DATA PROTECTION ACTS 1988 AND 2003

Data Protection Guidelines

1. Purpose of these Guidelines

The purpose of these Guidelines and Procedures is to assist staff in supporting the Department's **Data Protection Policy**, which affirms its commitment to protect the privacy rights of individuals in accordance with the legislation. These Guidelines should be read in conjunction with the Department's **Acceptable Use Policy** and the **Email and Internet Policy**.

2. What are the Data Protection Acts, 1988 and 2003?

The Data Protection Acts 1988 and 2003 are designed to protect an individual's privacy. The Acts confer rights on individuals in relation to the privacy of their personal data as well as responsibilities on those persons holding and processing such data. In particular, they provide for the collection and use of data in a responsible way, while providing protection against unwanted or harmful uses of the data.

All staff should familiarise themselves with the provisions of the Acts. Further information is available on the website of the Office of the Data Protection Commissioner **www.dataprotection.ie**

3. Department's Obligations

There are Eight Rules of Data Protection which govern the processing of personal data:-

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

These provisions apply to **ALL** personal data held. Personal data means data relating to a person who is or can be identified either from the data itself or in conjunction with other information that is in, or is likely to come into, the possession of the Department. It covers any information that relates to an identifiable, living individual. This data can be held on computers or in manual files.

The Acts also provide that a "duty of care" is owed to **data subjects,** which means that those controlling or processing the data should take care that their activities do not cause damage or distress to the people concerned by, for example, maintaining inaccurate information on our files, or disclosing personal data to someone who is not entitled to this data.

The Department holds data to administer its functions. Staff are provided with access to that data in order to do their jobs. **Under no circumstances should data be accessed without a direct business requirement. Confidential customer information must never be discussed with or disclosed to any unauthorised third party, either internal or external.**

4. Application of the Rules of Data Protection

In order to ensure the Department's compliance with the Rules of Data Protection, the following procedures must be observed at all times:

- **Rules 1, 2 and 6 (obtaining and processing all personal data fairly)**

  Personal data is obtained fairly if the data subject is aware of the purpose for which the Department is collecting the data at the point of collection and of the categories of person/organisation to whom it may be disclosed. This is a normal part of the claim registration and maintenance function and is noted on Departmental application forms. Investigating Officers also make this clear during the course of any enquiries. **Obtain personal data only when there is a clear purpose for doing so, obtain only that which is necessary for fulfilling that purpose and ensure that it is used only for that purpose.**

- **Rule 3. (disclosing personal data)**

  Personal data should only be disclosed in ways that are necessary or compatible with the purpose for which it is held. **Do not disclose any personal data to any third party without the consent of the data subject** (see exceptions below). Personal data should not be disclosed to work colleagues unless they have a legitimate interest in the data in order to fulfil official duties.

Permitted disclosures of personal data

Personal data **can** be disclosed without the express written consent of the data subject in the following circumstances:-

- ✓ to the data subject or to a person acting on his/her behalf:
- ✓ at the request or with the consent of the data subject or a person acting on his/her behalf;
- ✓ where the data subject has already been made aware of the person/organisations to whom the data may be disclosed;
- ✓ required by law or a court order;
- ✓ required for legal advice or legal proceedings, where the person making the disclosure is a party or witness ;
- ✓ required for the purposes of preventing, detecting or investigating offences, apprehending or prosecuting offenders, or assessing moneys due to the State, a local authority or a health board;
- ✓ authorised for safeguarding the security of the State (if it is in the opinion of a member of the Garda Siochana not below the rank of chief superintendent or an officer of the Permanent Defence Forces not below the rank of colonel);
- ✓ required urgently to prevent injury or damage to health or serious loss of or damage to property;
- ✓ required to protect the international relations of the State.

Further detailed guidelines will issue on the procedures to be followed in relation to the disclosure of personal data to authorised third parties.

NOTE: Apart from receiving a query from the data subject or a person acting on his/her behalf, if you receive a request for information required for any of these reasons you should pass it on to your supervisor/manager. If the supervisor/manager

has any doubt about the query s/he should contact Business Information Security Unit (BISU).

- **Rule 4. (securing personal data)**
  The Department must protect personal data from unauthorised access when in use and in storage and must protect it from inadvertent destruction, amendment, loss, disclosure, corruption or unlawful processing.

  - ✓ Personal electronic data should be subject to appropriate stringent controls, such as passwords, access logs, back-ups etc,
  - ✓ Screens, print-outs, documents and files showing personal data should not be visible to unauthorised persons,
  - ✓ Personal manual data should be held securely in locked cabinets, locked rooms, or rooms with limited access,
  - ✓ Special care must be taken where mobile computing and storage devices, such as laptops, are used. **Further Guidelines will issue in respect of mobile devices**.
  - ✓ The Department, as a Data Controller, in disclosing personal data to a Data Processor (e.g. a Branch Office) should only do so under a written agreement, specifying the security arrangements which must be in place.

- **Rule 5. (accuracy and completeness of personal data)**
  Data subjects have a responsibility to advise the Department of any errors or changes to data. Once informed, it is imperative that the data be amended accordingly.

- **Rule 7. (retention and disposal of personal data)**
  Data should not be kept for any longer than is necessary for the purpose for which it was collected and should not be subject to further processing that is not compatible with that purpose.

  Personal data should be disposed of **securely** when no longer required. The method should be appropriate to the sensitivity of the data. Shredding or incineration is appropriate in respect of manual data; and reformatting or overwriting in the case of electronic data. Particular care should be taken when PCs or laptops are transferred from one person to another within the Department, or outside the Department, or when being disposed of. **Further detailed guidelines will issue in respect of appropriate retention and disposal procedures**.

- **Rule 8. (rights of data subjects)**
  The DP Acts provide for the right of access by the data subject to his or her personal information. **Subject Access Requests are dealt with by Data Access Section.** Accordingly, if you receive a request of this nature you should send it to **Data Access Section, Shannon Lodge, Carrick-on-Shannon, for immediate action.**

5. Responsibilities of data subjects

All staff, customers and other data subjects are entitled to be informed how to keep their personal information up-to-date. All staff, customers and other data subjects are responsible for:

- ✓ checking that any information that they provide to the Department is accurate and up-to-date;

- ✓ informing the Department of any errors or changes to details that they have provided, e.g. change of address;

6. Implementation of Data Protection Guidelines

The Department takes its Data Protection obligations very seriously. All staff and third parties who are authorised to have access to personal data held by the Department must ensure that they are familiar with and adhere to these Guidelines.

7. Breaches of Data Protection

The Department will investigate all allegations of suspected breaches of data protection. All complaints, from whatever source (e.g. the data subject, staff, management, etc.), should be forwarded to line management who must immediately notify the Head of Information Security (PO, Risk Management Division) who is responsible for the co-ordination of investigations across the Department.

Any breach of trust with regard to the confidentiality of personal data will be treated as serious misconduct under the Disciplinary Code and comes under immediate consideration for dismissal.

8. Further Information

If you have any queries or require clarification on any aspect of these procedures and guidelines, please contact the Business Information Security Unit (BISU), Risk Management Division, Goldsmith House. All contact with the Data Protection Commissioner's Office should also be channelled through this section. BISU may be contacted at extension 42784.

Extensive information is available from the Data Protection Commissioner's website (www.dataprotection.ie).