Applicable from 25th May 2018

**13.9 Data Protection**

**13.9.1 Introduction**

This Data Protection Policy applies to all current, former and prospective directors, employees, workers, agents and contractors (including, for the avoidance of doubt, self-employed consultants) working with or for Plastica Ltd. Throughout this policy we refer to employees. In the context of this policy only the phrase “employee” should be taken to include directors, employees, workers, agents and contractors (including, for the avoidance of doubt, self-employed consultants) but does not imply nor should be assumed to imply or create any specific relationship between any person to whom this policy applies and Plastica Ltd.

This policy does not form part of an employee’s contract of employment and may be amended at any time.

In the course of your work, you may come into contact with and use confidential personal information about other employees, clients, customers, suppliers, agents, contractors and other people, such as their names, email addresses and home addresses. This Policy helps you to ensure that you do not breach the General Data Protection Regulations. The regulations provide strict rules governing the collection, retention, storage, use and disclosure of personal information. Information protected by the Regulations includes not only personal data held on computer but also certain manual records that form part of a structured filing system. If you are in any doubt about what you can or cannot disclose and to whom, do not disclose the personal information until you have sought further advice from your Manager. It is a criminal offence to knowingly or recklessly disclose personal data in breach of the Regulations and any such action could also result in significant fines for the Company, as well as irreparable damage to the Company’s reputation. Accessing another employee’s personal records without authority is a disciplinary offence and may amount to potential gross misconduct.

We hold personal data about you and will process this data in accordance with your rights under the Regulations.

Under the Regulations we are required to provide you with information regarding our status as a data controller and who you can contact with any queries or concerns you may have regarding how we are obtaining and handling your data. This information is outlined below:

Data Controller: Plastica Ltd, Perimeter House, Napier Road, Castleham Industrial Estate, St Leonards on Sea, East Sussex, TN38 9NY.

Data Protection Officer: Daniel Sawyer, Plastica Ltd, Perimeter House, Napier Road, Castleham Industrial Estate, St Leonards on Sea, East Sussex, TN38 9NY, [dan@plasticapools.net](mailto:dan@plasticapools.net).

* + 1. **The Data Protection Principles**

The Regulations requires that personal data must be:

* Processed lawfully, fairly and in a transparent manner in relation to individuals;
* Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
* Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
* Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
* Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
* Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

We are committed to following these principles and will be open and transparent about what the data will be used for. We will process personal data about you only as far as is necessary for the purpose of managing the Company’s business in which you are employed. Unless you expressly authorise its disclosure, your personal data will not be disclosed to anyone else other than authorised employees, those who provide relevant products to the Company (such as advisers, payroll and pension administrators), regulatory authorities, potential or future employers, governmental or quasi-governmental organisations and potential purchasers of the Company or of that part of the business in which you work. We will only obtain personal data about you that we require for the purpose of managing our business and dealing with you as an employee of that business. If you have any concerns regarding the way in which we are handling or processing your personal data, including whether you believe that we have obtained personal data regarding you that we do not need, please discuss this with your Manager who will ensure that any such queries are dealt with in an appropriate manner. If it is determined that we are holding personal data about you that we do not require, we will ensure that such data is deleted without delay.

The categories and source of the personal data we hold about you can be found in the Company’s Data Retention Policy, a copy of which has been provided to you in this Handbook and can be obtained upon request or from the Company’s Intranet.

We will take all reasonable steps to ensure that the personal data we process is accurate and not excessive. Personal data will be retained as necessary during the course of your employment and records will be retained for up to seven years after you leave the Company’s employment in case legal proceedings arise during that period. Different categories of data may be retained for different periods of time depending on legal, operational, regulatory and financial requirements. Data will only be retained for a period of longer than seven years if it is material to ongoing legal proceedings or it should otherwise be retained in the interests of the Company or for regulatory reasons after that period (for example, relating to a company pension scheme or employee benefit scheme).

Manual personal data, such as personnel files, is stored in filing cabinets in a locked room (room is locked in the absence of the HR Officer) and is only accessible by certain authorised persons. Personal data held on computer is stored confidentially by means of password protection. We have a network of back-up procedures to ensure that data on computers cannot accidently be lost or destroyed.

**13.9.3 Lawful Reasons for Processing**

As your employer we hold a variety of information about you in our systems. This data includes but is not limited to your name and address, salary details, bank details, date of birth, age, sex, next of kin, sickness records, medical reports and details of criminal convictions. This information will only be used in order that we can monitor our compliance with the law and best practice in areas such as recruitment, equal opportunity, pay and benefits, administration, performance appraisal and disciplinary matters. If your personal information changes, you should let us know so that our records can be updated. In any event, we will conduct an annual data accuracy review with you to ensure the data is accurate and up to date.

It is a requirement under the Regulations that we have a lawful reason for processing personal data about you. The lawful reasons for processing are as follows:

* Consent – where the data subject has given us explicit, informed and unambiguous consent to process their data.
* Contractual Obligations – where we are required to process personal data pursuant to a contractual obligation we have with the data subject.
* Legal Obligations – where we are required to process personal data pursuant to a legal obligation we have to a third party or the data subject.
* Vital Interests – where we have to process personal data in situations where it is necessary to do so to protect the data subject’s vital interests (including health and wellbeing).
* Public Task – where we process personal data to allow us to perform a task that is in the public’s interest.
* Legitimate Interests – where we wish to process your personal data and doing so is in our, or a third party’s legitimate interest.

As an employee we have a variety of legal obligations to you, as well as to a variety of government organisations (such as HMRC for example) and we are required to process certain personal data to ensure we comply with these obligations. We are, therefore, processing our employees’ personal data using the lawful bases of ‘Contractual Obligations’ and ‘Legal Obligations’ and, on occasion, ‘Legitimate Interests’.

In addition, some data is referred to in the Regulations as ‘sensitive’ personal data. This means personal data comprising information relating to:

* Race or ethnic origin.
* Political opinions.
* Trade Union membership.
* Religious or other beliefs.
* Physical or mental health or condition.
* Sexual life.
* Genetic or biometric data
* Criminal offences both committed and alleged.

In some circumstances, we may have to hold, and process, sensitive personal data about you. This will be, for example, information about your physical or mental health in order to monitor sick leave and take decisions about your fitness for work and your racial or ethnic origin, or religious or similar beliefs, in order to monitor compliance with equal opportunities legislation.

In addition, there may be situations where we process information relating to your criminal record. This may include, for example, undertaking criminal records and/or DBS checks against potential employees and/or keeping on our files information relating to certain criminal convictions of employees whilst in our employment.

In both of these circumstances the lawful basis for processing is slightly different. When processing this ‘sensitive’ personal data, including criminal record information, we will rely upon the lawful bases of ‘Consent’ (only for medical information that you voluntarily provide to us), ‘Legal Obligations’ and ‘Vital Interests’. No matter what kind of personal data we hold about you (whether sensitive or otherwise) we will only hold the minimum amount of data that we require to comply with our obligations and it will only be retained for as long as it is required to enable us to comply with our legal obligations. After this time it will be permanently deleted. All data is retained in accordance with our Data Retention Policy, a copy of which has been provided to you in this Handbook and can be obtained upon request or from the Company’s Intranet.

Finally, there may be situations where we have to pass certain personal data regarding our employees to third parties. This may include, for example, passing information to our professional advisers to enable them to best advise us in relation to a specific matter. In such circumstances, we will only pass the minimum amount of information that is required to enable those advisers to provide us with the advice required. The lawful basis for this processing will be ‘Legitimate Interests’. We have a legitimate interest in passing your information to such third parties but will ensure at all times that your rights are not infringed in any way and that the personal data we transfer is kept secure and only used for the purpose for which it was provided.

**13.9.4 Your Rights in Respect of Your Personal Information**

Under the Regulation, you have the right to find out what personal information we hold about you, and to ask for a copy of that personal data. You also have the right to demand that any inaccurate data be corrected or removed and to seek compensation where you suffer damage as a result of any breach of the Regulation by the Company.

You have the right on request to:

* Be told by the Company whether and for what purpose personal data about you is being processed.
* Be given a description of the personal data concerned and the recipients to whom it is or may be disclosed.
* Have communicated in an intelligible form the personal data concerned, and any information

available to the Company as to the source of the data.

* Be informed in certain circumstances of the logic involved in computerised decision-making.

A request for access to any personal data that relates to you should be made in writing to your Manager and should specify what personal data your request relates to. You can use our Personal Data Request Form for this purpose, a copy of which can be obtained from the Company Intranet. The Company also reserves the right to make further enquiries of you in order to satisfy ourselves as to your identity and to help us locate the personal data that you have requested.

Upon receipt of a request it is our policy to provide copies of all personal data that we are obliged to disclose within one month of your request being received. We consider that if a period of less than six months has elapsed since any previous request for access to your personal data was complied with, it is not reasonable to expect us to be obliged to comply with a further request unless there are exceptional circumstances.

Should you wish to bring any inaccuracy in disclosed data to our attention you must do so in writing to your Manager or the Data Protection Officer outlined in section 13.9.1 of this Data Protection Policy. It is the Company’s policy to ensure that all data is as accurate as possible and all necessary steps will be taken to ensure that this is the case and to rectify any inaccuracies.

Where we have requested a reference in confidence from a referee and that reference has been given on terms that it is confidential and that the person giving it wishes that it should not to be disclosed to you, it our policy that it would not normally be reasonable to disclose such a reference to you unless the consent of the person who gave the reference is first obtained. In any event, we will only retain such references for the same length of time as the probation period outlined in your contract of employment (including any extension to this period). After this time, they will be deleted.

We reserve the right not to disclose to you any management forecasts or management planning documentation, including documents setting out the Company’s plans for your future development and progress. We will also not disclose to you any information that contains personal data of any other person.

In addition to the specific rights outlined above, the Regulations also provide you with a number of other rights. However, whether or not you can exercise these rights depends entirely upon the lawful basis under which the personal data is being processed. The additional rights you may have are:

* The Right to Erasure – this gives you the right to have all personal data held about you deleted in its entirety.
* The Right to Portability – this gives you the right to have all personal data held about you transferred to you, or to a third party of your election.
* The Right to Object – this gives you the right to object to us processing upon the lawful basis under which we are processing it.

The table below outlines your rights and which can be exercised depending upon the lawful basis under which we are processing your personal data.

|  |  |  |  |
| --- | --- | --- | --- |
| **Lawful Basis for Processing** | **Right to Erasure?** | **Right to Portability?** | **Right to Object?** |
| Consent | Yes | Yes | No\* |
| Contractual Obligations | Yes | Yes | No |
| Legal Obligations | No | No | No |
| Vital Interests | Yes | No | No |
| Public Tasks | No | No | Yes |
| Legitimate Interests | Yes | No | Yes |

\* This does not change your right to withdraw consent to us processing your personal data where we are relying upon consent as the lawful basis.

If you have any questions regarding which rights you have in respect to the personal data we hold and process about you please speak to your Manager or the Data Protection Officer who will be able to assist.

If you believe that we have not handled any complaints relating to your personal data appropriately, you can contact the Information Commissioner’s Office (see [www.ico.gov.uk](http://www.ico.gov.uk)) who will be able to guide you as to your options should you wish to pursue the matter further.

**13.9.5 Your Obligations in Relation to Personal Information**

You must comply with the following requirements at all times:

* Do not give out confidential personal information except to the data subject. In particular, it should not be given to someone, either accidentally or otherwise, from the same family or to any other unauthorised third party unless the data subject has given their explicit consent to this.
* Be aware that those seeking information sometimes use deception in order to gain access to it. Always verify the identity of the data subject and the legitimacy of the request, particularly before releasing personal information by telephone.
* Only transmit personal information between locations by fax or email if a secure network is in place, for example, a confidential fax machine or encryption is used for email.
* If you receive a request for personal information about another employee, you should forward this to your Manager.
* Ensure that any personal data which you hold is kept securely, either in a locked filing cabinet or, if it is computerised, it is password protected.
* Do not include personal data in any email addressed to a recipient outside the European Economic Area (EEA) without their prior explicit consent. Note: the EEA comprises Members States of the European Union plus Iceland, Liechtenstein and Norway.

**13.9.6 Automated Decision-Making**

Automated decision-making occurs when an electronic system uses data to make a decision without any human intervention. We may use automated decision-making in the following circumstances:

* Where it is necessary to perform the contract of employment and we have put appropriate measures in place to safeguard your rights.
* With your explicit consent and where we have put appropriate measures in place to safeguard your rights.

You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making unless we have a lawful basis for doing so and we have notified you of this fact.

**13.9.7 Data Retention Policy**

Having completed an audit of the data held by Plastica Ltd, the General Data Protection Regulations requires the Company to have in place a Data Retention Policy that clearly defines how long we will hold your personal data, together with the reasoning behind the decision to hold that data.

Save for exceptional circumstances which must be raised with, and approved by, all personal data must be retained in accordance with this policy. Often, in respect of certain types of information, we are under a legal obligation to retain the information for a minimum period of time. Where this is the case, the minimum time we have stipulated is the same as the time required under law. Furthermore, there are occasions where it is appropriate for us to retain personal data for longer than the period prescribed in law (for example, where there may be litigation in process or expected where the data will form part of the evidence for this case). In such circumstances the requirements of the litigation will override the policies outlined below.

Plastica Ltd is committed to enforcing this policy as it applies to all forms of data. The effectiveness of Plastica’s efforts, however, depends largely on employees. If you feel that you or someone else may have violated this policy, you should report the incident immediately to your Manager. If you are not comfortable bringing the matter up with your Manager, or you do not believe the Manager has dealt with the matter properly, you should raise the matter with a Senior Manager or the Data Protection Officer. If employees do not report inappropriate conduct, Plastica may not become aware of a possible violation of this policy and may not be able to take appropriate corrective action. No one will be subject to and Plastica prohibits any form of discipline, reprisal, intimidation, or retaliation for reporting incidents of inappropriate conduct of any kind, pursuing any record destruction claim, or cooperating in related investigations.

Where this is a requirement for the Company to retain information for longer periods of time, consideration must be given to whether any personal data within it should be ‘anonymised’ such that the data subject can no longer be identified but the contents and context of the document still reviewed and understood. Where, in the table below, the data is identified as being capable of being anonymised, anonymisation should take place as soon as reasonably possible once the need to retain the personal data has expired.

A full list of our Data Retention Timescales can be obtained from the Company Intranet, the HR Department or your Manager or Supervisor.