DATA PROTECTION AND CONFIDENTIALITY POLICY

1.0 Purpose of policy

The purpose of this Data Protection and Confidentiality policy is to inform employees of their rights and obligations under Data Protection and to provide employees with an understanding of confidentiality and clear guidelines regarding handling of confidential information.

2.0 Introduction and purpose

This policy applies to the employees of the company, including temporary and fixed term employees and contractors who are subjects of this data or who process any personal data. Employees have obligations as a user of personal data (e.g. on a customer) as an employee of the Company. The Data Protection Acts gives individuals (employees and customers) certain rights regarding information held about them. It places obligations on those who process information while giving rights to those who are the subject of that data. Personal information covers both facts and opinions about an individual.

It is crucial that all staff understands the reasons for processing personal information. This policy will describe the purpose of obtaining sensitive information from service users, the principles to follow to safe-keep the information provided in confidence, circumstances when this information may need to be shared, disclosed or accessed and will signpost staff to relevant procedures.

The company is required to register with the Data Commissioner as a Data Controller under the Data Protection Acts. The entry on the Register specifies the purpose, description, individuals and bodies information is disclosed to and details on any transfer of information abroad. If employees handle personal data in any way, they should take as much care as possible that they are operating according to the practices registered by the Company.

3.0 Definitions

"**Confidential Information**" – refers to any information, material or data that the organisation considers and treats as confidential, sensitive or proprietary, and is not in the public realm through due process of the company, shall be defined as confidential, whether or not it is explicitly marked as such.

Examples of Confidential Activities & Sources: Information that is confidential, sensitive or proprietary may result from various activities and sources. These may include but are not limited to:

1. Current and prospective customer data (e.g quotation or premium details, claims information etc.), including sensitive information on medical conditions and criminal convictions.
2. Employee personnel matters and actions, including personnel records with responsibilities, qualifications and compensation information as well as medical records or data that will be unduly invasive of personal privacy
3. Information generated by self-regulatory proceedings, such as ethics and professional conduct investigations, certification, standards-setting, accreditation or other business or governance enforcement.
4. Opinions and other privileged information received from inside or outside legal counsel or other learned experts, including staff
5. Monthly financial statements and quarterly executive financial summaries.
6. Certain business and financial discussions, agreements, and financial data. This includes multi-year program plans and budgets, information about programs, projects, intellectual property

rights, business processes, marketing procedures, products and services under development as well as data generated through confidential merger or acquisition processes, or other cooperative or partnership agreements
7. Trade secrets or confidential commercial information generated through the corporation's business endeavours, or shared with the corporation by outside business concerns on the condition of maintenance of confidentiality
8. Programs, products, and services being developed but not yet made public.

"**Data**" – Data means information that is being processed automatically or is recorded with the intention that it should be processed automatically. Any manual data that forms part of a relevant filing system is also included in this definition.
"**Personal Data**" – Personal Data is data relating to a living individual (not a company) who can be identified either from the data or from the data in conjunction with other information in the possession of the Data Controller. The Company holds Personal Data on both employees and customers and this policy relates to both categories. Examples of Personal Data could include Address, Bank Account details, Insurance Information etc.
"**Data Subject**" – The Data Subject is the individual to whom the personal data pertains.
"**Data Controller**" – The Data Controller is a person who controls the contents and use of personal data.
"**Data Processor**" – The Data Processor is an external person who processes personal data on behalf of the Data Controller. The employees of the Data Controller who processes personal data in the course of their employment are not data processors.
"**Relevant filing system**" – This is a file or system which has a structure or index that enables the retrieval of specific information about an identifiable individual. Manual files only fall under the Acts if they are of sufficient sophistication to provide the same or similar ready accessibility as a computerised filing system.

4.0 Employee rights

Under the Acts, employees have rights because they are the subject of personal data held or processed by the company, including:

- To be informed if personal data is held concerning yourself.
- Access at reasonable intervals to any personal data held concerning yourself.
- If such data is inaccurate to have the data corrected or erased.

5.0 Purpose(s) for which the company processes data

The company processes personal data relating to its employees for the purposes of employment including performance monitoring, measurement and complaint investigation. Personal data may include employee HR records, the monitoring and recording of telephone calls for training and quality purposes and the monitoring of email and internet usage. Some areas of company premises are covered by CCTV cameras for security purposes.

The company processes personal data relating to customers in the management and administration of insurance, including underwriting, claims handling, and statistical analysis. Personal data may also be processed where this is required by law.

6.0 Data Protection principles

The company will administer its responsibilities under the Data Protection Acts in accordance with the eight stated data protection principles as follows:

1. Obtain and process information fairly
We will obtain and process personal data fairly and in accordance with the fulfilment of its functions

2. Keep it only for one or more specified and lawful purposes
The company will keep data for purposes that are specific, lawful and clearly stated on the Register held by the Data Protection Commissioner and the data will only be processed in a manner compatible with these purposes.
3. Use it and disclose it only in ways compatible with these purposes
The company will only disclose personal data that is necessary for the purposes or compatible with the purposes for which it collects and keeps the data.
4. Keep it accurate and up-to-date
The company have clerical and computer procedures that are adequate to ensure high levels of data accuracy. Policyholders are responsible to keep us informed. Employees should ensure that they inform the company of any changes to the personal data they have provided e.g. change of address.
5. Ensure that it is adequate, relevant and not excessive
All information collected is necessary for the purposes outlined in register. Information is collected for administration of policy including underwriting, claims handling and statistical analysis.
6. Retain it for no longer than is necessary for the purpose for which it was created
A document Retention Strategy has been agreed by the Heads of Department, which is compliant with all relevant legislation and is aligned to business requirements.
7. Ensure that the data is secure against unauthorised access, alteration, disclosure or destruction
We take our security responsibilities seriously, employing the most appropriate physical and technical measures, including staff training and awareness. We review our security measures and procedures regularly
8. Give a copy of his/her personal data to that individual, on request
The company have a Data Protection client requests procedure in place to ensure data subjects can exercise their rights under the Data Protection Acts. (See the **Subject Access Request procedure** for further details).

Any breach of the Data Protection and confidentiality Policy, whether deliberate, or through negligence may lead to disciplinary action being taken or even a criminal prosecution, so all employees need to be aware of the provisions under the Acts. If in doubt, consult your Team Leader, Supervisor, Manager or the HR department.

7.0 Consent to process data

Where the company collects sensitive data including data relating to medical conditions or criminal convictions, the policyholder must give their explicit consent to the collection and processing of this information.

8.0 Direct marketing

Customers are given the opportunity to update their marketing preferences on the website, telephony and documentation. There are two marketing questions on the IT systems which you should tick if a customer wishes to receive marketing information.

9.0 Data security

All employees are responsible for ensuring that:

- Any personal data they hold, whether in electronic or paper format, is kept securely.
- Personal information is not disclosed deliberately or accidentally either orally or in writing to any unauthorised third party.

Place any papers with Personal Data in the shredding bins located beside the printers/photocopiers. Do not use the waste bins for disposal of Personal Data. Also you must collect customer information from the printer as quickly as possible (i.e. Certificates, Proposals, etc…). Do not leave personal data on your desk and keep work documents in work. All pedestals are lockable. Clear your desk at the end of each day and observe the **Tidy desk policy**.

If information is deliberately manipulated or altered you are in serious breach of the Acts. Divulging passwords or discussing cases or customers is a serious breach of the Acts. You should always lock your PC when you leave your desk unattended. Observe the **IT security** and **laptop policy**.

10.0 Training

All employees must attend the compulsory induction training when they start their employment with the company. Data Protection refresher training is also delivered at regular intervals. In the event that you have not attended an induction you must inform your line manager immediately.

11.0 Subject access requests

Policyholders have the right to access any personal data that is being kept about them either on computer or in structured and accessible manual files. Any person may exercise this right by submitting a request in writing to the Customer Services Manager. The company reserve the right to charge £10 (UK policyholders) or €6.35 (ROI policyholders) for each official Subject Access Request under the Acts.

Comments and notes on Notepad should be complete, accurate and as factual as possible. A customer has the right to see all of this information if requested.

12.0 Confidentiality and Disclosure Responsibilities

The company is responsible for ensuring that all employees involved in dealing with confidential information receive appropriate training, supervision and support regarding the policy and their legal responsibilities.

Employees are required to act in accordance with this policy, failure to do so will may be considered as an act of gross misconduct and may result in disciplinary action up to and including dismissal. General responsibilities of employees include but are not limited to:

1. To notify management if the employee detects any improper usage, modification or disclosure of any private or personal information.
2. Not to access any confidential information without the express authorisation of management. An employee should only have access to confidential information on a strictly "need to know basis".
3. Employees are strictly prohibited from viewing or making amendments to their own policies or claims, or policies or claims belonging to other customers that they are connected to e.g. a relative or friend.
4. Not to disclose any trade secrets or other information of a confidential nature relating to the company or any of its businesses or in respect of which the company owes an obligation of confidence to any third party during or as required by a lawful authority. Specifically you should:
   (a) Confirm the identity of who you are speaking to before disclosing personal details
   (b) Don't discuss policy or payment details with anyone except the policy holder
   (c) Don't disclose details about third parties to the policy holder

(d) Information requests from Garda Síochána and Police Service should be in writing (See **Garda/Police Referrals Procedure** for further information).

5. Not remove, reproduce or transfer any documents, computer disks, tapes or any other means of recording data or any confidential information at any time without proper authorisation. All such documents, disks tapes and any other copies are property of the company.
6. Following termination of employment (howsoever caused) you will not discuss the business of the company, its subsidiaries or associated companies with any competitor or interested person.
7. On termination of employment of your employment, (howsoever caused), all books, documents, customer lists, samples and other documentation or items including notes prepared in the course of your employment shall be returned by you to the company and no copies of such documentation or items shall be retained by you.

If you are in any doubt with regards your responsibilities under confidentiality, consult your Team Leader, Supervisor, Manager or the HR department immediately.

13.0 Wrongful disclosure

Wrongful disclosure can occur in at least two ways. It can be by either act or omission. The first would be where confidential information is deliberately passed on to a third party. The second would be where confidential information is disclosed to a third party through negligence. Wrongful disclosure will be considered as an act of gross misconduct and will result in disciplinary action

14.0 Limits to confidentiality

In exceptional circumstances the organisation may need to break confidentiality for example when it is required to be disclosed to a court of law, regulatory authority or tribunal of competent jurisdiction. In as far as is possible, in such cases, a full explanation will be given regarding the necessary procedures that may need to be taken.

15.0 Penalties

Any breach of the Data Protection Policy or Confidentiality Policy, whether deliberate, or through negligence may lead to disciplinary action being taken or even a criminal prosecution, so all employees need to be aware of the provisions under the Acts. If in doubt, consult your Team Leader, Supervisor, Manager or the HR department.

16.0 Review

This Policy will be reviewed regularly in light of any legislative or other relevant developments.

Relevant regulation and legislation

Industry Code of Practice on Data Protection for the Insurance Sector [ROI]
Data Protection Act, 1988 [ROI]
Data Protection (Amendment) Act 2003 [ROI]
Data Protection Act, 1998 [UK]