**

Data Protection Policy

# 

|  |  |  |  |
| --- | --- | --- | --- |
| Version History | | | |
| Version No | Version Date | Author | Summary of Changes |
| 1.0 | 26/05/2020 | IMcG | First Issue |
| 1.1 | 11/05/2022 | IMcG | UK GDPR |
|  |  |  |  |

|  |  |  |
| --- | --- | --- |
| Approvals | | |
| Name | Title | Date of Approval |
| Matt Harper | ICT Director | 26/05/2020 |
| Matt Harper | ICT Director | 11/05/2022 |
|  |  |  |

|  |  |  |
| --- | --- | --- |
| Distribution | | |
| Audience | Date of Issue | Version Number |
| Public | 26/05/2020 | 1.0 |
| Public | 11/05/2022 | 1.1 |

Table of Contents

1. Purpose
2. Scope
3. Definitions
4. Data Controller
5. Disclosure
6. Data Collection
7. Data Storage
8. Data Access and Accuracy
9. Retention and Disposal of Information
10. Data Breach
11. Personal Information Request

#### **1.0 Purpose**

The Erith Group needs to collect and use certain types of information about the customers that we deliver products and services to and the Erith Group Employees. This personal information must be collected and dealt with appropriately whether it is collected on paper, stored on our servers, collected by email, stored on phones, or recorded on other material and there are safeguards to ensure this under the UK Data Protection Act 2018 and the General Data Protection Regulations.

**2.0 Scope**  
This policy covers all personal information stored by the Erith Group on customers and employees of the Group.

#### **3.0 Definitions** ‘The Erith Group’ is a collection of companies that lie under the Erith umbrella. All these companies are referred to as the Erith Group. For the purposes of this document the companies within the Erith Group are; Erith Contractors Ltd, Erith Haulage Company Ltd, Erith Business Solutions Ltd, Erith Training Services Ltd, Swanton Consulting Ltd and Erith Plant Services Ltd.

UK GDPR – The UK General Data Protection Regulation is a legal framework that sets guidelines for the collection and processing of personal information from individuals. It was taken and used in the UK as part of Brexit.

DPO – A Data Protection Officer is an enterprise security leadership role required by the UK General Data Protection Regulation. Data protection officers are responsible for overseeing a company's data protection strategy and its implementation to ensure compliance with GDPR requirements.

Information Commissioner – The Information Commissioner's Office (ICO) is responsible for enforcing the data protection legislation in the UK. They have the power to carry out investigations and issue fines, and advise businesses on how to comply with the GDPR.

**4.0 Data Protection Officer**

Vicky Stokes is designated as the Erith Group’s Data Protection Officer, which means that she determines what purposes personal information held, will be used for in line with GDPR. She is also responsible for notifying the Information Commissioner of the data it holds or is likely to hold, and the general purposes that this data will be used for.

**5.0 Disclosure**

The Erith Group will not share information with any other companies or agencies unless legally bound to do so. If Information is shared for any reason, the Employee/Customer will be made aware of how and with whom their information will be shared.

There are circumstances where the law allows The Erith Group to disclose data (including sensitive data) without the data subject’s consent, these are:

* Carrying out a legal duty or as authorised by the Secretary of State
* Protecting vital interests of an Employee / Customer or other person
* The Employee / Customer has already made the information public
* Conducting any legal proceedings, obtaining legal advice or defending any legal rights
* Monitoring for equal opportunities purposes – i.e. race, disability or religion
* Providing a confidential service where the Employee’s / Customer’s consent cannot be obtained or where it is reasonable to proceed without consent: e.g. where we would wish to avoid forcing stressed or ill Employee’s / Customer’s to provide consent signatures.

The Erith Group regards the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those we work with. The Erith Group intends to ensure that personal information is treated lawfully and correctly. The Erith Group adhere to the Principles of Data Protection, as detailed in the General Data Protection Regulations, specifically, the principles require that personal information:

* Shall be processed fairly and lawfully and shall not be processed unless specific conditions are met.
* Shall be obtained only for one or more of the purposes specified in the Regulations, and shall not be processed in any manner incompatible with that purpose or those purposes.
* Shall be adequate, relevant and not excessive in relation to those purpose(s).
* Shall be accurate and, where necessary, kept up to date.
* Shall not be kept for longer than is necessary.
* Shall be processed in accordance with the rights of data subjects under the Act.
* Shall be kept secure by the Data Controller who takes appropriate technical and other measures to prevent unauthorized or unlawful processing or accidental loss or destruction of, or damage to, personal information.
* Shall not be transferred to a country or territory outside the European economic area unless that country or territory ensures an adequate level of protection for the rights and freedoms of Employee’s/Customers’ in relation to the processing of personal information.

The Erith Group will, through appropriate management and strict application of criteria and

controls**:**

* Observe fully conditions regarding the fair collection and use of information.
* Meet its legal obligations to specify the purposes for which information is used.
* Collect and process appropriate information, and only to the extent that it is needed to fulfil its operational needs or to comply with any legal requirements.
* Ensure the quality of information used.
* Ensure that the rights of people about whom information is held, can be fully exercised under the Regulations. These include:
* The right to be informed that processing is being undertaken.
* The right of access to one’s personal information.
* The right to prevent processing in certain circumstances
* The right to correct, rectify, block or erase information which is regarded as wrong information.
* Take appropriate technical and organisational security measures to safeguard personal information.
* Ensure that personal information is not transferred abroad without suitable safeguards.
* Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information.
* Set out clear procedures for responding to requests for information

**6.0 Data Collection**

Data Collected by the Erith Group for the most part is collected under the lawful basis of having a contract in place i.e. an employment contract is in place or an order has been placed to progress with works. Where a contract is not in place the lawful basis will be consent, which is received in an appropriate manner with an Employee / Customer clearly understanding why their information is needed, who it will be shared with, the possible consequences of them agreeing or refusing the proposed use of the data.

The Erith Group will ensure that data is collected within the boundaries defined in this policy. This applies to data that is collected in person, or by completing a form. When collecting data, The Erith Group will ensure that the Employee / Customer:

* Clearly understands why the information is needed.
* Understands what it will be used for and what the consequences are should the Employee / Customer decide not to give consent to processing.
* As far as reasonably possible, grants explicit consent, either written or verbal for data to be processed.
* Is, as far as reasonably practicable, competent enough to give consent and has given so freely without any duress.
* Has received sufficient information on why their data is needed and how it will be used.

**7.0 Data Storage**

Information and records relating to Customers and Employees will be stored securely and will only be accessible to authorised staff. Information will be stored for only as long as it is needed or required statute and will be disposed of appropriately. It is The Erith Group’s responsibility to ensure all personal and company data is nonrecoverable from any computer system previously used within the organisation, Please review the Erith Groups WEEE policy, *8.3.2.1 ICT - WEEE Waste Policy*.

1. **Data Access and Accuracy**

All Employees / Customers have the right to access the information The Erith Group holds about them. The Erith Group will also take reasonable steps ensure that this information is kept up to date by asking data subjects whether there have been any changes at appropriate review dates. In addition**,** The Erith Group will ensure that:

* It has a Data Controller with specific responsibility for ensuring compliance with Data Protection.
* Everyone processing personal information understands that they are contractually responsible for following good data protection practice.
* Everyone processing personal information is appropriately trained to do so.
* Everyone processing personal information is appropriately supervised.
* Anybody wanting to make enquiries about handling personal information knows what to do.
* It deals promptly and courteously with any enquiries about handling personal information.
* It describes clearly how it handles personal information.
* It will regularly review and audits the ways it holds, manages, the use of personal information.
* It regularly assesses and evaluates its methods and performance in relation to handling personal information.
* All staff are aware that a breach of the rules and procedures identified in this policy may lead to disciplinary action being taken against them.

**9.0 Retention and Disposal of Information**

**Retention**

Records should be kept for as long as they are needed to meet the operational and legal needs of the Erith Group in accordance with the legal and regulatory requirements, more information on this can be found in the Classification of Information policy, *8.2.1 ICT - Classification of Information*. We have assessed our records to:

* Determine their value as a source of information about the Erith Group, its operations, relationships and environment.
* Determine their value as a source of valuable information regarding customers, their conditions and treatments.
* Assess their importance as evidence of business activities and decisions.
* Establish whether there are any legal or regulatory retention requirements.

**Disposal**

Personal records will be destroyed as set out in the policy above after an agreed period or kept for no longer than is necessary. Please review the Classification of Information policy - *8.2.1 ICT - Classification of Information* for more detail into the Destruction of records.

**Document Deletion / Disposal**

A record / log of deletions and disposals must be maintained within the Document Deletion Log – *18.1.4 Document Deletion Log*. This

Will include: -

* The details of the record.
* The type of record
* The retention period
* The reason for deletion / disposal
* The method of deletion / disposal
* The person responsible for the deletion / disposal

**10.0 Data Breach**

In the event of a data breach by loss of data, whether in hard copy or electronic copy

or malware on an Erith Group asset that causes loss or unauthorised access to data the Erith Group will firstly address the physical breach by shutting down systems and processes to ensure the data breach does not continue.

The Erith Group will then fully investigate the breach to determine why and how this happened and put in place measures to prevent the re-occurrence of the breach. We will then determine the classification of the data as per the classification of Information policy - *8.2.1 ICT - Classification of Information*. If the breach contains data that is classed as reportable, then The Erith Group will notify the ICO and the victim of the data breach (the person or company that the data pertains to) within 72 hours of the data breach. The Data breach will be processed through the Erith Group ICT Information Security Incident Management channel and logged within *A.16 Information Security Incident Report.*

**11.0 Personal Information Request**

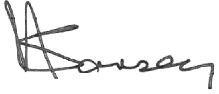
The Erith Group will provide all information pertaining to an employee or customer to the

employee or customer that the information pertains to within one month of receipt of the

request. These requests must be sent to the [Helpdesk@erith.com](mailto:Helpdesk@erith.com) for processing. The Erith Group will then either provide the information in hard copy format or emailed as a password protected zip file where appropriate. The information will be encrypted as appropriate to the data requested. Where the request comes from a person who is no longer employees or customers of The Erith Group, we will provide information in the same manner as detailed above within one month. This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the UK GDPR or UK Data Protection Act 2018. In case of any queries or questions in relation to this policy please contact Vicky Stokes at The Erith Group.

Signed for and on behalf of

The Erith Group



Steven Darsey

Chairman