

# Good Practice in Records Management and Information Security



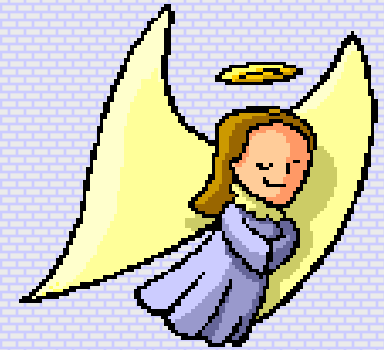
# How Valuable are Records & Documents?

- Valuable only because of the information they contain.
- Usable if they can be accessed when needed.
- Retain some records for legal and business reasons.
- Which ones and for how long?
- Avoid this question by keeping everything?
- As volume grows, operational efficiency would be hindered and space consumed.
- Contravene DPA - keeping for longer than necessary & it would be difficult to locate records effectively.
- **So what do we keep and how do we manage them?**

# We Often Keep Records for-

- Compliance with legislation and regulations.
- Cost benefit- balance the retention costs against potential cost of not having the record available.
- Audit requirements/accountability.
- Need to share information.
- We don't know what else to do with them!
- Records are an important resource. They are evidence of our activities and conduct.
- Expensive to produce and keep-space costs money.
- Common sense- don't keep any records that are not required for legal or administrative purposes.

# Perfect World



- " A systematic and planned approach to the management of records within an organisation, from the moment they are created to their ultimate disposal, ensures that the organisation can control both the quality and the quantity of the information it generates"

*Public Record Office Management Standard 1998.*

# Records Don't Manage Themselves

- There are legal obligations to protect records and manage information.
- Public Bodies have a records management duty in the following enactments:
  1. Public Records Act (NI)1923. (They have ownership of all Public Records)
  2. Disposal of Document Order (No 167)1925.
  3. Freedom of Information Act 2000 (code of practice refers).
  4. Data Protection Act 1998.
- **We need to understand why we retain and manage our records.**

*Not managing paper work is like dropping a stone into a pond. The ripples affect everyone around.*



# STRATEGY - POLICIES - SYSTEMS

How to find it

What we hold

What we disclose

How do we know?

What we publish

What to keep and what to dispose off

# Records Management-Key to FOIA



- What information do you hold?
- Why are you keeping it?
- Can you access information easily?
- Do you record information legibly?
- Do you use retention guidelines?
- Do you dispose off information correctly?- a generic disposal schedule has been developed for NI schools.- You should use it.

# Document Retention Policy

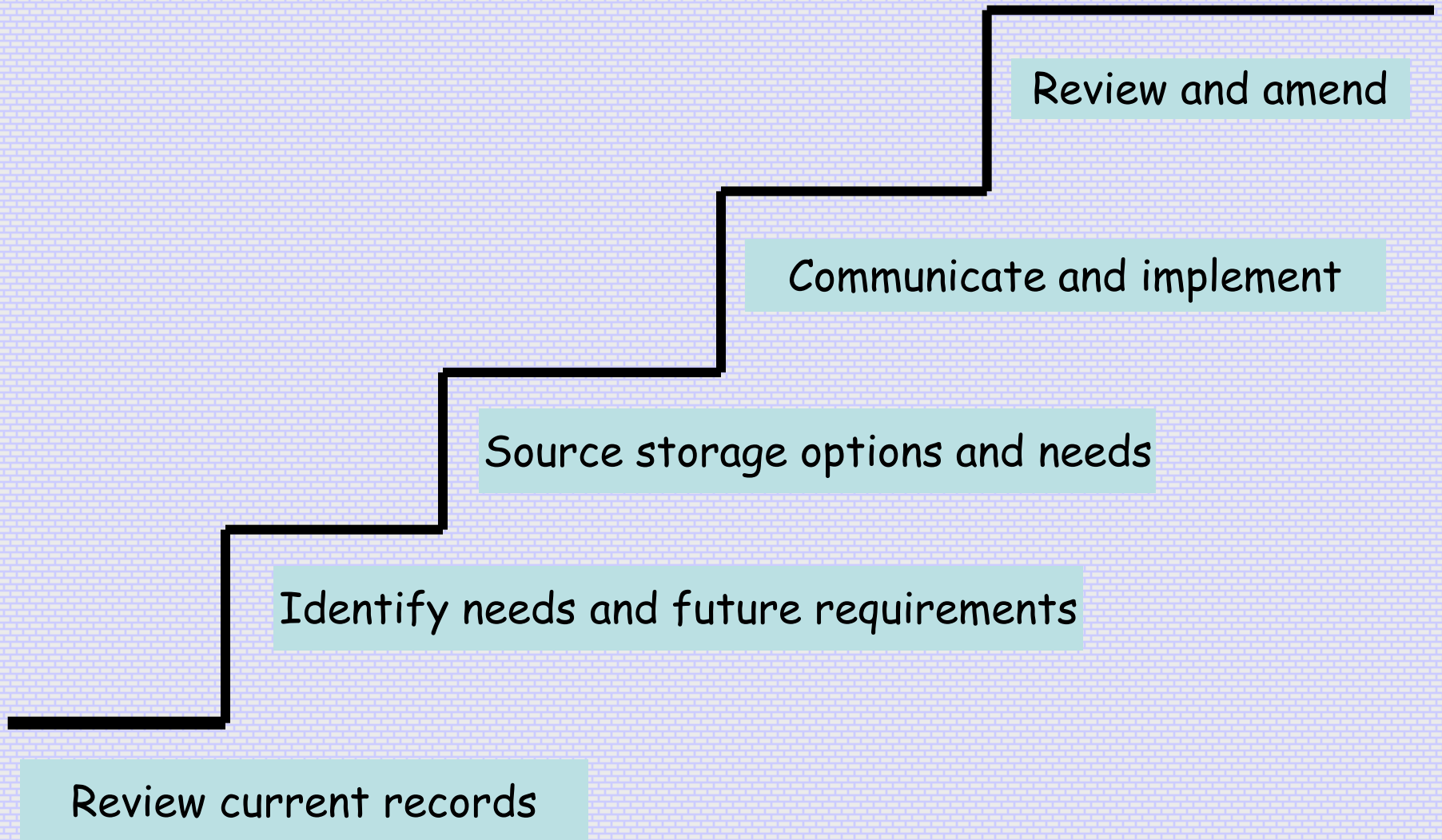
- Document management is not an accident.
- It has to be planned and implemented.
- A policy should set out:
  - What records should be kept.
  - How and where they are stored.
  - How they are accessed.
  - When and how they should be destroyed.
- It should also identify who is responsible for managing the documents/records.



# Why have a Policy?

- Even if your policy is not set out formally- you must have a policy of sorts, by default.
- People get to know who has which records and documents are usually destroyed as space dictates.
- Maintains consistency and accountability.
- Meets legislative needs.
- Releases space for other needs.
- Frees up staff time.
- Gets away from a "*we must keep everything, just in case*" approach.

# Steps Towards Document Retention Policy

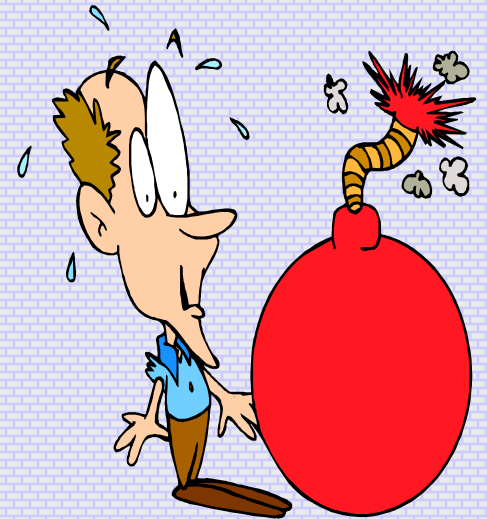


# Records Management- The Benefits.

- Complete and accurate records in the right place, at the right time.
- No gaps ensures good audit trails and reduced legal risks.
- Compliance with time scales.
- Savings. No space, equipment or stationery wasted storing unnecessary records.
- Reduced disposal costs/ improved working space.

# Risks in Not Managing Records

- If you don't know what you have or where it is, how will you know if someone takes, loses or destroys it?
- Time consuming costly investigations. Fines and other penalties- FOIA and DPA



# What is a Disposal Schedule?

- A disposal schedule gives legal authority to dispose of your records.
- Advises the minimum period you should keep certain series of records.
- Advises what can be destroyed and what has to be preserved/ offered to PRONI.
- A generic schools disposal schedule has been developed. It is on the DE web site.- [www.deni.org.uk](http://www.deni.org.uk) Link to- schools/school management, then disposal of school records- for a copy.
- Common sense- don't keep any records that are not required for legal or administrative purposes.

## Benefits of Using a Schedule?

- Impact on information requests - you should be able to say immediately if you have/do not have the record.
- You know the minimum retention period for each specific series of records.
- Costs - staff time, space- files going to archive storage will have a clear date of disposal and action.
- Retention periods/disposal actions are relevant to your work.
- Records no longer used can be removed.
- New records can be added.



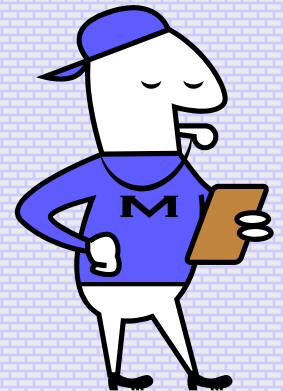
# Outcomes to be Achieved

- Information stored, organised and disposed enables best use and easy retrieval.
- Staff know what they should be doing and are doing it!
- Proper recording and documentation of requests and decisions so you know you are acting fairly, consistently and in compliance with legal obligations.
- Information valued by everyone.
- Embrace a culture of recording what is important and structuring it so that decisions on whether it can be released are easily facilitated.

**We manage our records by design- not by accident.**

# What is Required ?

- Collective ( and realistic) decisions on what needs to be kept.
- Knowledge of what information is held.
- Ability to find information easily.
- Ability to balance the cost in keeping the information against the cost in not keeping it.
- Decide what information should be kept close to hand and what can be away from the " desk", in archive storage.



# Don't forget electronic records.



Where Tom keeps things



General



Miscellaneous



The team



The team (2)



Comms



Lost and never found



# In the Beginning.....

- Records Management—low priority.
- No policies or procedures.
- Variety of filing methods. No guidance.
- Arbitrary approach to retention.
- Not just about filing.
- Storage problems—Where do we start???
- Long way to go.....



# Good Practice

- Sensitive paper based records- lock away when not in use, in desks, filing cabinets or cupboards. Keys should be kept in a safe place.
- Ensure you securely dispose of paper and electronic records. Issue guidance and procedures for staff.
- Encryption- use- if your job *requires* taking information out of the office setting. Have you a policy on this?
- Do not keep paper records for longer than necessary. Destroy when not needed.
- Allocate and use disposal dates.



# Good Practice

- Paper record storage locations and destruction of records should be approved. You need to know what records you have , why you are keeping them, where and how you are keeping them and how long you *really* need to keep them.

REMEMBER



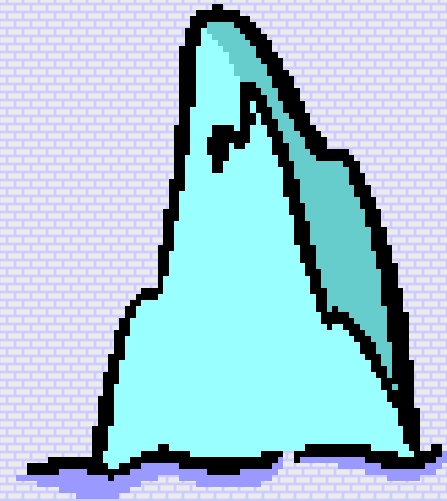
- Follow any guidance issued. Existing practices often need revisited and reviewed .
- Information security is everyone's responsibility.

# Information Security



# Why Think about Security?

"I have never been in an accident of any sort and have never been wrecked, nor was I ever in any predicament that threatened to end in disaster of any sort"



E. J. Smyth - Captain of the Titanic

**Information Security** means guaranteeing the confidentiality, integrity and availability of information.

- **Confidentiality**- only people who are authorised to process information can handle it.
- **Integrity**- personal information should be accurate and not kept for longer than necessary.
- **Availability**- **ONLY** authorised users should be able to access the data if they need it for specific purposes.

# Computer Security -User Responsibilities

- Make sure you know and follow your school's procedures for using computers securely.
- If removing information from school, look at using encrypted software/ memory sticks.
- Never give anyone your password or use another persons password.
- If allowing third party access to your systems make sure you have assurances and controls in place.



# Named and Shamed in Media

- Education records found by road side in NI.
- Unencrypted discs with names and addresses of 6,000 NI motorists -missing in post.
- Hospital laptop with 5000 medical records lost.
- DVLA lost three million learner driver records.
- Citizens Advice Bureau in Belfast lost 60,000 records along with bank details - stolen laptop.
- TK Maxx lost up to five million UK credit card records.
- Member of staff sold 250,000 records from "loans. co. uk."
- Leeds Building Society lost data on its entire workforce.
- 600,000 personal details of applicants to armed services were stolen with an unencrypted MoD laptop.
- MoD admits having lost 658 laptops containing unencrypted information since 2005.



THE Ministry of Defence is facing ridicule after admitting yesterday that 658 of its laptop computers have been stolen over the past four years – nearly double the figure previously claimed.

It also said that 26 portable memory sticks containing classified information had been stolen or misplaced since January.

The Liberal Democrats condemned the latest security breaches – which happened despite a desperate cross-Whitehall drive to tighten procedures – as evidence of ‘shocking incompetence’.

However, the MoD insisted that its policies were ‘generally fit for purpose’, and said all data losses were fully investigated.

The embarrassing details were disclosed by ministers in response to questions tabled in Parliament.

Previously the MoD had confessed to 347 laptops being stolen between 2004 and 2007.

But Defence Secretary Des Browne was forced to issue revised figures after ‘anomalies in the reporting process’ were discovered.

The official total is now 658 laptops stolen, with another 89 lost. Only 32 have been recovered. In a separate response, ministers said that 131 of the department’s USB memory

# We’ve had 658 laptops stolen, MoD confesses

sticks had been taken or misplaced since 2004.

Some 26 of those went this year – including three which contained information classified as ‘secret’ and 19 which were ‘restricted’.

Lib Dem frontbencher Sarah Teather said: ‘It seems that this Government simply cannot be trusted with keeping sensitive information safe.’

‘It is frightening to think that secret MoD information can be lost or stolen. How can they expect us to trust them to keep our personal information safe in their unnecessary and expensive ID card scheme?’

Last month the MoD was heavily criticised by a review of its data procedures which warned that basic security discipline had been forgotten and

there was ‘little awareness’ of the danger of losing information. A spokesman for the department said yesterday: ‘Any loss of data is investigated fully. The recent report on data losses found that MoD policies and procedures are generally fit for purpose, but

---

## ‘Working through an action plan’

---

also identified a number of areas where MoD needs to do better in protecting personal data.

‘MoD has developed, and is now working through, an action plan to address all of the report’s recommendations

and bring the department’s handling of personal data to an acceptable state.’

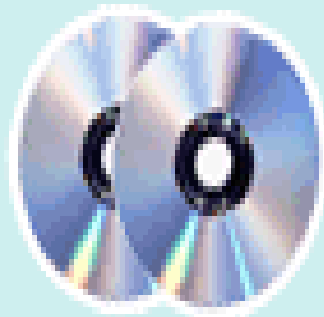
The ministry’s admission is the latest in a series of catastrophic data losses by the Government. In November last year Revenue and Customs admitted it had lost the details of more than 25million child benefit claimants.

Two discs had been mislaid which included names, dates of birth, bank and address details.

In December Transport Secretary Ruth Kelly admitted her department had lost personal details held by the Driver Vehicle and Standards Agency. Later that month nine NHS trusts admitted they had lost details of hundreds of thousands of patients.



CDs sent  
by courier



Second  
package sent



Managers told  
of loss

## 25 Million Lost Records



Parliament told



Police informed



Prime minister  
informed

“During 2007 alone, **36,989,300** people in the UK have had their private records compromised.”

and they all thought...

It could never happen to us.



# Are Things Improving?

# SONY



**Sony announces service restoration and enhanced customer data protection after 100 million gamers have their personal information compromised**

*This is not just any laptop theft, this is an M&S laptop theft*

*Unencrypted laptop with 26,000 employee details*

YOUR M&S

# Are Things Improving?



Belfast Health and  
Social Care Trust

Thousands of cancer patients  
notes abandoned at Belvoir Park  
Hospital.



# Are Things Improving?

## BREAKING NEWS- MARCH 2012- SECURITY BREACH

NAMES

BANK DETAILS

DATE OF BIRTH

HOME ADDRESS

PASSPORT NUMBERS

CAR REGISTRATIONS

NATIONAL INSURANCE NUMBER



**Belfast City Council**

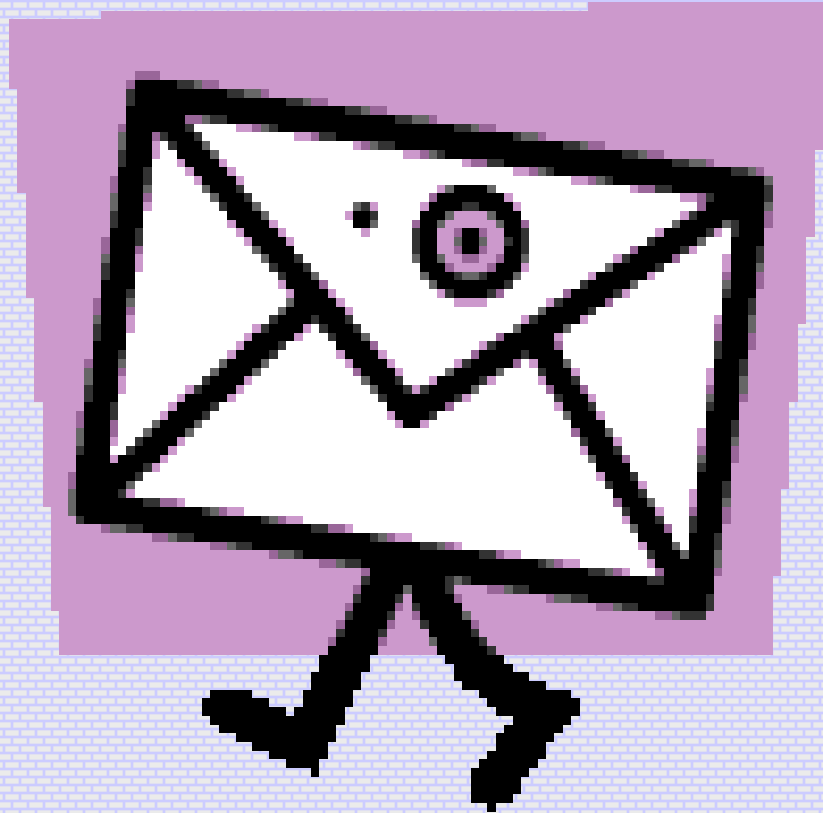
**BELFAST CITY COUNCILLORS**

# Penalties

Note:-

- Everyone has a shared responsibility to secure personal information used in their day to day professional duties.
- Be aware of risks and threats and how to minimise them.
- Individual staff can be liable for fines/ damages if they breach the DPA.
- ICO can impose fines for serious breaches- up to **£500,000**.
- Media may publish details.
- Lack of trust between school and parents.
- Breaches of security must be reported to ICO.

# Using E-Mail



# E-mails are Public and Permanent.

- E-mail is insecure. Compare it to sending a post card- anyone who receives it can read it.
- E- mails are hard to destroy. Don't assume that deletion means its gone for ever. Electronic documents are backed up and recoverable.
- Have you an internet and e-mail usage policy?



# E- Mails are Public and Permanent

You have a responsibility not to:

- waste time or resources;
- expose the network to risk of corruption;
- breach any law or statute;
- bring the school into disrepute.

**Remember -don't do any thing that will harm you privately or professionally.**

# E- Mails are Public and Permanent

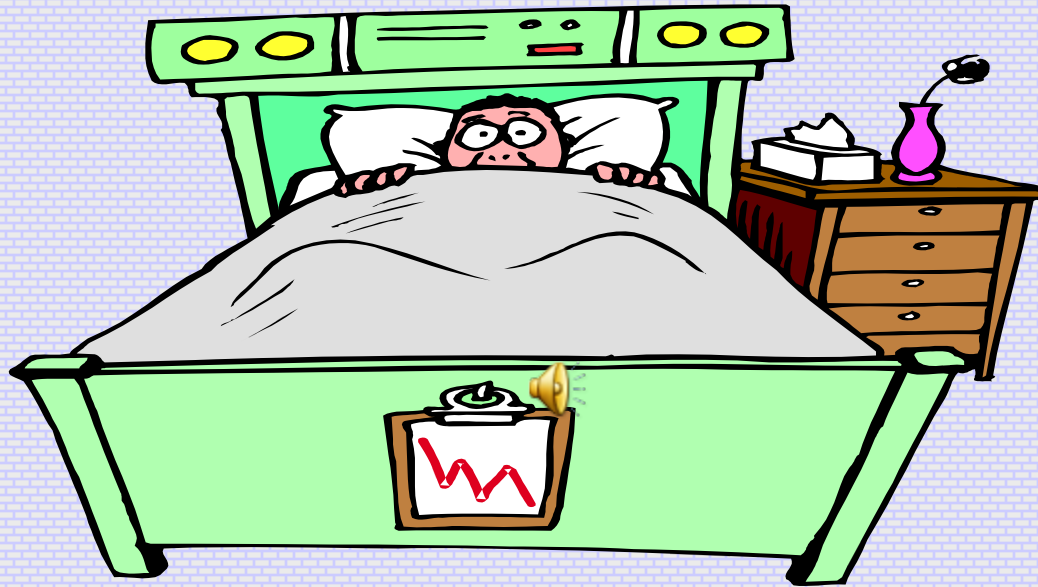
- Don't discuss sensitive issues.
- Beware sending inappropriate material- it could be misunderstood.
- Be careful what you say- you cannot control who will read your comments.



**REMEMBER**

**E- mail is a fast and easy way to communicate non confidential information.**

# Information Security in the Workplace



Neglecting information security  
can seriously damage your schools  
health!