DATA PROTECTION ACT 2002
The Basics
Purpose of the Act

- Balance the rights of an individual with an organisation’s legitimate need to process personal data
- Promote openness and transparency
- Establish and maintain trust and confidence
- Promote good practice in the processing of information
- Prevent damage and distress caused by unlawful or unauthorised processing
The Jargon

- Data
- Personal data
- Processing
- Data Controller
- Data Subject
- Data Processor
- Data Protection Principles
The Jargon

‘Data’ means information which:

- is being processed or is intended to be processed by means of equipment operating automatically in response to instructions given for that purpose,
  - e.g. computer files & databases, email, video surveillance, audio recordings

- is recorded as part of a “relevant filing system” or with the intention that it should form part of a relevant filing system,
  - e.g. structured paper records, such as employee files

- is an “accessible record”;
  - i.e. health, education, social work and local authority housing records
‘Processing’ in relation to information or data, means

- obtaining,
- recording or holding the information or data, or
- carrying out any operation or set of operations on the information or data, including-
  - (a) organisation, adaptation or alteration of the information or data,
  - (b) retrieval, consultation or use of the information or data,
  - (c) disclosure of the information or data by transmission, dissemination or otherwise making available, or
  - (d) alignment, combination, blocking, erasure or destruction of the information or data
‘Relevant filing system’ means

any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.

For example, a relevant filing system may be structured A-Z or by cross-reference to an identification number from which the individual could be identified.

  e.g. account number, customer reference number or staff number
The Jargon

‘Sensitive personal data’ means personal data relating to:

- Racial or Ethnic Origin
- Political opinions
- Religious beliefs
- Trade Union membership
- Physical or mental health
- Sex life
- Offences or alleged offences
The Parties

- **Data subject**
  - The individual that the information relates to

- **Data controller**
  - The legal ‘person’ who determines how data will be processed

- **Data processor**
  - A third party who processes personal data on behalf of the data controller
Data Protection Principles

1. Fairly and lawfully processed
2. Used for specific purposes
3. Adequate, relevant and not excessive
4. Accurate and where necessary kept up to date
5. Kept for no longer than necessary
6. Used in accordance with the rights of individuals under the Act
7. Kept secure
8. **NOT** transferred to another country outside the EEA without adequate protection
The Data Protection Principles

First and Second Principles – The Transparency Principles

1. Fairly and lawfully processed

2. Used for specific purposes
The Data Protection Principles

First Principle: Fair and lawful processing

Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless —

(a) at least one of the conditions in Schedule 2 is met, and

(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
The Data Protection Principles

First Principle: Fair processing

You must state:

- Data Controller’s identity
- The purpose for which the data are intended to be processed
- In specific circumstances, any further information which is necessary to make the processing generally fair.

  e.g. if you are going to use personal data for direct marketing you must inform the data subject

Must NOT deceive or mislead
CORPORATE SERVICE PROVIDER

We are seeking a Manager to assist the Directors to continue the development and expansion of our business.

A business qualification would be an advantage but not essential for an applicant with a number of years experience.

Applications will be treated in the strictest confidence.

Full curriculum vitae with an indication of salary requirements is requested.

Please note that this is a strictly non-smoking office.

Please apply in writing to
Box No 1801
Isle of Man Newspapers
Peel Road
Douglas
Isle of Man IM1 5PZ
The Data Protection Principles

First Principle: conditions for processing

- The processing of personal data is **necessary**: for the performance of a contract with the individual; to comply with a legal obligation; to protect the vital interests of the individual; for the administration of justice, or the exercise of any statutory function; for the legitimate interests of the organisation, unless the interests of the individual would be prejudiced.

- Or is with the consent of the individual
  - (Schedule 2 of the Data Protection Act 2002)

- If **sensitive personal data** is processed a condition set out in Schedule 3 must also be met
The Data Protection Principles

Second Principle:
Purpose for which data are obtained and processed

Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.
The Data Protection Principles

Third, Fourth and Fifth Principles

3. Adequate, relevant and not excessive

4. Accurate and where necessary kept up to date

5. Kept for no longer than necessary
The Data Protection Principles

Third Principle – adequacy and relevance of data

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
Adequate, relevant and not excessive?

Extracted from an application form to use school facilities:

Discounts are available for voluntary groups involving children in full time education.

If you wish to apply for a discount, please complete the following and supply a full list of members including dates of birth for junior members.
The Data Protection Principles

Fourth Principle - accuracy of data

Personal data shall be accurate and, where necessary, kept up to date.
The Data Protection Principles

Fourth Principle - accuracy of data

Isle of Man

A copy of a medical file was posted to the patient addressed to

“E Smith”

The letter was opened by Emma, who found the contents disturbing as she was unaware that her mother, Elizabeth, had mental health problems, or had threatened to commit suicide on several occasions.
The Data Protection Principles

Fifth Principle – time for keeping data

Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
The Data Protection Principles

Fifth Principle – time for keeping data
The Data Protection Principles

Fifth Principle – time for keeping data

- The Act does not specify any retention periods

- Retention periods will vary depending on:
  - Legal requirements for keeping data
  - Industry best practice
  - Ongoing investigations/litigation

- “Just in case” is not a reason to retain personal data after it is no longer required for the specified purpose(s)
The Data Protection Principles

Fifth Principle – time for keeping data

- Information is expensive to keep
- Brings legal liability
- Record and information management policies assist in complying with the fifth principle
The Data Protection Principles

Sixth Principle: rights of data subjects

Personal data shall be processed in accordance with the rights of data subjects under this Act.
The Data Protection Principles

Sixth Principle: rights of data subjects

- Right of access to personal information
- Right to prevent processing likely to cause damage or distress
- Right to prevent processing for the purposes of direct marketing
- Right in relation to automated decision making
- Right to seek compensation for any damage or distress caused by the failure of a Data Controller to comply with the requirements of the Act
- Right to take action to rectify, block, erase or destroy inaccurate data
The Data Protection Principles

Seventh Principle: measures against misuse and loss of data

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
The Data Protection Principles

Seventh Principle: measures against misuse and loss of data

- Adherence to Information Security policies?
- Are staff properly trained and aware of their responsibilities?
- Is access to the information properly controlled and auditable?
- Do procedures exist for detecting breaches?
Case Study – INFORMATION SECURITY

The Department of Social Care and Praxis Care Limited have signed undertakings as a result of the loss in August 2011 of an unencrypted memory stick containing the personal data, and in some cases the sensitive personal data, of 160 individuals.
The Data Protection Principles

Eighth Principle: transfer of data abroad

Personal data shall not be transferred to a country or territory outside the Island 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.
The exemptions

The rights and duties set out in the Act are designed to apply generally, but there are some exemptions from the Act to accommodate special circumstances.

The Act does not provide any blanket exemptions, but in certain specific circumstances it provides exemptions from the requirement to:
- grant subject access to personal data; and/or
- give privacy notices; and/or
- not disclose personal data to third parties.
The exemptions

The main exemptions are set out in Part 4 of, and Schedule 7 to, the Act and include:

- National Security
- Crime and Taxation
- Health, education and social work
- Regulatory activity
- Journalism, literature and art
- Research, history and statistics
- Public information
- Legal proceedings
- Tynwald privilege
- Domestic purposes

The application of an exemption must be considered on a case-by-case basis because the exemptions only permit you to depart from the Act’s general requirements to the minimum extent necessary.

It is not mandatory to apply any exemption – it is the choice of the Data Controller.
Resources

Information Commissioner
- www.inforights.im
- ask@inforights.im

UK Information Commissioner
- www.ico.org.uk

GOV.UK - Data protection and your business
- www.gov.uk/data-protection-your-business

Chartered Institute of Personnel and Development
- www.cipd.co.uk