

Everyone in the workplace has a legal duty to protect the privacy of information about individuals



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."

.



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

- **Confidentiality**- only people who are authorised to process information can access.
- **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.

Named and Shamed in Media

- Education records found by road side in NI.
- Unencrypted computer discs containing the 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.
- Nine NHS trusts lost 168,000 confidential records.
- Citizens Advice Bureau in Belfast lost 60,000 records along with bank details - stolen laptop.
- TK Maxx lost an estimated five million UK credit card records and compromised accounts for 200 million customers worldwide.
- 250,000 records from loans. co. uk were compromised when a member of staff sold them.
- Leeds Building Society managed to lose data on its entire workforce of 1,000 people.
- 600,000 personal details of applicants to armed forces were stolen with an unencrypted MoD laptop.- MoD admits having lost 658 laptops containing unencrypted information since 2005. ETC, ETC, ETC



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.

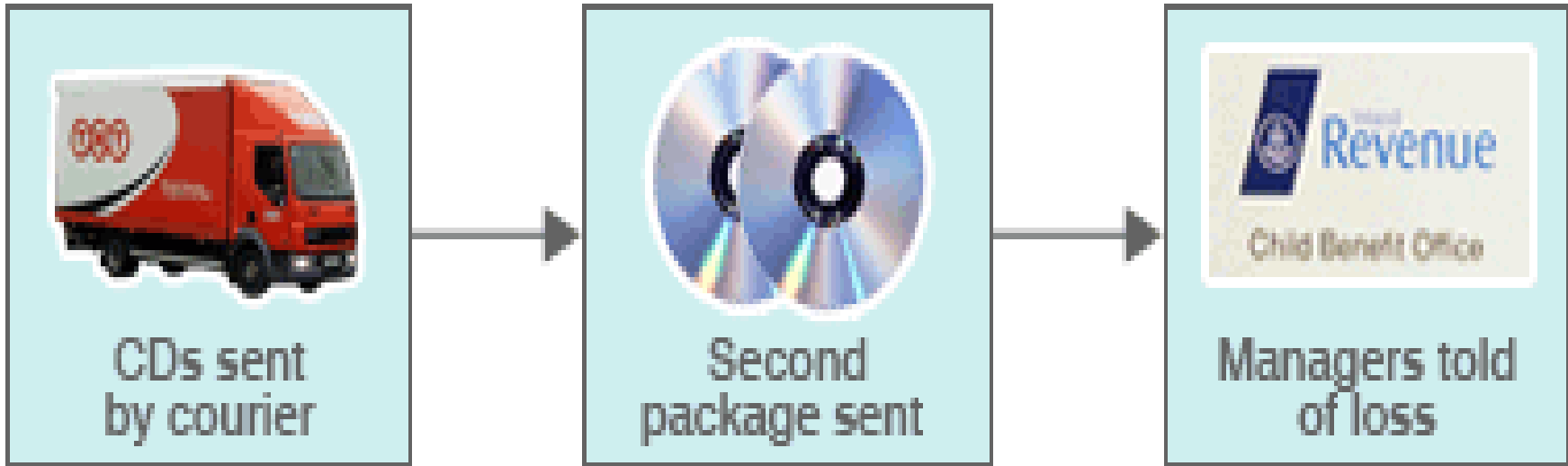
‘MoD has developed, and is now working through, an action plan to address all of the report’s recommendations

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.



25 Million Lost Records

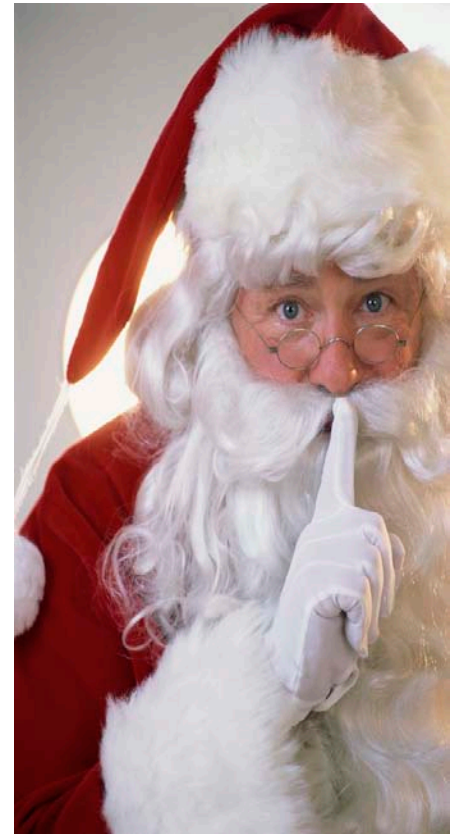


Everyone has a Duty to Protect Information

- Do not keep paper records for longer than necessary. Destroy when not needed. Adopt disposal dates. Seek advice from school/belb on protocols.
- 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.
- Encryption- USE- if your job *requires* taking information out of the office setting. Have you a policy on this?
- REMEMBER -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.

Good Practice

- Never give anyone your password or use another persons password.
- Make sure you have and follow procedures for using computers securely.
- If working in an open plan office be careful if discussing a persons details- you don't know who is listening.
- Ensure information displayed on your computer screen cannot be seen by any unauthorised person.



Security - Everyone's Responsibility!

- Refer to guidance offered by belb/schools or the office of the Information Commissioner.
- Existing practices often need revisited and reviewed .
- Remember- data security is everyone's responsibility.



Ask Yourself

- Are you registered with ICO.
- Do you have a policy for handling data.
- Are you aware of your responsibilities under DPA.
- Are your staff aware of their responsibilities.
- Are you aware of the 8 Data Protection Principles.
- Do you keep information securely.
- Do you dispose of information securely.
- Do you know how long you need to keep information-
You need to identify the information you have,
understand why you are keeping it, know where / how
it is kept and agreed how long it needs to be kept.

Who can Ask for Information?

Anyone can ask for information-They have legal rights under law.

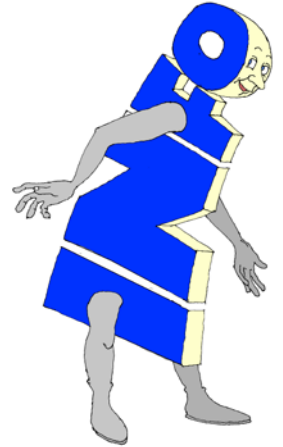
1. Data Protection Act (DPA)- subjects personal information. - applies to anyone who keeps data.
2. Freedom of Information Act (FOIA)- policies, procedures, decision making etc. - applies to those designated. If you hold information which originated from a school or elb's, you can be asked for it.
3. Environmental Information Regulations.- e.g. recycling, fuel use, car parking etc. - those designated.

Data Protection Act

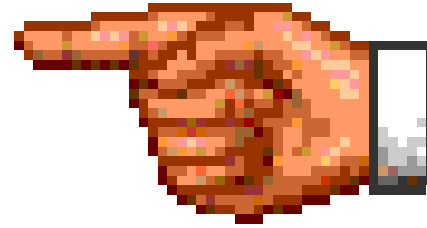


Belb Responsibilities

- All contractor's, agents and other non-permanent staff used are aware of and comply with the Data Protection Act 1998.
- All personal data they hold is kept securely and is disposed off in a safe and secure manner when no longer needed.
- Comply with protocols agreed with schools/belb.



DPA -YOU MUST



1. Register with the Information Commissioner (IC)- this is known as 'notification'. This is done annually.
2. Observe the eight data protection principles or rules of good information handling.
3. Allow the data subject to exercise their rights. This can include pupils!

Criminal offence not to register with IC.

ARE YOU REGISTERED?

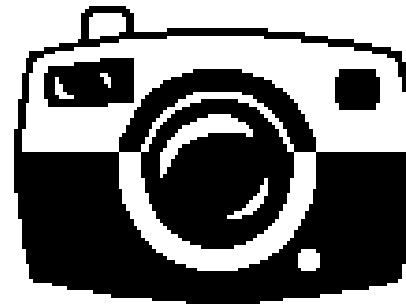
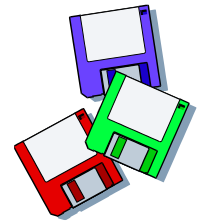
About DPA

- Applies to **both** public and private sectors.
- Gives individuals certain legal rights to access information held about themselves.
- Sets rules about the way personal data should be handled and processed.
- Establishes 8 rules of good information handling.
- Organisations must be open about how information is used, kept and destroyed.





Applies to all recorded information, whether stored electronically/paper based filing systems, all media such as audio, video, photographs, camcorder footage, internet.



8 Data Protection Rules.

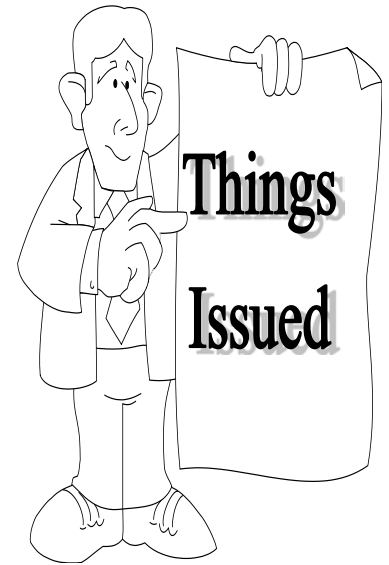
1. Fair and lawful processing.
2. Processing for specific & lawful purpose.
3. Relevant not excessive.
4. **Accuracy of data. Personal data shall be accurate, and where necessary, kept up to date".**
5. **Not kept for longer than necessary. Personal data shall not be kept for longer than is necessary, for the purposes for which it is being processed."**
6. Processed in accordance with data subjects rights.
7. **Kept securely. Appropriate security measures shall be taken against the unauthorised or unlawful processing, accidental loss , destruction, or damage of personal data.**
8. Personal information shall not to be exported outside the European Economic area - i.e. to any country without adequate subject protection rights.

DPA Requests

- Must be made in writing and responded to within 40 calendar days.
- Telephone enquiries-make sure you have a policy on releasing information that your staff know about. Do not release information verbally.
- Always check applicants identity.
- Never give out information about another person i.e. home address to friends or relatives of an employee/pupil.
- Do not be bullied into giving information.
- Police should submit a Form 81 if requesting information.

DPA Requests

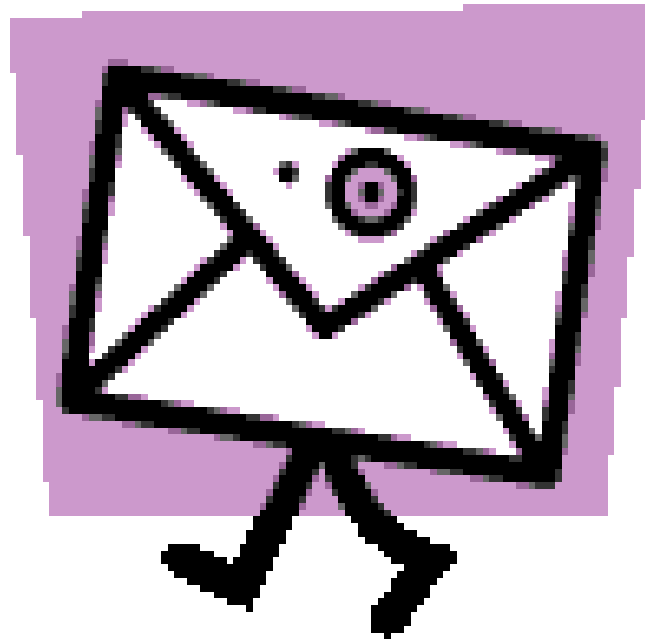
- If you are not sure what information you can release - Ask.
- Check if you can legally withhold information- remember the data subject has rights.
- Always keep a record of exactly what you have released or withheld.
- If handling sensitive data- think- Is releasing it by post/fax/ e- mail really a secure format?
- Could applicant collect it in person?



Handling Requests

- Don't release information to **ANYONE**- unless you have been authorised to do so.
- Remember the DPA applies to all personal data held in whatever format.
- Wilful disclosure of personal information may be treated as a disciplinary offence. Individual staff can be liable where it can be shown they acted outside their authorized limits or if they deliberately or recklessly acted in breach of the law- Fines, criminal record and damages can be imposed.

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.
- 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.

E- Mails are Public and Permanent

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



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

Freedom of Information Act



What does the FOIA Do?

Gives greater access and establishes two related rights in law:

1. The right to be told if information exists;
2. The right to receive the information-

There are specific exemptions from that right.

- FOIA provides for the release of "exempt" information if assessed to be in the public interest.
- Applicant can make a complaint if not satisfied with how their request is handled.

Note: Does not apply to applicants personal data- this is handled under DPA.

The FOIA became law in 2005. Information is available on the Information Commissionersweb site -

www.ico.gov.uk

Are you a Public Authority for Purposes of FOIA?

- FOIA applies to organisations designated as “public authorities” under legislation.
- Your designation depends on the amount and type of information you process.
- Groups with charitable status may be subject to FOIA.
- To find out if your organisations status you need to contact the Information Commissioners Office-

<http://www.ico.gov.uk> Phone- 0303 123 1113

- They will discuss with you if your organisation is exempt from answering FOI requests.

If you hold Data on Behalf of a Public Authority?

- Schools and elb's are Public Authorities.
- If you hold information on behalf of either and the ICO has advised that your organisation is exempt from FOI, you must however advise the school or the board that such information has been requested and redirect the request. FOIA schedule 3 (2) (b) refers.
- Requests are time sensitive- 20 working days to respond. You need to be able to identify such requests and pass them on quickly.



If you are NOT Exempt from Responding to FOIA requests

- FOIA became law 2005.
- Anyone can access minutes, financial details, job descriptions, correspondence etc- everything you hold.
- Advice available from the ICO at <http://www.ico.gov.uk>
- Brief FOIA guidance follows-



Key Elements FOI Process

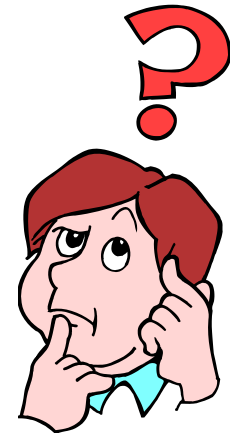
- Handling the request.
- The response.
- Internal review. (appeal)
- Communication.



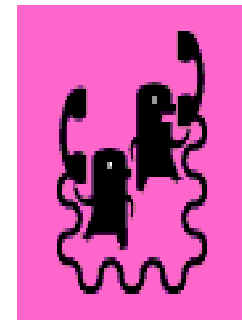
Reason for Request.

Curiosity- commercial reasons-research- public interest-
existing dispute-whistle blowing- to understand how you
make decisions.

Pure guess - we cannot ask for reasons!



What is a Valid FOI request?



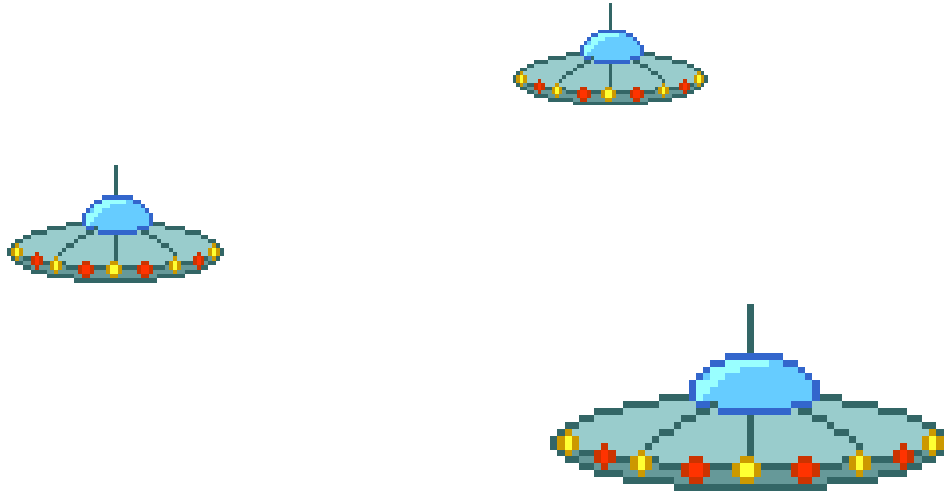
1. Verbal enquiries -NOT covered by the FOIA.
2. An FOI request should:
 - Be in writing (includes fax & e-mail)
 - Give name and address (e- mail address OK)
 - Describe the information.
 - No need for applicant to mention FOIA when making the request. You decide if the information requested is dealt with under the Act.
 - 20 working days to respond.
 - A subjects own personal information cannot be requested using the FOIA- refer to DPA.

Important to Know

- FOI requests must be made in writing.
- Anyone in workplace can receive a request.
- You need to have a procedure in place to identify requests quickly and refer them to line manager/ designated person.
- Check post or e- mails of staff who are not at work- consider using "out of office assistant" in e- mails.
- Make sure date of receipt is stamped on all post.
- Acknowledge receipt of request ASAP.



Who can Ask for Information?



- Anyone- a body or individual.
- From anywhere

Beware of Unstructured Information

- Every Note
- Every Doodle
- Every Scribble

Information access laws such as FOIA and DPA have implications on how we record information. Don't write anything embarrassing. There is no exemption for embarrassment.



What Happens if you don't get it Right?

- Complaint to Information Commissioner.
- IC can inspect information & order release.
- Breach of the act to fail to respond within the designated time limit- 20 days.
- Criminal offence to remove, hide, or not disclose information recorded in a document

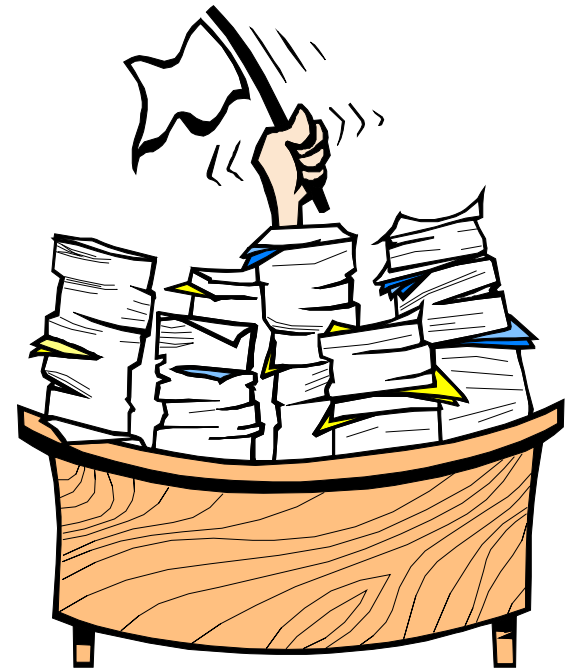
**Maximum penalty
2 years prison- plus fine**



Adopting clear policies for handling records will make life much easier- *really!*

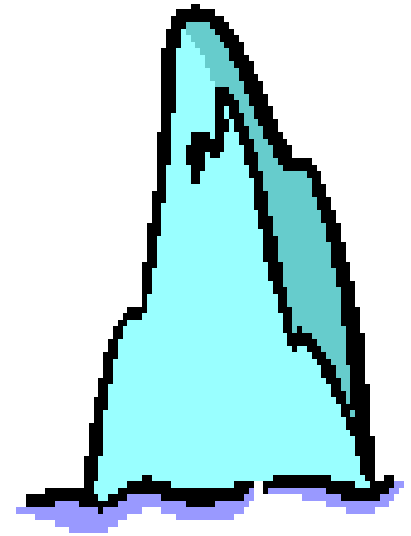
You need to think about:

- What you record.
- How you record it.
- Who you circulate to.
- What you keep!
- How long you keep it.
- Method of storage and disposal.
- Information is valuable- but it is only useable if it can be easily accessed when needed.



Why do I need take extra care?

Who said? "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