Isolde Harpur

Unit 5
Ethics in Using Information
Data Protection
imharpur@tcd.ie
What is Data Protection?

Purpose – to safeguard the privacy rights of living individuals regarding the processing of their personal data by those who control those data.

Data Protection is overseen in Ireland by the Data Protection Commissioner.
What is the difference between FOI and DP?

According to the Data Protection Commissioner it is the following:

“The FOI Acts grant every person a right, subject to certain restrictions, to access information held by Government Departments, agencies and other designated bodies in receipt of State funding. The FOI Acts also allow for persons to seek access to their own data held by such bodies”

“The requirements of the Data Protection Acts apply to all legal entities in this jurisdiction whether Government, private, voluntary or charitable that control personal data”
Are you a data controller processing personal data?

“Data controller” means a person who, either alone or with others, controls the contents and use of personal data.

“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.

The legislation also defines ‘sensitive personal data’, which is a subset of personal data to which more restrictions apply (e.g. health data).
Are you a data controller processing personal data? (continued)

“Processing” means performing any operation or set of operations on the information or data, whether or not by automatic means, including:

a) obtaining, recording or keeping the information or data

b) collecting, organising, storing, altering or adapting the information or data

c) retrieving, consulting or using the information or data

d) disclosing the information or data by transmitting, disseminating or otherwise making it available

e) aligning, combining, blocking, erasing or destroying the information or data

‘processing’ covers doing practically anything imaginable with data
Are you processing sensitive personal data?

“Sensitive personal data” means personal data as to:

a) the racial or ethnic origin, the political opinions or the religious or philosophical beliefs of the data subject
b) whether the data subject is a member of a trade-union
c) the physical or mental health or condition or sexual life of the data subject
d) the commission or alleged commission of any offence by the data subject
e) any proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings
The Eight Rules of Data Protection

1. Obtain and process information fairly
2. Keep only for one or more specified, explicit and lawful purposes
3. Use and disclose it only in ways compatible with these purposes
4. Keep it safe and secure
5. Keep it accurate, complete and up-to-date
6. Ensure that it is adequate, relevant and not excessive
7. Retain it for no longer than is necessary for the purpose or purposes
8. Give a copy of his/her personal data to an individual, on request

Principle 1: Obtain and process information fairly

**Fair obtaining** – there are specific conditions for obtaining data. These include providing, at the time the data is obtained, the name of the data controller and representative where appropriate, the purpose of collection, any planned disclosures to others, provide all necessary information to ensure fairness, inform the data subject of their right to access and to rectify the data.

**Fair processing of personal data** – data subjects must have given their consent, or the processing must be necessary for one of a specified list of purposes.

**Fair processing of sensitive personal data** – data subjects must have given informed and explicit consent, or the processing must be necessary for a more restricted list of purposes.
Principle 2: Keep only for one or more specified, explicit and lawful purposes

Data may not normally be collected for one purpose and used for another. Remember the issue of consent.
Principle 3: Use and disclose it only in ways compatible with these purposes

Would the data subject be surprised to learn of a use or disclosure?

If there is someone processing personal data on your behalf then there must be a written contract in place to cover the data protection aspects of this
Principle 4: Keep it safe and secure

“appropriate security measures shall be taken against unauthorised access to, or unauthorised alteration, disclosure or destruction of, the data, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.” [DP Acts, section 2 (1) (d)]
Principle 5: Keep it accurate, complete and up-to-date

Procedures for data handling
Maintenance and review of data collected
Checks and audits of data
Principle 6: Ensure that it is adequate, relevant and not excessive

These criteria relate to fulfilling the purpose for which the data are gathered.

Data collected should be reviewed periodically in the light of this principle.
Principle 7: Retain it for no longer than is necessary for the purpose or purposes

Define retention periods for personal data
Establish procedures to implement these
Principle 8: Give a copy of his/her personal data to an individual, on request

Access requests under the Data Protection legislation
Put in place a procedure to enable an access request to be met without undue difficulty rather than be faced with a problem that could have been avoided by proper planning
Exporting personal data

Within the European Economic Area (EEA) [EU + Norway, Iceland and Liechtenstein]

Outside the EEA where there is not an approved level of data protection law

Role of consent of the data subjects to the export data
Data Protection and medical research

Medical research may involve sensitive personal data.

The Commissioner has issued ‘Data Protection Guidelines on Research in the Health Sector’ which is available on his website.

The Commissioner emphasises that the optimal approach is one of anonymising medical data prior to research processing.
Data Protection and medical research (continued)

His advice indicates best practice on processing personal data.
Any proposed health research should be carefully scrutinised from a data protection viewpoint well in advance of the proposed research.
All prospective work involving individual people as subjects must first be reviewed by the appropriate Faculty Research Ethics Committee in the university.
Data Protection

Introduction

Data Protection aims to protect individuals' right to privacy in regard to the processing of their personal data by those who control such data. The legislation governing this is the Data Protection Acts 1988 and 2003 which lay down rules about the safeguarding of the privacy of personal data, covering such areas as the obtaining, processing, keeping, use, disclosure, accuracy, appropriateness, retention and an individual's right to access and correct their personal data. The legislation applies to personal data held in both manual and electronic format. The Data Protection legislation is the transposition into Irish law of the relevant European Union directives.

The College information available includes its Data Protection policy, procedures and advice and also provides information on the College's Information Compliance Committee which oversees the implementation of the Data Protection Acts in Trinity.
Sources of further information

The Office of the Data Protection Commissioner
www.dataprotection.ie

The European Commission’s Data Protection website
http://ec.europa.eu/justice_home/fsj/privacy

Example of a university’s Data Protection website
www.tcd.ie/info_compliance/dp/