GDPR -Data protection Policy and Procedures

General Data Protection Regulation (GDPR) came into force across the EU on 25 May 2018, replacing the current data protection framework in Ireland. The Company is committed to complying with its legal obligations in this regard. The Company collects and processes personal data relating to its employees in the course of business *i.e.* recruitment, training, remuneration. They also give individuals certain rights in relation to personal data that is held about them.

This policy covers any individual about whom the Company processes data; this may include current and former employees and customers. It applies to information held manually (*i.e.* in documents on an employee's personal file). Processing of data includes collecting, recording, storing, altering, disclosing, destroying and blocking.

It is important you read this policy to ensure that you are aware of the nature of the information that the Company holds, and the reasons why we need to process this information.

What is Personal Data?
Personal data is data relating to a living individual who is or can be identified either from the data or in conjunction with other information that is in, or is likely to come into, the possession of the Company.

Examples of personal data held on the records in the possession of the Company may include: an employee's address, age, contact details, bank details, position, medical details, performance reviews etc. CCTV images are also a form of personal data. In some cases, Managers may also hold employee information in their own files.

Certain personal data is likely to be considered as "sensitive personal data". This is personal data relating to a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health, sexual, criminal convictions or proceedings and requires higher levels of protection.

The Company will also hold in its records personal data, including sensitive personal data, relating to customers.

Data Quality Principles

The Company will ensure that all personal information will be processed in accordance with the principles of data protection as outlined in the GDPR; we will ensure that it is:

- obtained and processed fairly
- used and disclosed only for specified, explicit and legitimate purposes

- adequate, relevant and not excessive
- accurate, up-to-date and complete
- retained only for as long as required to complete the purpose specified
- kept safe and secure
- not further processed in a manner incompatible with the purposes for which it was obtained
- Not transferred outside the European Economic Area without adequate levels of data protection.

Personal information is normally obtained directly from the employee concerned. In certain circumstances, it will however be necessary to obtain information from a third party *i.e.* references from previous employers.

Security and disclosure of information

The Company will take all reasonable steps to ensure that appropriate security measures are in place to protect the confidentiality of both electronic and manual information in accordance with GDPR and current Irish Legislation. Security measures will be reviewed from time to time. You must implement all Company policies and procedures *i.e.* use of computer passwords, locking filing cabinets etc. You may have access to a certain amount of personal information relating to colleagues, customers and other third parties. You must play your part in ensuring its confidentiality.

- You must adhere to the data protection principles and must not disclose such information except where necessary in the course of your employment, or in accordance with law
- You must not remove or destroy personal information except for lawful reasons

If you are in any doubt regarding your obligations you should contact your Manager. Any breach of the data protection principles is a serious matter and may lead to disciplinary action up to and including dismissal.

Medical Information

Where the Company carries out pre-employment medicals as part of the recruitment process this information will be retained by the Company. Occasionally it may be necessary to refer employees to the Company doctor for a medical opinion and you are required by your contract of employment to attend in this case. The Company will receive a copy of the medical report, which will be stored in a secure manner with the utmost regard for confidentiality. The Company will not retain medical reports on job applicants who do not become employees for longer than is necessary

Employees are entitled to request access to their medical reports. Should you wish to do so, please contact your Manager who will consult with the Doctor who examined you and request the information. The final decision lies with the

Doctor in accordance with Statutory Instrument No 82 of 1989. Employees are required to submit medical certificates in accordance with the sick absence and sick leave policy. These will be stored by your Manager having the utmost regard for their confidentiality.

Interview Records

The Company will retain records of interview notes, application forms etc. in order to ensure compliance with the Employment Equality Acts 1998 and 2004 and with the Equal Opportunities Policy for a period of 12 months.

CCTV

The use of CCTV is necessary in order to protect against theft and pilferage, for the security of staff, customers and Company property. Access to the recorded material will be strictly limited to authorised personnel.

Processing employee information

The Company is required to collect and use personal data (including sensitive personal data) about employees for a variety of personnel, administration and general business management purposes. These include administration of the payroll system, administration of employee benefits (such as pension schemes), carrying out appraisals, performance and salary reviews, operating and checking compliance with your employer's rules and policies, operating your employer's IT and communications systems and checking for unauthorised use of those systems and to comply with record-keeping and other legal obligations.

The Company may transfer some or all of the personal data about employees held on its records to any third party with which your employer is at any time in advanced negotiations regarding the sale of your employer's business.

Transfer of Employee Information

The Company may make some information about employees available to its advisers and/or data processors such as lawyers, accountants, payroll administrators, benefits providers (for example, pension scheme providers), to those providing products or services to the Company (such as IT and other outsourcing providers) and to government and/or regulatory authorities. These recipients may be located outside the European Economic Area. In this case, the Company will, as far as is possible, ensure that the recipients of the information, both within and outside your employer's business, comply with the principles set out in this policy.

Employees' Rights under the GDPR and current Irish Legislation

A person is entitled to:

Both the current Irish legislation and the GDPR provide you with a right to see a copy of any personal data held by the company about you. If you believe the company is processing personal data about you, you can request that they tell you whether they are processing this data. If your data is being processed you will be able to request a copy of that data to be sent to you. The company will be able to charge a reasonable administrative fee for this. Under the current legislation, the fee cannot be more than €6.35.

You are entitled to the following information:

- The purposes of the processing
- The categories of data being held
- The identity of any recipients who may see this data
- The period for which it will be stored
- Your right to lodge a complaint with a supervisory authority
- Where the information was not collected from you, information about the source
- The use of any automated decision-making processing and information about that process
- If the data is being transferred to a country outside the EU, the data safeguards in that country

Both the current Irish legislation and the GDPR provide you with the right to request the company to rectify inaccurate or incomplete personal data they hold about you.

You currently have a right to restrict the company from processing your personal data where:

- The accuracy of the data is in question
- The processing of the data is unlawful
- The company no longer needs the data for the original purpose but it is required by you for other reasons
- You have challenged the legal basis for the processing

Once the processing has been restricted, the controller must inform you before lifting that restriction.

Under the GDPR you have a strengthened right of *erasure*. You can request the company to erase your data and the company has an obligation to erase your data if one of the following applies:

- The data is no longer needed for the purpose it was collected
- You have withdrawn your consent to the processing of your data
- You object to the processing of your data
- There is no lawful basis for the processing
- The data must be erased to comply with law
- The data was collected in relation to an offer of online services

The right of erasure also includes the right to have publicly available personal data erased or as far as technologically possible, removed from public availability.

The GDPR introduces the right to *data portability*. This means that you can request and receive personal data that you have previously provided to the

company in a commonly used and machine-readable format. The right also means that you can request one controller to transfer your personal data to another controller.

You have the right to object to the processing of your data at any time - for example, to prevent your data being used for marketing purposes, including profiling. The company will stop processing your data unless you can show that there are legitimate grounds or legal reasons for such processing that override your interests.

Access requests

Requests for access to the personal data that the Company holds about you must be made in writing to the Manager. A charge of €6.35 per access request will be levied to cover administration costs. The Manager will reply to the access request as soon as possible and in any event, within 28 days.

There are a number of circumstances where the right of access will not apply, and these include:

- where personal data is kept for the purpose of preventing, detecting or investigating offences and related matters; and
- Where the data is an expression of opinion about an employee given by another person in confidence and it was given on the understanding it would be treated confidentially *i.e.* in certain circumstances, a reference given by a previous employer.

If you receive a request from someone to give them any personal data about an employee (or other individual) you should refer them to the Manager. The Company needs to verify the identity of the person making such a request and has to balance various considerations when deciding whether and how to respond to such request. It is therefore important to refer such requests to the Manager so that it can ensure compliance with data protection obligations.

Accessing, disclosing or otherwise using employee records or other employee personal data without authority will be treated as a serious disciplinary offence and may result in disciplinary action up to and including dismissal.

If an employee is unsure about the application of these guidelines to the information he/she holds as part of his/her job, he/she should contact the Manager for further guidance.

Data Protection – Customers

Customer/Client Information

All customer/client information held on the Company's systems is confidential such as home address, telephone numbers, credit card numbers, bank account details, medical history, medical condition, prescription details, doctors, etc. The Company and its employees must comply with the Data Quality Principles and all other data protection obligations in respect of this client/customer information. The guidelines in respect of processing of an employee's personal data as outlined above will also apply to data held in respect of clients/customers.

If a customer/client requests information, you must:

- ensure that the customer/client makes a formal written request detailing the information sought;
- explain to the customer/client that they may be charged a fee of up to €6.35 for the supply of the information requested;
- On receipt of the written request, immediately refer the request to your Manager who has responsibility for monitoring compliance with the Data Protection legislation in relation to customers/clients.
- Never disclose any information or personal data in relation to any customer or client to a third party under any circumstances.
- Always establish the identity of the person asking for the information by carrying out standard checks on the date of birth and address details *i.e.* ask to see a driver's licence or other form of identification. The person making the request must confirm these details to the employee, not the other way around and you should make and keep a copy of the identification.

An employee cannot take instructions from someone else to alter the details held on our systems.

A customer/client has a right to make an access request for all data records held on paper as well as on computer files, so employees must always ensure that any notes or expressions of opinions that they make on customer files are factual and not offensive or defamatory.

Roles and Responsibilities

Employees

- Familiarise yourself with the content of this policy procedure and adhere to the conditions set out in this policy
- Adhere to the data quality principles outlines in this policy
- Inform your Manager of any changes to your personal circumstances *i.e.* Change in address