

3.3.8. Authorisation

This statement authorises the policy with an appropriate signature and date. For example:

This policy has been approved by:
[*Name of President/Director*], [*Date*]
[*Signature*]

3.3.9. Definitions

This statement is a list of definitions to clarify certain terms used within the policy. For example:

Records mean any information, in any format, created, received, and/or maintained by officers or employees in the course of their duties on behalf of the organisation.

Active Records mean records that are required and referred to constantly for current use, and that need to be retained and maintained in office space and equipment close to users.

Semi-active Records mean records that are referred to infrequently and are not required constantly for current use. These are removed from office space to lower cost off-site storage until they are no longer needed.

Inactive Records mean records for which the active and semi-active retention periods have lapsed and which are no longer required to carry out the functions for which they were created.

Archives are defined as records that include those with legal, operational, administrative, historical, scientific, cultural and social significance.

Records Management means the formal application of systematic controls to the creation, use, maintenance and/or disposal of records.

Records Retention Schedules means control documents that specify the periods of time, varying from a few months to permanency during which a record has to be maintained. This is determined by statute, legal, regulatory or business compliance, or where these do not apply, by a best assessment of risks involved in destruction against the costs of retention.

3.4. Implementing a Records Management Policy

A records management policy needs to be implemented as a distinct control mechanism in the organisation even if it has been developed alongside other records management products, such as detailed procedure manuals. This will help to ensure that staff clearly recognise the corporate mandate for records management in the organisation. Steps towards successful implementation include:

3.4.1. Promotion

A records management policy needs to be widely promoted to clearly inform staff of its contents and implications, and most importantly, to make staff aware of their responsibilities as defined within the policy. However, it is also vital to promote staff compliance with the policy. The responsibilities of all staff members can be made conditions of employment in job descriptions and performance management procedures. It may also be useful to highlight how poor records management may affect individual staff and the organisation through legal action or media exposure.

The support of senior management is vital when promoting policy. This needs to be made visible through clear authorisation of policy, allocation of appropriate resources, and subsequent monitoring of organisational compliance. This support could also be documented in the employment contracts of senior management, to mandate and create incentives for the effective management of good record management practices within the organisation.

3.4.2. Training

Staff who can effectively implement the directives of policy are critical to its success. Staff training is essential for this purpose, ensuring that staff do not merely understand their records management responsibilities but are able to carry them out.

3.4.3. Supplementary guidelines and procedures

To accompany the policy framework, supplementary guidelines and procedures will need to be developed within the organisation. See Appendix II (b) for an example of a Records Retention Schedule in place in a university learning resource centre.

3.4.4. Monitoring and review

The success of a records management policy depends on effective monitoring and review mechanisms, to ensure its proper and continued use and relevance. Ideally this would be undertaken at a set time after policy implementation, and continued on an ongoing basis. It would involve:

- evaluating the policy document for comprehensibility and relevance
- measuring policy impact and results against initial objectives
- looking for unforeseen effects
- surveying organisational awareness of policy and contents
- monitoring staff adoption and application of policy.

3.5. The Implications of poor Records Management

The interrelationship between records management practice and public accountability is best demonstrated by some case histories. For example, in 2003, the Data Commissioner found that a company had breached the security requirements of the DP Acts as adequate safeguards regarding access to the data, which resulted in an individual's personal data being disclosed to a third party without consent, were not in place (Data Commissioner Annual Report 2003, p. 35). In another case involving the publication of personal data relating to individuals making FOI requests in a personal capacity (as opposed to a professional or business capacity), the Data Commissioner advises that such practice "constitutes a disclosure under the Data Protection Acts 1988 and 2003" (Data Commissioner Annual Report 2003, p.45).

In her reviews in 2003, the Information Commissioner "came across two particular situations which demonstrated the importance of a proper records management policy in relation to the destruction of records." (See Annual Report of the Information Commissioner 2003 http://www.oic.gov/report03/221e_20a.htm). The same report documents a separate issue relating to records management which arose in a review involving the Athlone Institute of Technology where the Commissioner found that the retention period for the relevant records had not been appropriate to meet the legislative requirements.

As demonstrated by these-cited cases, poor records management can contribute to non-compliance. Non-compliance can incur heavy penalties, up to €100,000 in the case of the DP Acts. In addition, poor records management can also result in a lack of confidence in the organisation, not to mention the bad press that publicised legal cases can generate.

3.6. Implications for libraries

3.6.1. Institutional policy

Many of the CONUL libraries' parent institutions have already introduced records management policies as detailed in Appendix I - Survey. Any records management practices in the library

would need to be informed by institutional guidelines or best practice (see Appendices I-IV for some guidance) where none exists.

3.6.2. Obtaining personal data indirectly

Under DP legislation, an organisation is obliged to inform individuals (data subject) from whom it is obtaining data, why it is required and if it will be disclosed to any third parties. In disclosing data to third parties, the data subject must be given the identity of the third party, the reason the data is required and any other information relevant to the specific circumstances. This is usually done at the time the data is collected and in third level institutions where students are concerned this would be at registration. This means that the data subject would need to be informed if his/her personal data is disclosed to the library and to what purpose it is required, etc. However, this would not include users who register directly with the library.

3.6.3. Third party disclosure

Under DP legislation, records must be kept secure and not made available to third parties without consent. Front-line staff are particularly vulnerable to breaching this law if they are not fully aware of the legislation. For example, a staff member at a Circulation Desk may be innocently asked by a user to disclose the name of the borrower of an item required by that user.

3.6.4. Currency of records

Under FOI and DP legislation individuals have a right to amend their own personal record and in addition, under DP legislation, records must be kept up-to-date. Most CONUL libraries obtain their student records from the central registration office so any update to common information made directly to the library would not be made to the central registration record. In addition, there may be a delay in supplying amendments from the central registration office to the library. Under DP legislation, if the organisation fails to maintain accurate, complete and up-to-date data, it may be liable to an individual for damages under the duty of care provision applying to the handling of personal data.

3.6.5. Defaulters

Under FOI and DP legislation, individuals have the right to access their records and in addition, under DP legislation, records may only be retained for as long as is necessary to fulfil a specified purpose. Information regarding users will be provided to other sections of the institution as appropriate. As such, the library is responsible for the recording and maintenance of this information. Ideally, library regulations would include the full procedures for dealing with such issues, including the procedure for recording details.

3.6.6. Manual records

Certain parts of the Data Protection (Amendment) Act, 2003 will only apply to manual data (i.e. files which are part of a relevant filing system created prior to enactment i.e. July 2003) and from the 24 October 2007, such data will need to:

- be accurate, complete and up-to-date
- be adequate, relevant and not excessive
- be retained for no longer than is necessary for the specified purpose
- in the case of personal and sensitive personal data, comply with at least one of a number of extra conditions

Although a lot of personal data held in libraries is now computerised, data such as staff records and inter-library loan forms will still be held manually. There may also be other files holding personal data that have not been updated since July 2003 such as correspondence, manual files pre-dating computerisation, etc.

Bibliography

This statement is a list of resources for further information. It may include contact details of relevant staff within the organisation as well as reference material. For example:

- Archives Ireland - <http://www.archives.ie/rmanagement.htm>
- ISO 15489-1:2001 Information and documentation – records management – part 1: general. International Standards Organization.
- ISO/TR 15489-2:2001 Information and documentation – records management – part 1: guidelines. International Standards Organization.
- JISC infoNet - http://www.jiscinfonet.ac.uk/InfoKits/records-management/index_html
- Records Manager
- Shepherd, Elizabeth & Geoffrey Yeo. Managing Records: a handbook of principles and practice. London: Facet Publishing, 2003.

4. Data Protection and Freedom of Information Legislation Checklists of Issues for Library Staff

4.1. Introduction

Part A of this document clearly outlines the legislative framework and associated implications arising from the Data Protection Acts 1988 and 2003 and from the Freedom of Information Acts 1997 and 2003.

Because all library staff are collecting, holding or processing personal data as a legitimate part of their daily employment, they are affected directly by the Data Protection legislation. Every member of library staff is responsible for ensuring that personal data is held and processed in accordance with the legislation and can be held personally liable. Equally, under Freedom of Information legislation, there is an obligation for libraries to have records management systems that are easily accessible and provide for the efficient and timely retrieval of information.

The checklists contained in this section are intended to give some practical guidelines and examples to encourage the development and maintenance of good systems and practices in our libraries. They are not intended to be exhaustive and should be read in conjunction with institutional and library guidelines and policies. Advice should also be sought from institutional Data Protection and Freedom of Information Officers and in matters of specific legal interpretation advice should be sought from the office of the Data Protection Commissioner at **www.dataprivacy.ie**

The checklists are based on the SCONUL produced document "Data Protection Issues: Checklists for Libraries" and on good practice examples received from a number of academic libraries and their institutional Data Protection and Freedom of Information offices. (See Data Protection Issues: checklists for Libraries/prepared by Karen Senior for the Advisory Committee on Access to Information Systems and Services of SCONUL (Society of College, National and University Libraries)),

4.2. Checklist of issues for setting up a Records Management system

Libraries necessarily need to collect and retain information for a variety of purposes in the course of their business. Records are legitimately kept about both staff and library users.

Typical examples of records in each category include:

User Records	Staff Records	Administrative Records
<ul style="list-style-type: none"> ▪ Borrower records with associated personal data (addresses, phone numbers) ▪ Recalls ▪ Reservations ▪ Overdue and fines records ▪ Cash transactions ▪ Inter library loan records ▪ Photocopying requests ▪ Enquiry forms ▪ Room bookings ▪ Copyright data on requesters of theses ▪ External borrower records (reciprocal, corporate, graduate member, long term visitors, ALCID etc) ▪ Registration forms ▪ Access forms ▪ Disability records ▪ Passwords ▪ Incident/Accident reports and medical details ▪ Queries ▪ Suggestions ▪ Complaints ▪ Rule infringement records ▪ Correspondence ▪ Photographs of users 	<ul style="list-style-type: none"> ▪ Personnel files with addresses, phone numbers and other personal data. ▪ Salary details ▪ Expenses ▪ Applications ▪ CVs ▪ References ▪ Results of recruitment processes ▪ Probation records ▪ Annual leave and absence records ▪ Staff development and training records ▪ Time in lieu and overtime records ▪ Results of performance management processes ▪ Grievance/disciplinary information ▪ Correspondence ▪ Information about staff held on library/university websites including photographs 	<ul style="list-style-type: none"> ▪ Donations ▪ Budget allocations ▪ Accounts ▪ Supplier details ▪ Contractor details ▪ Order records ▪ Invoices ▪ Contracts ▪ Licences ▪ Results of tendering exercises ▪ Health and Safety records ▪ Security incidents ▪ Telephone log ▪ Diaries ▪ Minutes of meetings ▪ Correspondence

There are **8 guiding principles** or rules underpinning Irish Data Protection legislation and all must be considered when setting up any records system; manual or computerized and for any of the above data types.

1. Obtain and process information fairly

- At the time when the information is collected about individuals, are they made aware of all the uses for that information?
- Are individuals made aware of any disclosures of their data to third parties? This might include fines data to Registry or borrower data to alumni associations.
- Has consent been obtained from individuals for any secondary uses of their personal data?
- Are our records management systems and practices open and transparent?
- Has responsibility for the maintenance of all record types been clearly assigned?
- Has permission been obtained to keep, copy or use photographs of individuals?
- If your library uses CCTV surveillance, it is essential to have notices in place alerting users to the presence of the cameras Guidelines on the use of CCTV cameras is available from the Commissioner's website at (<http://www.dataprotection.ie/viewdoc.asp?m=m&fn=/documents/guidance/cctv.htm>)

2. Keep information only for one or more specified, explicit and lawful purpose

- Is the information being kept for a clear and stated purpose?
- Are the people about whom information is held clear about that purpose?
- Is the purpose included in the institutional register entry submitted to the Data Protection Commissioner? If you are using personal data for a purpose not listed on your register entry, you may be committing an offence. Your institutional Data Protection Officer will be able to assist you in this.

3. Use and disclose only in ways compatible with purpose

- Are there clear rules for access, processing and disclosure of information? The rules should cover:
 - *Who* is allowed access to the information
 - *Who* can process the information,
 - *How* the information is collected and stored
 - *How* long the information will be kept
 - *How* the information will be kept accurate and up-to-date
 - *To whom* the information will be disclosed and under what circumstances
- Ensure all staff are aware of the rules
- Ensure the rules are documented and readily available

4. Keep it safe and secure

- Record systems must not be set up in such a way that easily allows unauthorized access or disclosure of information.
- Store manual files in locked cabinets or drawers.

- Ensure relevant computer security mechanisms and procedures such as passwords, encryption, locked server rooms etc. are in place and are used.
 - Keep desks clear of papers containing personal data.
 - Keep computer screens clear of personal data, particularly those screens in public areas. Screens should be cleared after each transaction.
 - Lock offices and workstations when leaving them unattended.
 - Develop and review security provisions according to need.
 - Be cautious about putting personal information in e-mails. Where strict confidentiality is necessary e-mails should not normally be used, as they are at present less secure than paper mail.
 - Personal data records should not be transferred to home computers
 - Computers should not be redeployed or discarded without deleting personal data records appropriately. Advice should be sought from relevant computer services departments.
- 5. Keep it accurate, complete and up-to-date**
- Are records checked for accuracy?
 - Are procedures in place to ensure record systems are kept up-to-date?
- 6. Ensure that it is adequate, relevant and not excessive**
- Does the information kept serve our purpose effectively?
 - Is the information relevant and not excessive for our specified purpose?
 - Is the information duplicated elsewhere. It may be preferable to negotiate access to an existing system rather than create a duplicate.
- 7. Retain it for no longer than is necessary**
- Is there a clear statement on how long records will be retained?
 - Are staff clear about legal requirements to retain certain records for a certain period?
 - Are record systems regularly purged of data that is no longer required?
 - Is there a policy on deleting personal records as soon as the purpose for which the data was retained has been completed?
- 8. Give access to personal data to an individual on request**
- Are there clear procedures and guidelines for dealing with access requests from individuals?
 - Is a named individual responsible for handling access requests?
- 9. Respond appropriately to Freedom of Information requests**
- Are there clear procedures and guidelines for dealing with FOI requests from individuals?
 - Is a named individual responsible for handling FOI requests?

4.3 Checklist of issues for a Records Management policy

1. Does the institution have a records management policy?
2. Has the policy been authorized at an appropriate senior level?
3. Does the policy cover all records in all formats
4. Does the policy identify legislation, standards and codes of best practice to which the institution is subject?
5. Does the policy identify the institution's records management requirements?
6. Has the policy been promoted throughout the institution?
7. Is the policy addressed in the institution's operating procedures and manuals?
8. Is the policy known and understood by all staff?
9. Does the policy outline the various roles and responsibilities for staff who manage or perform records management processes throughout the institution?
10. Are records management responsibilities documented in job descriptions?
11. Have staff received the appropriate level of training to help them carry out the records management responsibilities outlined in the policy?
12. Is staff compliance with the policy monitored?
13. Is the policy reviewed at regular intervals?

4.4 Checklist of issues for staff working at service desks

As a general principle, data about library users should **never** be revealed to third parties either deliberately or accidentally. This includes, friends, parents, relatives, classmates, lecturers/tutors, landlords, Gardaí, etc.

1. If anyone asks for information about a library user, or anyone else, do not give it to him or her.
2. Do not even reveal whether the library has information about an individual.
3. Enquiries from the Gardaí should be referred to Security, Registry, HR or other named people in the institution. A procedure should be in place to deal with such enquiries.
4. Requests for information about loans, overdue, renewals, reservations etc. can be answered on production of an ID card, staff card or other identification. These should be checked carefully.
5. Telephone, written or email enquiries about loans etc. require the quotation of a library ID, often the barcode number. In some cases another unique identifier such as a PIN number may be required.
6. Treat all information about library users as private and secure.
7. Do not allow other users to deliberately or inadvertently see another user's personal information on a screen. Screens should be cleared after each transaction.
8. Dispose appropriately of any paper records such as correspondence regarding fines overdue etc. Appropriate disposal may include shredding or the use of confidential waste bins.
9. Where relevant, refer to library or institutional records retention schedules. Files should be purged or weeded regularly and should be deleted/destroyed when no longer required for the stated purpose.
10. Do not discuss library users, in person or on the phone, within the hearing of other library users.
11. Requests for loan history information in cases of plagiarism should be referred to a senior member of staff. Information may be released as appropriate.
12. If information is held about an individual, they have the right to inspect this data. Any request under right of access should be referred to the appropriate named person in the library or institution.
13. When adding a message to a user's borrower account on the library management team the message should be shown to the user and the reason for recording the message explained. (Infringement of library rule, fines message etc.)

4.5 Sample Questions

The following examples, which are not exhaustive, may help in dealing with some typical queries that may arise at issue and information desks in the library. Frequently the questions will seem reasonable and the requestor may not understand your refusal. It helps if the procedure and reason for it is explained.

Q.1 *Please can you tell me which books I have on loan?*

You can give this information provided the user shows you his/her current Library card.

If this request is made by someone who has forgotten his or her card, some other identification is required preferably with a photograph.

Q.2 *I am ringing (or emailing) to enquire what books I have on loan?*

This information can be given over the phone or by email once the user can give you their library ID number or barcode.

Q.3 *You may not have my correct address. Can you tell me what address you have?*

Addresses should not be divulged. Remember cards can be stolen. Instead ask for their library ID and then ask the user for their correct address. If the address is different do not disclose it. Refer the user to student records/registry to have their address amended.

Q.4 *Can I renew my books, I don't have my library card.*

As with Q.1, if the user has come to the desk in person you can renew books based on another acceptable form of ID.

Telephone or email requests to renew should not be done without a library ID number or barcode.

Q.5 *My friend has asked me to check what books they have on loan?*

You cannot do this. Borrower details should not be supplied to a third party – friend or relative. The exception to this rule may be where a user has a designated assistant in the case of illness or where there may be mobility issues.

Q.6 *I have requested a book and it is overdue. I think someone in my class might have it – can you tell me who it is?*

You cannot do this. Borrower details should not be supplied to a third party.

Q.7 *I have reserved a book but someone has reserved it before me – can you tell who it is?*

You cannot do this. Borrower details should not be supplied to a third party.

Q.6 *A lecturer asks for information about who has a course book on loan*

You cannot do this. Requests from lecturers can be hard to refuse but again borrower details should not be supplied to a third party.

Q.7 *I am trying to trace an old friend who may be on your files. Could I have their address?*

You cannot do this. Personal information should not be supplied to a third party.

Q.8 *This is the Gardaí. We need to locate someone urgently and the only identification we have is their library card.*

Firstly you need to verify that the call is legitimately from the Gardaí. Ask the caller for details of their name, phone number and Garda Station and refer the query to the appropriate person within the library or institution.

Q.9 *I am trying to fill out an application form on your website and it is asking for my library ID number. I don't have it with me as I am at work – can you give it to me?*

You cannot do this. The ID/barcode is a unique identifier and cannot be disclosed.

Q.10 *I think my daughter/son/friend/partner is in the library – I need to find them urgently – can you tell me if they are there?*

You cannot do this. Personal information should not be supplied to a third party. Also you do not know that they are who they say they are.

Q.11 *I am preparing a video/photographic assignment. May I film/take photographs in the library?*

Photographs and images are considered personal data. Inform the requestor that permission must be sought from the library. They must also ask permission of any person they wish to photograph or film.

Q.12 *You are holding a copy of my thesis, can you tell me who has asked to see it?*

You cannot do this. Borrower history information should not be disclosed to a third party even if the requestor is the author of the item borrowed.

4.6 Checklist of issues for staff about their own rights

1. Right of access

Under Section 4 of the Data Protection Acts, 1988 and 2003, you have a right to obtain a copy of any information relating to you kept on computer or in a structured manual filing system by your employer.

2. Institution's right to process employee data

As part of the contract of employment it is implied that employees have agreed for the institution to hold and process personal data about them for designated purposes. In turn as an employee you have the right for all data recorded about you to be correct, securely held and not held for longer than the purpose for which it was intended.

3. Right of rectification or erasure

If you find out that information held about you by your employer is inaccurate, you have the right to have it corrected or if the information is irrelevant or excessive for the purpose you have the right to have that information erased.

4. Notification of changes in personal data

Employees have a duty to inform the institution of any changes of name, address etc. to ensure the accuracy of information held.

5. Freedom from automated decision making

As an employee important decisions about you, such as rating your work performance or reliability, may not be made solely by computer automated means. As a general rule, there has to be human input into such decisions.

4.7 Checklist of issues for staff holding files that might include comments or opinions about individuals

Frequently in the course of library business, comments and opinions about individuals are recorded and retained. Examples would include comments about staff performance, comments on problems with individual users etc.

Under Data Protection or Freedom of Information legislation all such records are subject to disclosure upon request. Before deciding to retain and record such comments and in the interests of good practice a useful test is to ask yourself two questions:

1. Is the comment objective, fair, accurate and justifiable?
2. If I were to show this information to the individual concerned would I still be confident that the comment is objective, fair, accurate and justifiable?

4.8 Checklist of best practice for Records Management

Objective

- To ensure the creation and maintenance of authentic, reliable, complete and secure records that serve as evidence and support of past, present and future organisational activity.

Composition

- Compose in a clear, concise, factual and objective style
- Be aware of the responsibility to be accountable
- Record opinions in the context of the facts
- Avoid personal or anecdotal remarks
- Write manual notes and annotations legibly
- Date and sign all notes and documents
- Record attendees of meetings
- Record discussions that contribute to decisions
- Record decisions as soon as they are made
- Only record third-party comments with consent

Maintenance

- Use a communication medium appropriate to the subject matter
- Maintain documents that support decisions
- Destroy notes and drafts that have not contributed to decisions
- File records in a logical sequence
- Classify records in a structure that reflects the function of the office they serve
- Ensure storage and security of records are appropriate to the subject matter

Retention/Disposal

- Keep records for a specific purpose
- Retain records no longer than is required for the specified purpose
- Dispose of records in a manner appropriate to the subject matter

Appendix III: Bibliography

Archives Ireland. Records Management <http://www.archives.ie/management.htm> (accessed 26/11/2004)

Comhairle: Citizens Information Database (1999) The Information Commissioner: Protecting your right to know <http://www.cidb.ie/live.nsf/0/8025636c004d1a8d80256778003f3fa2?OpenDocument> (accessed 26/11/2004).

Data Protection (Amendment) Act 2003
<http://www.oireachtas.ie/viewdoc.asp?fn=/documents/bills28/acts/2003/a603.pdf>
(accessed 26/11/2004).

Data Protection Act 1988 <http://www.irishstatutebook.ie/ZZA25Y1988.html> (accessed 26/11/2004).

Data Protection Commissioner (2003) Data Protection (Amendment) Act, 2003: A Summary Guide. <http://www.dataprivacy.ie/images/New%20Act%20Summary-website%20version.pdf> (accessed 26/11/2004).

Data Protection Commissioner <http://www.dataprivacy.ie/index.htm>.

Data Protection Commissioner. Self-assessment checklists for data controllers
<http://www.dataprivacy.ie/3k.htm> (accessed 26/11/2004).

Data Protection Commissioner. Data Protection Acts, 1988 and 2003 – A Guide to your Rights
http://www.dataprivacy.ie/images/A%20Guide%20to%20Your%20Rights_web%20version.pdf
(accessed 26/11/2004).

Department of Finance. Freedom of Information Act, 1997 - Short Guide
<http://www.finance.gov.ie/viewdoc.asp?fn=/documents/foi/foi2.htm> (accessed 26/11/2004).

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *Official Journal L 281*, 23/11/1995 P. 0031 - 0050

Fifteenth Annual Report of the Data Protection Commissioner, 2003.
http://www.dataprivacy.ie/images/annual_report_2003.pdf (accessed 26/11/2004).

Freedom of Information (Amendment) Act 2003
<http://www.oireachtas.ie/documents/bills28/acts/2003/a903.pdf> (accessed 26/11/2004).

Freedom of Information Act 1997 <http://www.gov.ie/bills28/acts/1997/a1397.pdf> (accessed 26/11/2004).

ISO 15489-1:2001. Information and Documentation – Records Management – Part 1: General. International Standards Organization.

ISO 15489-2:2001. Information and Documentation – Records Management – Part 2: Guidelines. International Standards Organization.

JISC infoNet. Records Management InfoKit. Joint Information Systems Committee.
http://www.jiscinfonet.ac.uk/InfoKits/records-management/index_html (accessed 26/11/2004).

Office of the Information Commissioner <http://www.oic.gov.ie> (accessed 26/11/2004).

Office of the Information Commissioner: Annual Report, 2003.
<http://www.oic.gov.ie/2612/OICAR03e.pdf> (accessed 26/11/2004).

Senior, Karen (2003) Data Protection Issues: checklists for Libraries. Advisory Committee on Access to Information Systems and Services of SCONUL.
http://www.sconul.ac.uk/activities/info_systems/papers/dpa_checklist.doc (accessed 26/11/2004).

Shepherd, Elizabeth & Yeo, Geoffrey (2002) Managing Records: a handbook of principles and practice. London: Facet Publishing. ISBN 1-85604-370-3.