

General Data protection Regulations

The purpose of this policy is to ensure that Employees understand why we need personal details and to be assured of how their personal information is used within the Company. Equally so it is to assure Clients of their right to privacy and the way in which we handle and store their data.

Act: The Data Protection Act is superseded by the General Data Protection Regulations (GDPR) on 25 May 2018. The new regulations control how your personal information is used by organisations, businesses or the government.

It is our policy that everyone who is responsible for using data has to follow strict rules called 'data protection principles'. They must make sure the information is:

- used fairly and lawfully
- used for limited, specifically stated purposes
- used in a way that is adequate, relevant and not excessive
- accurate
- kept for no longer than is absolutely necessary
- handled according to people's data protection rights
- kept safe and secure
- not transferred outside the UK without adequate protection
- The organisation will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure.

There is stronger legal protection for more sensitive information, such as

- ethnic background
- political opinions
- religious beliefs
- health
- sexual health
- criminal records

Procedure

- All new starts are required to fill in a personal details form, Bank details form, medical conditions form, and various other forms as required for our system.
- All information will be scanned to a **Password protected** digital file held in the individual's name.
- Hard Copy forms will be filed in folder held in individuals name and stored in **the locked** Personnel Filing Cabinet
- Personal Details and Bank Details will be scanned to the Payroll Department and to the person responsible for compiling wage data
- Details will not be given out to anyone unless we are bound by law to do so.

Individual rights

Right to be informed	Right of access	Right to rectification
Right to erasure	Right to restrict processing	Right to data portability
Right to object	Rights related to automated decision making including profiling	

Please read following Guidance Notes :

**The Data Protection Act applies to all organisations processing personal data.
Updated to The General Data Protection Regulations (GDPR) – May 2018**

Data Protection Policy, including Key Procedures

Aims of this Policy - This section explains:

- why data protection is important to your organisation
- the legal basis for the policy
- general aim of this policy
- who in the organisation needs to comply with this policy and key procedures

This policy covers all employees and LOCs

To meet our responsibilities we will

- Ensure any personal data is collected in a fair and lawful way;
- Explain why it is needed at the start;
- Ensure that only the minimum amount of information needed is collected and used;
- Ensure the information used is up to date and accurate;
- Review the length of time information is held;
- Ensure it is kept safely;
- Ensure the rights people have in relation to their personal data can be exercised

Find out what the GDPR has about you

The Data Protection Act gives you the right to find out what information the government and other organisations stores about you.

Write to the organisation and ask for a copy of the information they hold about you. If you do not know who in the organisation to write to, address your letter to the Company Secretary.

The organisation is legally required to provide you with a copy of the information they hold about you if you request it.

When information can be withheld

There are some situations when organisations are allowed to withhold information, they don't have to say why they are withholding information. It could be to do with:

- the prevention, detection or investigation of a crime
- national security or the armed forces
- the assessment or collection of tax
- judicial or ministerial appointments

Interface Environment Management processes the following personal information

- name, address, date of birth, NI number, next of kin, existing medical conditions convictions
- Personal information is kept in the following way; Hard Copy in locked personnel file and **password protected** Digital copy on Server.
- Groups of people within the organisation who will process personal information are: ***Personnel Manager and Area Managers, Directors.***

All **authorised personnel** who process personal information must ensure they not only understand but also act in line with this policy and the data protection principles.

Data Controller in Interface Environment Management Ltd is responsible for:

- understanding and communicating obligations under the Act
- identifying potential problem areas or risks
- producing clear and effective procedures
- notifying and annually renewing notification to the Information Commissioner, plus notifying of any relevant interim changes

We will ensure that:

- Everyone managing and handling personal information is trained to do so.
- Anyone wanting to make enquiries about handling personal information, whether a member of staff, volunteer or service user, knows what to do;
- Any disclosure of personal data will be in line with our procedures.
- Queries about handling personal information will be dealt with swiftly and politely.

Breach of this policy will result in a disciplinary hearing

The DPA covers manual data as well as electronic if it is:

- A set of information relating to individuals which is not processed on a computer
- A set of information held in a 'relevant filing system'
- A filing system with a structuring/ indexing mechanism that gives easy access to personal information

This could include information held on computers, fax machines, microfiche, paper in filing cabinets, on desks, paper in archives, index cards etc.

The Personal Data Guardianship Code

In line with the Data Protection Act 1998 principles, Interface Environment Management Ltd will ensure that personal data will:

- Be obtained fairly and lawfully and shall not be *processed unless certain conditions are met
- Be obtained for a specific and lawful purpose
- Be adequate, relevant but not excessive
- Be accurate and kept up to date
- Not be held longer than necessary
- Be processed in accordance with the rights of data subjects
- Be subject to appropriate security measures
- Not to be transferred outside the European Economic Area (EEA)

(*The definition of 'Processing' is obtaining, using, holding, amending, disclosing, destroying and deleting personal data. This includes some paper based personal data as well as that kept on computer.)

The organisation will seek to abide by the following five key principles of good data governance and good practice.

- **Accountability:** those handling personal data follow publicised data principles to help gain public trust and safeguard personal data.
- **Visibility:** Data subjects should have access to the information about themselves that an organisation holds. This includes the right to have incorrect personal data corrected and to know who has had access to this data.
- **Consent:** The collection and use of personal data must be fair and lawful and in accordance with the DPA's eight data protection principles. Personal data should only be used for the purposes agreed by the data subject. If personal data is to be shared with a third party or used for another purpose, the data subject's consent should be explicitly obtained.
- **Access:** Everyone should have the right to know the roles and groups of people within an organisation who have access to their personal data and who has used this data.
- **Stewardship:** Those collecting personal data have a duty of care to protect this data throughout the data life span.

Anyone whose personal information we process has the right to know:

- What information we hold and process on them
- How to gain access to this information
- How to keep it up to date
- What we are doing to comply with the Act.a

They also have the right to prevent processing of their personal data in some circumstances and the right to correct, rectify, block or erase information regarded as wrong.

Individuals have a right under the Act to access certain personal data being kept about them on computer and certain files. Any person wishing to exercise this right should apply in writing to (insert name of person within the organisation or title and contact details).

GDPR and the Client

How will we use your information?

To manage your account and Process your orders or instructions

Who will we share your information with?

We will not share your information for marketing purposes with any other Companies outwith Interface Environment Management Ltd

Privacy Statement for Clients

- **What information do we collect from you?** Company name, Registration number, address, telephone number and contact person's name and any other contact details deemed necessary
- **Why do we collect this his information?** To effectively manage your accounts, process orders, make deliveries, carry put your instructions.
- **How do we store your information?** Your information will be stored in a password protected electronic file
- **Will we share it with others?** No we will not share your information with other companies for marketing purposes, only for the legitimate management of your account with us.
- **How long do we keep your information?** for the duration of the contract plus 3 years after termination of contract
- **How you can access the information we keep on you?** by applying to the Data Controller of this Company
- **Will we share it with others?** No we will not share your information with other companies for marketing purposes, only for the legitimate management of your account with us. We will however share your personal information with any law enforcement agency who has a legislative right to obtain such information.

Privacy Statement for Staff

- **What personal information do we collect from you?** Name, address, telephone number, date of birth; next of kin for emergency contact, medical history, bank details
- **Why do we collect this his information?** To effectively manage the payment of your wages and all aspects of your employment with this Company
- **How do we store your information?** Your information will be stored in a password protected electronic file and in hard copy format stored in a locked cabinet
- **How long do we keep your information:** for the duration of your employment with us plus 3 months thereafter.
- **Will we share it with others?** We will only share your personal information with any law enforcement agency who has a legislative right to obtain such information
- **Can you access the information we keep on you?** Yes by applying to the Data Controller of this Company