

		Data Protection Policy	
Doc. No:	DP01	Rev.	A

## 1 Introduction

We have to collect and use certain information about people with whom we work. This personal information must be handled and dealt with properly however it is collected, recorded and used and whether it be on paper, in computer records or recorded by any other means.

We regard the lawful and correct treatment of personal information as very important to our successful operation and to maintaining confidence between us and those with whom we carry out business. We will ensure that we treat personal information lawfully and correctly. To this end we fully endorse and adhere to the principles of the General Data Protection Regulation (GDPR).

This policy applies to the processing of personal data in manual and electronic records kept by us as described below. It also covers our response to any data breach and other rights under the GDPR.

This policy applies to the personal data of job applicants, existing and former employees, apprentices, volunteers, placement students, advisors, workers and self-employed contractors. These are referred to in this policy as relevant individuals.

## 2 Definitions

**Personal data:** information relating to an identifiable person who can be directly or indirectly identified from that information, e.g. a person's name, identification number, location, online identifier. It can also include pseudonymised data.

**Special categories of personal data:** data which relates to an individual's health, sex life, sexual orientation, race, ethnic origin, political opinion, religion, and trade union membership. It also includes genetic and biometric data (where used for ID purposes).

**Criminal offence data:** data which relates to an individual's criminal convictions and offences.

**Data processing:** any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

## 3 Data Protection Principles

Under GDPR all personal data obtained and held by us must be processed according to a set of core principles. In accordance with these principles, we will ensure that:

- Processing will be fair, lawful and transparent
- Data be collected for specific, explicit, and legitimate purposes
- Data collected will be adequate, relevant and limited to what is necessary for the purposes of processing

		<b>Data Protection Policy</b>	
<b>Doc. No:</b>	DP01	<b>Rev.</b>	A

- Data will be kept accurate and up to date. Data which is found to be inaccurate will be rectified or erased without delay
- Data is not kept for longer than is necessary for its given purpose
- Data will be processed in a manner that ensures appropriate security of personal data including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisation measures
- We will comply with the relevant GDPR procedures for international transferring of personal data

#### 4 Types of Data Held

We keep a range of personal data on our employees in order to carry out effective and efficient processes. We keep this data in an HR file relating to each employee and we also hold the data within our computer systems. This data includes:

- personal details such as your name, address, gender, date of birth, photograph, phone numbers and email address
- information gathered during the recruitment process including your CV or cover letter, details of your education, academic and professional qualifications, skills and experience, employment history, references provided by former employers, supervisors or colleagues
- information about your identity, nationality and entitlement to work in the UK including passports, birth certificate, driving licence, residence permits / cards and visas
- information about your marital status, next of kin, dependants and emergency contacts
- the terms and conditions of your employment (including SMT, Apprenticeship Agreement or contract for services for self-employed contractor, job title, job description, salary, offer letters and related correspondence)
- details of your schedule (days of work and working hours) and attendance at work, building access records, equipment usage and network / internet access
- information about your remuneration, including entitlement to benefits such as pensions or insurance cover
- details of your bank account, national insurance number, tax code and statutory deductions or benefits
- details of periods of absence, including holiday, sickness absence, family leave, study leave and the reasons for the leave
- details of any formal or informal disciplinary or grievance procedures in which you have been involved, including any warnings issued to you and related correspondence
- details concerning any internal or external training undertaken
- assessments of your performance, including development meeting records, appraisal and performance information, targets and objectives, performance improvement plans and related correspondence, and written warnings

		<b>Data Protection Policy</b>	
<b>Doc. No:</b>	DP01	<b>Rev.</b>	A

- information about your criminal record
- accident records
- information about medical or health conditions, including whether or not you have a disability for which the organisation needs to make reasonable adjustments

All of the above information is required for our processing activities. More information on those processing activities are included in our privacy notice for employees and our privacy notice for job applicants, which is available from the HR Manager.

## 5 Your Rights

As data subjects, individuals have the following rights in relation to their personal data:

- the right to be informed about the data we hold on you and what we do with it;
- the right of access to the data we hold on you. More information on this can be found in the section headed "Access to Data" below and in our separate policy on Subject Access Requests
- the right for any inaccuracies in the data we hold on you, however they come to light, to be corrected ('rectification')
- the right to have data deleted in certain circumstances ('erasure')
- the right to restrict the processing of the data;
- the right to transfer the data we hold on you to another party ('portability')
- the right to object to the inclusion of any information;
- the right to regulate any automated decision-making and profiling of personal data.

To ask us to take any of these steps, the individual should send their request to: [dataprotection@adaptiximaging.com](mailto:dataprotection@adaptiximaging.com).

## 6 Responsibilities

In order to protect the personal data of relevant individuals, those within our business who must process data as part of their role have been made aware of our policies on data protection.

We have also appointed employees with responsibility for reviewing and auditing our data protection systems.

## 7 Lawful Bases of Processing

We acknowledge that processing may only be carried out where a lawful basis for that processing exists and we have assigned a lawful basis against each processing activity.

Where no other lawful basis applies, we may seek to rely on the data subject's consent in order to process data. However, we recognise the high standard attached to its use. We understand that consent must be freely given, specific, informed and unambiguous. Where consent is to be sought, we will do so on a specific and individual basis where appropriate. Data subjects will be given clear

		<b>Data Protection Policy</b>	
<b>Doc. No:</b>	DP01	<b>Rev.</b>	A

instructions on the desired processing activity, informed of the consequences of their consent and of their clear right to withdraw consent at any time.

## 8 Access to Data

Individuals have a right to access the personal data that we hold on them. To exercise this right individuals should make a Subject Access Request. We will comply with the request without delay, and within one month unless, in accordance with legislation, we decide that an extension is required. Those who make a request will be kept fully informed of any decision to extend the time limit.

No charge will be made for complying with a request unless the request is manifestly unfounded, excessive or repetitive, or unless a request is made for duplicate copies to be provided to parties other than the individual making the request. In these circumstances, a reasonable charge will be applied.

Further information on making a subject access request is contained in our Subject Access Request policy (DP06).

## 9 Data Disclosures

We may be required to disclose certain data/information to any person. Disclosures will only be made when strictly necessary for the purpose. The circumstances leading to such disclosures include:

- ensuring smooth operation of any employee insurance policies, pension plans or other benefits such as share options
- administering any employee benefits operated by third parties
- administering any employee statutory payments and deductions
- determining whether any reasonable adjustments are required at work for people with disabilities
- compliance with health and safety or occupational health obligations towards the employee
- considering how an individual's health affects their ability to do their job
- assisting law enforcement or relevant authorities in prevention or detection of crime, prosecution of offenders or assessing or collecting any tax or duty

## 10 Data Security

The security of your personal information is important to us. We seek to use reasonable physical, technical, and administrative safeguards to protect the information we process. We have internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties. Further detail can be obtained in our Computer Systems Procedure, our Employee Handbook and the Company's Data Audit Log.

Failure to follow the Company's rules on data security may be dealt with via the Company's disciplinary procedure. Appropriate sanctions include dismissal with or without notice dependent on the severity of the failure.

		Data Protection Policy	
Doc. No:	DP01	Rev.	A

## 11 Third Party Processing

Where we engage third parties to process personal data on our behalf, we will request that the third parties have appropriate technical and organisational measures in place to ensure the security of such data as required under the GDPR.

## 12 International Data Transfers

We may be required to transfer personal data to a country/countries outside of the EEA. Transfers may take place where third party providers (e.g. Google, Microsoft) store our cloud data outside of the EEA. Where this occurs, we will request such third parties have appropriate technical and organisational measures in place to ensure the security of our data as required under the GDPR.

## 13 Requirement to Notify Breaches

All data breaches will be recorded on our Data Breach Register. Where legally required, we will report a breach to the Information Commissioner within 72 hours of discovery. In addition, where legally required, we will inform the individual whose data was subject to breach. More information on breach notification is available in our Breach Notification policy (DP05).

## 14 Training

New employees must read and understand our policies on data protection as part of their induction. All employees receive training covering basic information about confidentiality, data protection and the actions to take upon identifying a potential data breach. Our appointed compliance officer is trained appropriately in their role under the GDPR.

All employees who need to use our computer systems are required to protect individuals' private data, to ensure data security, and to understand the consequences to them as individuals and the Company of any potential lapses and breaches of our policies and procedures.

## 15 Records

We keep records of our processing activities including the purpose for the processing and retention periods in our Data Audit Log. These records will be kept up to date so that they reflect current processing activities.

## 16 Data Protection Compliance

Our appointed compliance officer in respect of our data protection activities is:

**Name:** Sarah Small  
**Role:** Company Secretary  
**Email:** [dataprotection@adaptiximaging.com](mailto:dataprotection@adaptiximaging.com)  
**Tel:** 01865 309619

 <b>Data Protection Policy</b>			
<b>Doc. No:</b>	DP01	<b>Rev.</b>	A

17 Document History

Rev.	Nature of Change	Change Owner
A	Initial Issue	Hannah Torrie

18 Owner and Approval

Reviewed by	<b>Title</b>	<b>Name</b>
	CEO	Mark Evans
Process Owner	<b>Title</b>	<b>Name</b>
	HR Manager	Hannah Torrie