

# The Data Protection Act 1998 and the Freedom of Information Act 2000

Tony Brett  
IT Support Staff Services  
OUCS



# Overview

- General overview of the DPA 1998
  - Definitions
  - Changes since 1984 Act
  - Sensitive Personal Data & Consent
  - The eight principles
  - Transitional Relief
  - Implications for Colleges and Departments
  - Things to keep in mind
- Freedom of Information Act 2000
  - Who it affects
  - Public Rights
  - Publication Schemes
  - Exemptions
  - Key Points
- Resources

# What is the Data Protection Act?

- Intended to balance interests of data subjects with data controllers.
- Freedom to process data vs. privacy of individuals.
- 1984 act was repealed by the 1998 act.
- 24 October 1998.
- 1 March 2000.



# Definitions


- **Personal Data**
  - Expression of opinion, or fact, E-mail address, photos, video footage etc. etc.
  - Some types are *sensitive* (a special new category).
- **Processing**
  - Reviewing, holding, sorting, deleting
- **Data Controller**
  - all of us! Users of data
- **Relevant Filing System**
  - Readily accessible information about living individuals
- **Information Commissioner**
  - New name for Data Protection Registrar

# Changes Since the 1984 Act

- Much broader than the old act.
- More rights for data subjects.
- Covers relevant manual filing systems.
- New category of data – sensitive data.
- Transitional relief – 23 October 2001, for existing automated data and 23 October 2007 for manual records.
  - Processing must have been in effect before 24 October 1998.
- Rules about export of data to non-EEA countries.



# Some Effects on Colleges and Departments

- Data subjects are students, staff, alumni, suppliers (sole traders or partnerships), tenants, legal advisers, fellows etc.
  - Not people “acting in a capacity”.
  - Anyone can be a data controller
  - Dead people have no rights.
  - Overseas transfers of data – notably to U.S.
  - Requirement to ensure data is secure, accurate, sufficient but not excessive.
  - Can’t hold data longer than is reasonable.
- 

# Principles of the act – 1.

- Non-sensitive Personal data must be processed *fairly and lawfully* and shall not be processed unless one of the below is met (schedule 2).
  - Consent – *the most important*
  - Contract
  - Legal Obligation
  - Vital interests of subject (life or death!)
  - Public functions
  - Balance of interest

# Sensitive Personal Data

- Racial or ethnic origin
- Political opinions
- Religious/similar beliefs (note food!)
- Trade Union Membership
- Health
- Sexual Life
- Offences





# Sensitive Personal Data

- May only be held if one of the below is met:
  - Explicit and *informed* consent
  - Employment Law
  - Vital Interests of Subject
  - Legal Proceedings
  - Medical Purposes (by medical professionals)
  - Equal opportunities monitoring



# Consent

- “Freely given specific and *informed* indication of wishes by which the data subject signifies agreement to personal data relating to him/her being processed.”
- Can't use implied consent – must get forms back.
- Can't use blanket consent as condition of entry.



# Fair processing

- Must not intentionally or otherwise deceive or mislead subject as to purpose of data use/collection.
- Must identify to subject data controller/nominated representative.
- Must identify to subject purpose of processing data.
- Exceptions are disproportionate effort (direct marketing not allowed) or legal obligation.



# Principles of the act – 2.

- Data must be obtained only for one or more specified lawful purposes.
  - Must not use data for a new incompatible purpose without subject's consent.
  - Have a data protection statement explaining what data will be held and why and get consent from new students/staff as they arrive.
  - Old members data is a grey area for Colleges.



# Principles of the act – 3 & 4.

- Personal data must be adequate, relevant and not excessive.
  - Must not stock up on data without a reason that can be justified – consent!
- Personal data shall be accurate and up-to-date.
  - This is an ongoing requirement and means data needs to be kept under constant review.



# Principles of the act – 5.

- Personal data may not be kept for any longer than is necessary for its stated purpose(s).
  - This potentially creates a problem with old staff/members data. Development offices beware!
  - Consent from all new staff/members to keep their data after they have left as this is a different purpose to keeping it while they are here.




# Principles of the act – 6.

- Personal data must be processed in accordance with the rights of data subjects
  - This means that you cannot do things that violate the rights given to data subjects under the new act, especially denying access to data.



# Rights of data subjects

- Must be informed if personal data are being processed and given a description of the personal data and for what purpose it is being held.
  - May prevent processing for purposes of direct marketing.
  - Right to see algorithms used in automated decision making (credit scoring etc.).
  - Compensation, rectification, blocking, destruction.
- 



# Access rights

- Right to have communicated to him/her in an intelligible form the information constituting the data.
- No right to rifle through filing systems, computers etc.
- Right to be informed of logic involved in automated processing.
- Request must be in writing, fee up to £10 may be charged and identity may be thoroughly checked.



# Access rights – 2.

- Data may be withheld if disclosure would disclose data about a third party unless:
  - Third party has consented to disclosure
  - It is reasonable to comply without the third party's consent.
- Duty of confidentiality, steps taken to seek consent, express refusal of third party.
- Witnesses, confidential reports, access to references .

# Access rights – 3.

- Don't have to disclose references you have written but must disclose those you have received unless the writer explicitly asked them to keep confidential.
- 40 days to comply (or state reason for refusal to comply) with requests.
- Don't need to comply with repeat requests until a reasonable amount of time has elapsed.
- Don't need to comply if disproportionate effort would be involved.
- Subject must provide reasonable data you request to assist in finding the data.

# Enforced Access

- It is an offence to force subjects to exercise their access rights to data held by others
  - Includes data about cautions, criminal convictions and certain social security records



# Right to prevent processing


- Unwarranted substantial damage or distress to subject.
- 21 days to comply with request.
- Exemption if processing is necessary for performance of contract with subject or there is a legal obligation, or the vital interests of the subject are at stake.



# Exemptions to access rights

- Prevention and detection of crime
- Apprehension or prosecution of offenders
- Collection of tax or other duty
- Research, history, statistics.
- Exam marks – 40 days after date of announcement or 5 months of access request.
- Confidential references.

# Principles of the act – 7.

- Technical or organisational measures must be taken to prevent unauthorised or unlawful processing of data and accidental loss, damage or destruction of data.
    - First is related to IT support staff (backups, password security etc.) but everyone can help.
    - Second is about being careful with keys, having access controls, CCTV monitoring etc.
    - Beware social engineering!
- 

# Principles of the act – 8.

- Personal data may not be transferred overseas unless the receiving country has an adequate level of protection for it.
  - US does not.
  - Putting things on a web site is tantamount to export of data.
- Transfer is OK if contract is in place with the abroad party or the subject has consented.
  - Data Protection Commissioner is preparing standard contracts.





# Notification

- Colleges are legally separate entities to The University so has to notify use to commissioner separately. Departments are not.
  - This is like the old registration process under the old act.
  - University counts as a third party in the case of Colleges.
- Penalties for failure to comply/notify are huge.
- Commissioner has draconian powers (search & seize).



# The Freedom of Information Act 2000

- The FOI act 2000 gives individuals the right to access information about certain public bodies (including HE institutions) by two routes:
  - Publication Scheme
  - General Right of Access
- There are exemptions
- FOI basically extends subject access rights given in the DPA 1998
- Colleges are separate legal entities so need their own Publication Scheme and procedures



# FOI – Public Rights

- To be told whether the information exists – known as the duty to confirm or deny
- To receive the information (and, where possible, in the manner requested)
- To receive reasons for a decision to withhold information
- All requests must be in “permanent form”
  - E-mail, Letter, Fax
- Reply must be sent within 20 working days
  - Use vacation auto-reply for contact person if they are away



# FOI – Publication Scheme

- Guide to the information which you have decided to make public
  - Chance to be proactive so people don't have to make requests
  - Guide to types of information available NOT a list of all of it!
- Scheme has to be approved by Information Commissioner
- Model schemes available on Information Commissioner's web site
- JISC has model schemes available too
- Put it on your College website! Some already have



# FOI – Exemptions

- Many exemptions, some absolute, some qualified e.g.
  - Commercial Interest
  - Communicating with the Queen
  - Law enforcement
  - Legal Professional Privilege
  - Parliamentary Privilege
- Need to Apply Tests before using Qualified Exemptions
  - Prejudice & Adverse Affect
  - Public Interest (not same as of Interest to the Public)
- FOI does not override DPA but DPA is not an excuse not to comply with FOI requests
  - Interaction is complex!

# FOI – Vexatious or Repeated

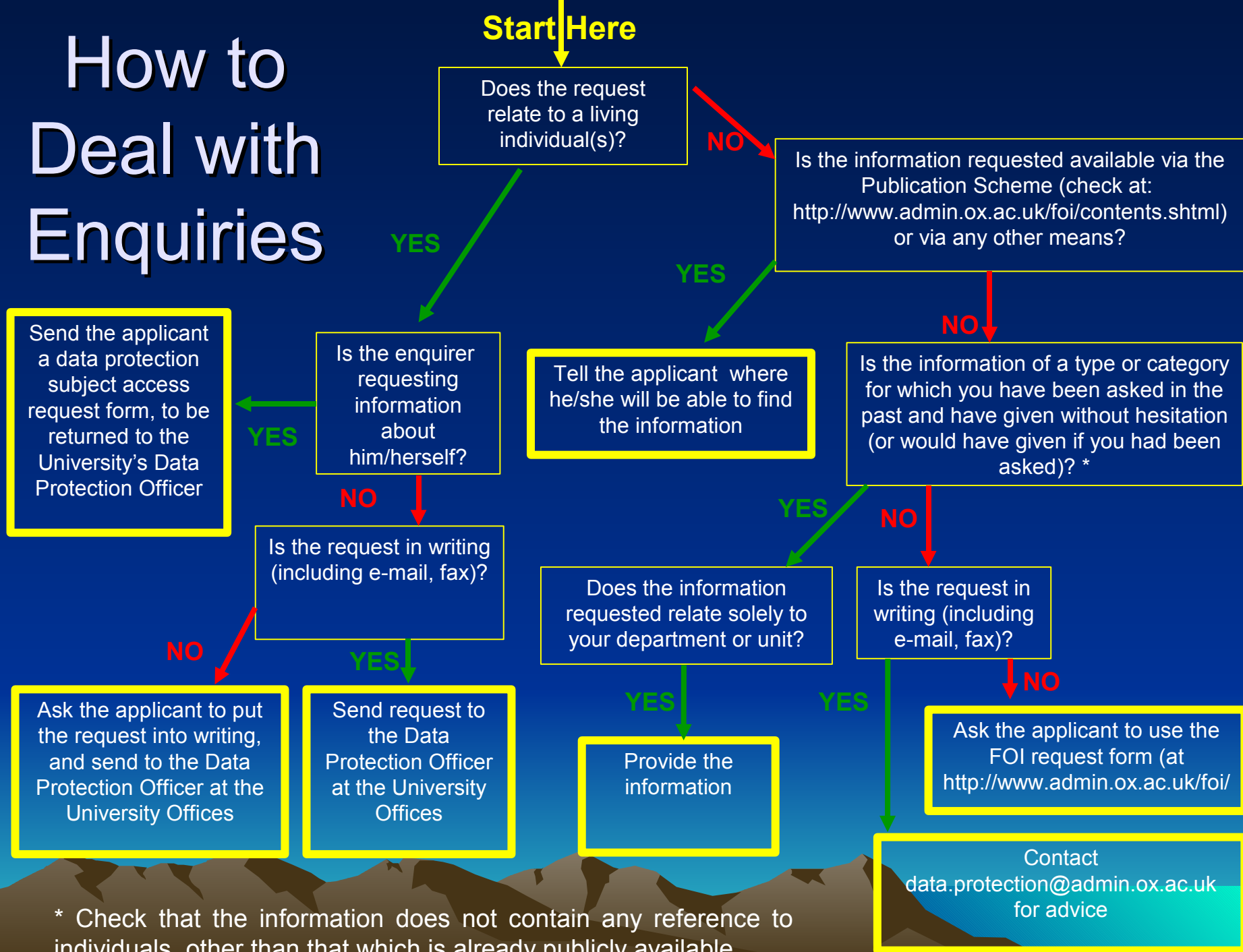
- **Vexatious means:**
  - clearly does not have any serious purpose or value
  - is designed to cause disruption or annoyance
  - has the effect of harassing the public authority
  - can otherwise fairly be characterised as obsessive or manifestly unreasonable.
- **Repeated means:**
  - More often than a “reasonable interval”
    - Needs defining
  - Requests asking if previously requested information has changed are OK
    - Reply can say when info is next to be updated and a request before then would be “repeated”

# FOI - Key points to note

- Requests can be received by anyone within the organisation and do not need to refer to the Freedom of Information Act
- Requests must be in writing (including e-mail, fax etc)
- Requests must be dealt within 20 working days
- No obligation to provide information which is already in the public domain/accessible by other means (e.g. via the publication scheme or in a book the organisation may hold)
- No obligation to create information that the Organisation does not already hold (e.g. statistical summaries)
- Organisation may charge a fee for the provision of information.
  - Charges must be calculated in accordance with the fees regulations prescribed by the Department for Constitutional Affairs. Currently £50 maximum.



# How to Deal with Enquiries



\* Check that the information does not contain any reference to individuals, other than that which is already publicly available



# FOI & DPA - Key Points

- Don't panic!
- Need to be seen to be aware of both FOI and DPA and working within them but the Information Commissioner will always try to help before getting heavy.
- Have a publication scheme and publish it!
- Little or no case law yet – many grey areas, but we don't want to be the test case!
- Don't write down anything you wouldn't say to someone's face.
- Avoid holding sensitive personal data if you can.
- Colleges need to act additionally to Central University

# Resources

- <http://www.informationcommissioner.gov.uk/>
- <http://www.admin.ox.ac.uk/councilsec/oxonly/dp/>
- <http://www.admin.ox.ac.uk/foi/>
- <http://users.ox.ac.uk/~tony/dpa-foi.ppt>
- [http://www.jisc.ac.uk/index.cfm?name=pub\\_ibsm\\_foi](http://www.jisc.ac.uk/index.cfm?name=pub_ibsm_foi)
- [information.officer@admin.ox.ac.uk](mailto:information.officer@admin.ox.ac.uk)
- [data.protection@admin.ox.ac.uk](mailto:data.protection@admin.ox.ac.uk)
- Conference of Colleges Legal Panel

Thanks to Sarah Cowburn at Admin for assistance and permission to use material

