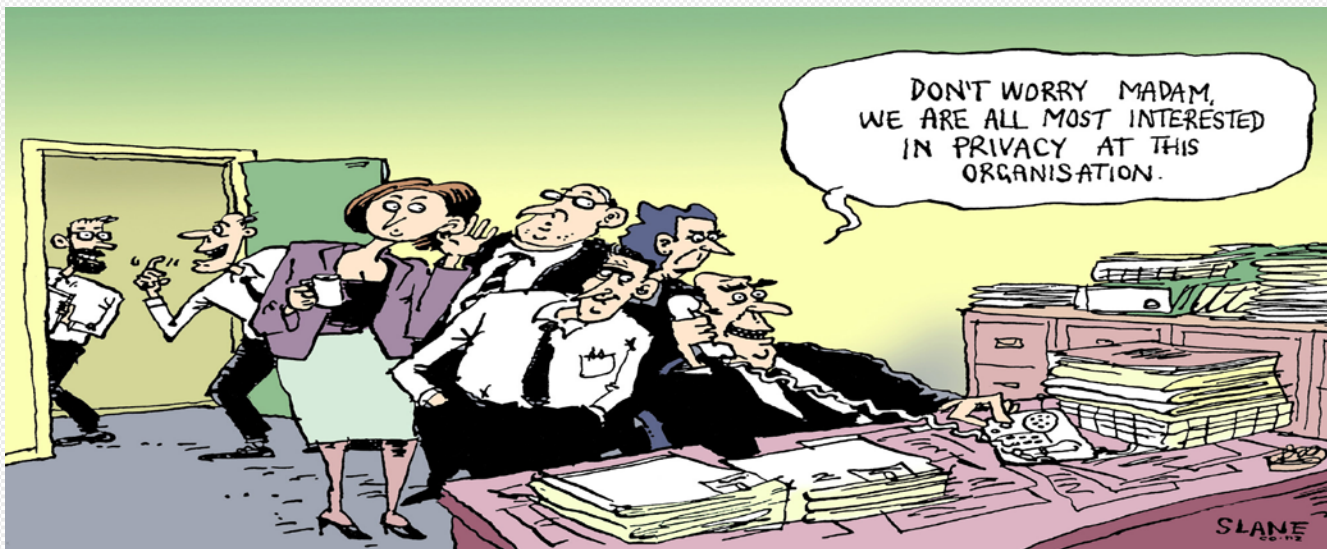


Everyone in the workplace has a legal duty to protect the privacy of information about individuals

Data Protection - How to Respond to Requests for Personal Information.



Data Protection Act



What does the DPA Do?

- Gives individuals (**data subjects**) certain rights to access information held about themselves. These rights are legally enforceable.
- Places obligations 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 **both** public and private sectors.
- Overseen by The Office of the Information Commissioner (ICO)

Does DPA Apply to my School?

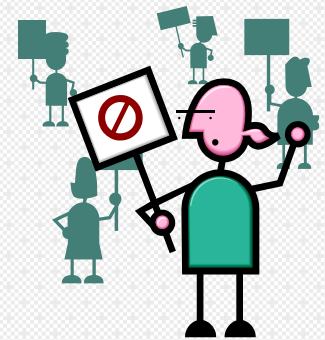
- Your school is a legal entity in its own right.
- It collects and makes decisions about the use of Personal Data.
- DPA regards your school as a Data Controller.
- DPA applies to a particular activity – processing personal data rather than to particular people or organisations.
- If you “process personal data”, then you must comply with the Act and you must handle personal data in accordance with the data protection principles in the Act.
- Broadly, if you collect or hold information about an identifiable living individual, or if you use, disclose, retain or destroy that information, you are likely to be processing personal data.
- If you are processing personal data you have to notify ICO.
- Failure to notify is a criminal offence.

What is a Valid Request?

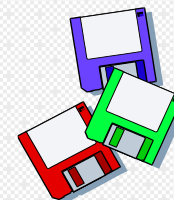
- Should be made in writing. A request by email or fax is as valid as one sent in hard copy.
- Request made verbally - good practice to explain how to make a valid request.
- If a disabled person finds it impossible or unreasonably difficult to make a subject access request in writing, you may have to make a reasonable adjustment for them under Disability Discrimination Act. (DDA)
- If an individual thinks you have failed to make a reasonable adjustment, they may make a claim under DDA.
- If DPA or subject access request, not stated, it is still a valid request.
- A request is valid if the individual has not sent it directly to the person who normally deals with such requests – so it is vital to ensure that staff can recognise a subject access request.

Rights of Individuals

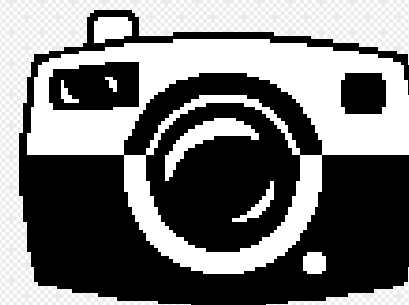
- DPA gives rights to individuals to access their personal data.
- This is known as a **subject access right**.
- These rights are legally enforceable.
- Right to prevent processing for the purposes of direct marketing.
- Rights in relation to automated decision making.
- Rectify, block, erase or destroy inaccurate data.
- Ask IC about whether the Act has been contravened.
- Prevent processing likely to cause damage or distress & take action for compensation if distress has been caused.



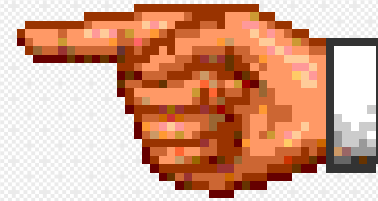
For the individual, the key to data protection is personal privacy and confidentiality.



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



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.

Criminal offence not to register with IC.

ARE YOU REGISTERED?

Remember its your responsibility to renew your registration annually- ICO will send a reminder.

Schools and the Data Protection Act

- Schools are legal entities in their own right. They collect and make decisions about the use of personal data.
- Schools must comply with the 8 data protection principles.
- Schools must notify processing with IC (notification)
- Requests are time sensitive- **40 calendar days to respond.**
- Can charge £10 per request. (if charging- be consistent- put charge in your school policy for handling information.
- No age limit to access contained in the Act – ICO advises that 12 years of age is a reasonable cut off- however school should consider if applicant aged under 12 has capacity to understand.
- Persons with parental responsibility can have access if the data subject is not capable.

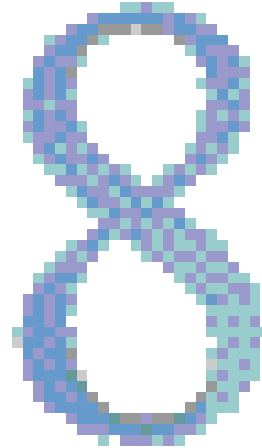
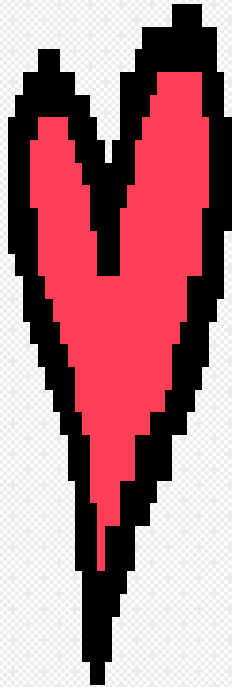
What is Notification?

- Information Commissioner (IC) maintains a register of Data Controllers. If you process personal data you must notify the IC about this.
- Failure to notify is a criminal offence.
- Notification lasts for one year and needs to be renewed annually at an annual charge of £35. Dedicated reference number allocated.
- Notification is how an organisation informs IC about its processing.
- IC is required to maintain a register describing your processing.
- The register is available for inspection on IC web site.
- The main purpose of notification and the public register is transparency and openness.

Basic principle of DPA that the public should be able to find out:

- Who is processing personal data.
- Other details about the processing such as why it is being carried out.

At the Heart of the Act there are Eight Principles of Good Practice



Data Protection Principles

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.

First Principle requires that personal data must be processed fairly and lawfully.

So, wherever your school wishes to use personal data, you must show that you have considered whether this would be fair to data subjects, taking everything relevant into account.

Second Principle states that data should be processed for limited purposes and not in any manner incompatible with those purposes.

- This amplifies Principle 1 by adding that your school must have a very specific reason or ***purpose*** for processing data. Further, the data can only be processed for that purpose and no other and what's more, all other processing must be comparable with the specified purpose.
- In short, if data are collected for personnel administration then personnel administration is all that you can do with it. You can't, for example, use it to target marketing material from a company offering services, even if they offer to pay you for your time and effort.

Third Principle - Information should be adequate, relevant and not excessive

- This means you should collect just the right amount of information for the specified purpose – no more and no less.
- To assess if you are collecting “excessive” personal data, review your forms and consider what information is necessary in order to enable you to do whatever it is you are trying to do.
- You could place an asterisk next to the fields that are essential for the intended purpose. This will enable individuals to decide whether or not to complete the fields. etc
- This is especially important in respect of data collection exercises that have been undertaken repeatedly over a long period of time.
- Often in such cases, the information originally collected becomes embellished with other information that is collected **because it might become useful.**
- This is a classic example of excessive and irrelevant data collection.

Fourth Principle- accurate and where necessary, up to date

- Personal data should be accurate at all times.
- Review at regular intervals (at least annually) to check that your “live” files are accurate and up to date.
- Avoid inconvenience or even damage or distress. For example: contacting parent in an emergency- not having the correct details could result in distress for families.
- DPA conveys the right to receive compensation where substantial damage or distress takes place so this could also be costly for school.
- Individuals not only have the right of access to their personal information but also the right to have this information corrected if necessary.
- This can be enforced through the courts- potentially causing adverse public attention through the media, which could be bad for the schools reputation.

Fifth Principle - not kept for longer than is necessary

- When any personal data that you hold has served its purpose, it must be disposed of securely.
- DE “school record disposal” schedule gives you an indication as to how long certain types of personal data should be retained. (*available DE web site <http://www.deni.gov.uk>*)
- In some instances, there are legal obligations in this respect; in others best practice determines this.
- The longer you hold “live” files, the longer you will need to ensure that they are accurate.
- Also, the longer that information is retained after its useful life, the less it becomes relevant and inconsistent with the third DPA principle.

Sixth Principle- processed in line with the data subject's rights

A Right to:

- Access the information comprised in their personal data .
- Object to processing that is likely to cause or is causing damage or distress.
- Prevent processing for direct marketing.
- Object to decisions being taken by automated means.
- In certain circumstances have inaccurate personal data rectified, blocked, erased or destroyed.
- A right to claim compensation for damages caused by a breach of Act.

Seventh Principle- kept securely

- All about having proper security.
- This does not just mean security on computer systems (such as password protection and the positioning of screens etc.)
- Includes measures such as locking filing cabinets.
- Not leaving confidential files on desks.
- Ensure waste personal data is disposed of by shredding etc.
- Ensure you are not disclosing personal data to someone who does not have a right to receive it- e.g. inadvertently by placing computer screen to be seen through school windows or at school reception.
- Similarly, by placing papers containing personal information in the ordinary waste or recycling bins at school.
- Disclosures made inadvertently like this are still unlawful and punishable by fines.

Seventh Principle- kept securely

A key aspect of the seventh principle, often overlooked is :

- It conveys the responsibility of training your staff about security procedures and the requirements of the Data Protection Act.
- This is to ensure that everyone dealing with personal information does so in a manner compliant with the Act .
- Staff appreciate that they themselves can be individually liable for any breach that they commit.

Seventh principle imposes another requirement.-

- This covers situations where contractors or persons (Data Processors) other than your staff process personal information on your behalf.
- You must ensure that security checks are undertaken.
- Any breaches of the Act by Data Processors would leave your school liable.

A close-up photograph of a wooden surface. Several pieces of crumpled, off-white paper are scattered across the wood. In the upper right, a black mesh strainer is partially visible, with more crumpled paper inside it. The lighting is warm, highlighting the texture of the wood and the paper.

**Data destruction –
be secure**



Eighth Principle-: Personal information shall not be transferred to countries outside the EEA without adequate protection

The Data Protection Act says that:

Personal data shall not be transferred to a country or territory outside the European Economic Area (EEA) unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Which countries are in the European Economic Area (EEA)

There are no restrictions on the transfer of personal data to
*EEA countries. These are currently:

Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden

*For an up to date list of such countries, please see the European Commission's data protection website at:
www.europa.eu.int/comm/justice_home/fsj/privacy/thirdcountries/index_en.htm.

New Powers to Issue Monetary Penalties.

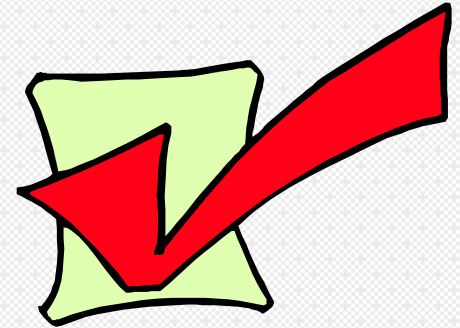


- The ICO's new power to issue monetary penalties for serious breaches of DPA came into force on 6 April 2010, allowing fines up to **£500,000** to be made.
- Case 1- Hertfordshire Council fined £160,000 for faxing sensitive data to the wrong recipients and the loss of an unencrypted laptop containing personal information relating to 24,000 people.
- Case 2- Ealing and Hounslow Councils fined £140,000 for the theft of an unencrypted laptop from an employee's home. Both councils had a policy in place that all laptops had to be encrypted. However laptops were issued in breach of this policy. ICO took the view that both councils failed to ensure that relevant policies were being followed or understood by staff.

Data can be Disclosed Where:

Main areas-

- Individual has given their consent.
- Disclosure is in the legitimate interest.
- The employer is legally obliged to disclose the data.
- The disclosure of data is required for the performance of a contract.
- Where specific exemptions for disclosure without consent apply.



Disclosure **WITHOUT** Consent



Certain disclosures are permitted under DPA if one or more of the following criteria are met: (Main areas)

- Safeguarding national security.
- Preventing or detecting crime.
- Assessment or collection of tax or duty.
- Discharge of regulatory functions.
- Preventing serious harm to a third party.
- Protecting the vital interests of the individual.

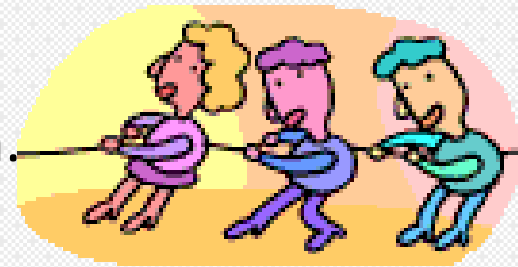
Can any Information be Withheld?

Main Exemptions.

- Information which may cause harm to the physical or mental health of pupil or other individual.
- Disclosure would reveal a child at risk of abuse.
- Information contained in adoption and parental records.
- Information given to a court in proceedings under the Magistrates Courts (Criminal Justice) (Children) Rules NI 1995.
- Copies of examination scripts and providing exam marks before they are officially announced.

Information Given in Confidence

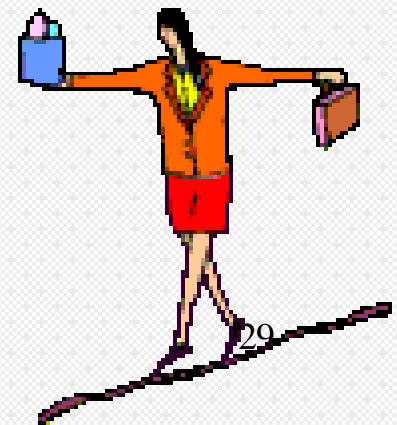
- Was the information given in circumstances that gave rise to the expectation of confidence? - in a one-to – one counselling session.
- Does the information have the quality of confidence? - would disclosure be a serious matter possibly naming bullies or abusers or is it trivial?
- Confidence can be overridden-child protection. Always seek advice before breaching confidence.
- Anyone with *parental responsibility can access. - popular pastime for non-custodial parent in dispute with custodial parent to ask for records?
- * See DE circular1999/17



Data Protection V Privacy

Generally, DPA does not prevent sharing with other professionals if:

- Subject gives consent.
- Public interest to safeguard child overrides the need to keep data confidential.
- Disclosure is required under court or other legal obligations.



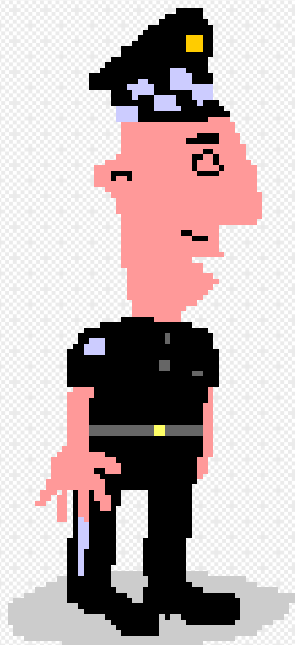
Data Sharing- a Problem?

- “Can’t do that because of Data Protection”- DPA perceived as overly restrictive.
- DPA seen to hamper crime prevention-public protection.
- Stops sensible use of personal information-even if in public interest.
- Results in lack of public trust.
- Collected/held with the best of motives.
- Elements of DPA not understood/used properly.
- Positive elements of DPA not appreciated.
- Role of consent/choice misunderstood.



Good practice to inform parent about how the information you collect will be used.

What if a Police Officer asks for information?



Form 81

Signed by rank of
inspector or above.

Covers you for releasing
information to a police officer.



Making Northern Ireland Safer For Everyone Through Professional, Progressive Policing

REQUEST FOR DISCLOSURE OF PERSONAL DATA

To _____
(Note 1)

(1) The following request is required to assist in enquiries which are concerned with; and are for the purpose of:

- (a) **Data Protection Act 1998 – Section 28(1) National Security Exemption** (Note 2)
- (b) **Data Protection Act 1998 – Section 29(3) Crime Exemption**
- (i) the prevention or detection of crime, and/or
- (ii) the apprehension or prosecution of offenders
- (c) **Data Protection Act 1998 – (Miscellaneous)** – the information is required urgently in the vital interests of an individual and disclosure is urgently required for preventing injury or other damage to the health of any person(s)

(2) Please provide information concerning the following individual

(Note 3)

(3) I require the following information

(Note 4)

(4)* The information is required for the following investigation

(Note 5)

***Where details are not supplied, this form must be signed by an officer not below the rank of Superintendent.**

and the information required relates to service/case reference number _____ (Note 6)

(5) I have reasonable grounds for believing that failure to disclose this information will be likely to prejudice those matters and confirm that it will not be used in any way incompatible with the purpose for which it is being disclosed. I understand that if any information on this form is omitted or wrong, I may be committing an offence under Section 55 of the Data Protection Act 1998.

Investigating Officer (Name) _____ Rank/Number _____

Signature _____ Station and Tel No _____

Authorising Officer (Name) _____ Rank/Number _____

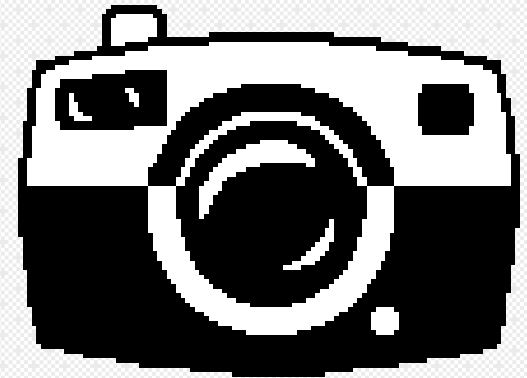
Signature _____

This application must be authorised by an officer senior to the requesting officer and of the rank of Inspector or above.

IN ORDER TO MAINTAIN POLICE CONFIDENTIALITY THIS REQUEST SHOULD BE TREATED IN CONFIDENCE

Snap away at School Events

- The Data Protection Act does not prevent parents taking photographs of their children and friends taking part in school events.
- Good Practice Guidance for schools is published on ICO Web site at www.ico.gov.uk



Basic Principles to Follow

- Treat personal data with care.
- Must be a good reason to hold and process data. Make sure data is accurate.
- Ensure consent has been provided, unless not required.
- If in doubt do not disclose , always ask for advice. Better to ask than get things wrong.
- Telephone enquiries-make sure you have a policy on releasing information that your staff know about. Do not release information verbally unless you are sure of the identity and the purpose the information is being used for.
- Keep notes of what has been disclosed and to whom. Never give out information about another person i.e. home address to friends or relatives of an employee/pupil.

Basic Principles to follow

- Do not be bullied into giving information.
- Can you legally withhold information- remember the data subject has rights.
- If handling sensitive data- think- Is releasing it by post/fax/ e-mail really a secure format? Could applicant collect it in person?
- 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- section 55 of DPA refers.
- The IC web site offers readily accessible guidance on all aspects of data protection. <http://www.ico.gov.uk/>
- General guidance is published on TEACHERS section of belb web site. Contact Liz Johnston 9056 4316.

Subject access
request

Train
Staff

Legally- can you
deny access

Data Subject
has rights



DPA-
40 Days to respond

THANK YOU

Valid written
request

Information
Security

Accurate
Data

Personal
Information

Data Controller

Good reason to
hold information