DATA PROTECTION POLICY

CONTENTS

PURPOSE

Nylacast collect and processes information about individuals (i.e., 'personal data') This includes personal data relating to employees, customers, suppliers and other third parties.

Compliance with data protection law is essential to ensure that personal data remains safe, business operations are secure, and the rights of individuals are respected. The Company is a controller under data protection law, meaning it decides how and why it uses personal data. This Policy explains procedures for complying with data protection law in relation to personal data. It also sets out the Company's obligations whenever it is processing any personal data in the course of employment.

The UK GDPR sets out seven key principles:

- Lawfulness. Fairness and transparency
- Purpose Limitation
- Data minimization
- Accuracy
- Storage Limitation
- Integrity and confidentiality (security)
- Accountability

The data both in electronic (softcopy) and hardcopy format at the end of any retention period.

SCOPE

This Policy applies to everyone who has a contractual relationship with Nylacast, including all employees, customers, and suppliers, consultants/self-employed freelancers carrying out roles which, if carried out by an employee would require disclosure no matter where they are located (within or outside the UK).

The policy covers data created or held, including:

- Paper records
- Electronic files (including database, Word documents, spreadsheets, webpages, and e-mails).
- Photographs, scanned images, CD-ROMs, and video & audio tapes.
- The following personal data about you will be kept by us:
- Original application form, including CV where submitted.
- Personal references.
- Your Contract of Employment and any amendments to it.
- Correspondence with or about you, for example
    a) Pay review details.
    b) At your request, letters to your mortgage company confirming salary.
- Information needed for payroll, benefits, and expenses purposes.
- Contact and emergency contact details.
- Records of holiday, sickness, and other absence.
- Information needed for our equal opportunities monitoring policy.

Records relating to your career history, such as training records, appraisals, other performance measures and where appropriate, disciplinary and grievance records Personal data about you will only be disclosed to third parties if we are legally obliged to do so.

REFERENCE DOCUMENTS

- IT Policy and Procedures
- IT Data & Hardware Disposal Policy
- Disciplinary Policy
- Whistleblower Policy
- The Employee Handbook

RESPONSIBILITY

The Board is ultimately responsible for the Company's compliance with applicable data protection law. The Company has appointed a Data Protection Lead who is responsible for overseeing, advising on and administering compliance with this Policy and data protection law.
The Data Protection Lead is the HR Manager.

All employees have some responsibility for ensuring that personal data is kept secure and processed in a lawful manner.

If an employee is in any doubt about how personal data should be handled or has any concerns or questions in relation to the operation (or suspected breaches) of this Policy, they should seek advice from the Data Protection Lead.

POLICY

Data protection law in the UK is regulated and enforced by the Information Commissioner's Office (ICO). Failure to comply with data protection law may expose the Company and, in some cases, individual employees to serious legal liabilities.

These can include criminal offences and fines of up to EUR20 million or 4% of total worldwide annual turnover, whichever is higher. In addition, an individual may seek damages from the Company in the courts if it breaches their rights under data protection law. Breaches of data protection law can also lead to considerable damage to the Company's brand and reputation.

In addition to the legal liabilities, failure to comply with the Company's obligations under this Policy could lead to disciplinary action and, in serious cases, it could result in the termination of employment.

WHAT IS PERSONAL DATA

Personal data means any information relating to any living individual (also known as a 'data subject') who can be identified (directly or indirectly) by reference to an identifier (e.g., name, NI number, employee number, email address, physical features). Relevant individuals can include colleagues, consumers, members of the public, business contacts, etc. Personal data can be factual (e.g., contact details or date of birth), an opinion about a person's actions or behaviour, or information that may otherwise impact on that individual. It can be personal, or business related.

WHAT DOES 'PROCESSING' PERSONAL DATA MEAN

'Processing' personal data means any activity that involves the use of personal data (e.g., obtaining, recording, or holding the data, amending, retrieving, using, disclosing, sharing, erasing, or destroying). It also includes sending or transferring personal data to third parties.

DATA PROTECTION OBLIGATIONS

The Company is responsible for and must be able to demonstrate compliance with data protection law. To ensure that the Company meets its responsibilities, it is essential that employees comply with data protection law and any other company policies, guidelines or instructions relating to personal data when processing personal data in the course of employment.

The Company has set out below the key obligations under data protection law and details of how it expects employees to comply with these requirements.

FAIR AND LEGAL GROUNDS FOR PROCESSING

Data protection law allows the Company to process personal data only where there are fair and legal grounds which justify using the information.

Examples of legal grounds for processing personal data include the following (at least one of these must be satisfied for each processing activity):

- complying with a legal obligation (e.g., health and safety or tax laws).
- entering into or performing a contract with the individual (e.g., an employee's terms and conditions of employment, or a contract for services with an individual customer).
- acting in the Company's or a third party's legitimate interests (e.g., maintaining records of
- business activities, monitoring business productivity); and
- obtaining the consent of the individual (e.g., for sending direct marketing communications).

Where consent is relied upon, it must be freely given, specific, informed, and unambiguous, and the Company must effectively demonstrate that consent has been given.

In line with ICO guidance regarding the employer/employee relationship, the Company does not use consent as a legal ground for processing employee data unless the data processing activities concerned are genuinely optional.

TRANSPARENCY

Data protection law also requires the Company to process personal data in a transparent manner by providing individuals with appropriate, clear, and concise information about how it processes their personal data.

The Company usually provide individuals with basic information about how the Company uses their data on forms which collect data (such as application forms, employee data forms or website forms), and in the longer Privacy Notice setting out details including: the types of personal data that the Company holds about them, how the Company uses it, the legal grounds for processing the information, who the Company might share it with and how long the Company keeps it for. For example, the Company provide information about the processing of employees' personal data in the Company's Privacy Notice.

The standard Privacy Notice that the Company issues, for example, to employees, customers, and suppliers, should normally be sufficient to ensure that individuals have appropriate information about how the Company is handling personal data. However, the Company considers whether reminders or additional information may be appropriate at the time particular processing activities take place. This is particularly important if the Company thinks that individuals may need further assistance to understand clearly how their data will be used as part of such activities.

Any new forms which collect personal data, and any proposed consent wording must be approved in advance by the Data Protection Lead.

If an employee or individual has any concerns about the legal grounds for processing personal data or if it is unsure whether individuals have been provided with appropriate information (in relation to any new processing activities), please check with the Data Protection Lead.

SENSITIVE OR SPECIAL CATEGORIES OF PERSONAL DATA

Some categories of personal data are 'special' because they are particularly sensitive. These include. information that reveals details of an individual's:

- racial or ethnic origin.
- political opinions.
- religious or philosophical beliefs.
- trade union membership.
- physical or mental health.
- sexual life or sexual orientation.
- biometric or genetic data (if used to identify that individual); and
- criminal offences or convictions.

Where special category personal data is concerned, data protection law requires the Company to have an additional legal ground to justify using this sensitive information. The appropriate legal ground will depend on the circumstances.

Additional legal grounds for processing special category data include the following (those marked with an asterisk (*) are particularly relevant to processing employees' special category personal data):

- complying with a legal obligation/exercising a legal right in the field of employment*.
- assessing working capacity (based on expert medical opinion, and subject to obligations of confidentiality) *.
- carrying out equalities monitoring in relation to racial or ethnic origin, religious beliefs, health, or sexual orientation*.
- exercising, establishing, or defending legal claims*.
- preventing or detecting unlawful acts; or
- explicit consent of the individual. (In addition to the requirements for consent outlined above, this requires an express statement from the individual that their special category of data may be used for the intended purposes.)

If the Company is handling special category personal data in the course of employment, it needs to take extra care regarding compliance with data protection law. In particular, the Company tries to ensure that:

- all processing activities are strictly in accordance with our lawful job duties and the Company's instructions.
- there are appropriate legal grounds for processing the data (basic and additional grounds) which have been assessed for our specific activities.
- individuals have received adequate information regarding how their data is being handled. In some cases, an existing Privacy Notice may need to be supplemented with more specific information regarding special category.
- the Company applies additional security and confidentiality measures, considering that the impact on individuals of loss or misuse of their special category data may be greater than with other types of data. See also see below; and

  if the Company is relying on consent as a legal ground for processing, it obtains advance approval of any consent wording from the Data Protection Lead.

If the Company is routinely handling special category data as part of the requirements of a role and job duties, it will ordinarily have put in place procedures which ensure that the processing activities satisfy the requirements above.

However, if alternative circumstances apply (e.g., the Company is involved in a new project or updating an existing system which involves new types of processing of special category data), the Data Protection Lead must be contacted to ensure that the correct compliance procedures are followed.

Similarly, if an employee has any concerns over the legal grounds that apply when the Company is processing special category data or the appropriate information to be provided to individuals, they must contact the Data Protection Lead.

ONLY PROCESS PERSONNAL DATA FOR SPECIFIED, EXPLICIT AND LEGITIMATE PURPOSES

The Company will only process personal data in accordance with legitimate purposes to carry out business operations and to administer employment and other business relationships.

The Company must only use the personal data that it processes in the course of its duties for legitimate and authorised purposes. The Company must not process personal data for any purposes which are unrelated to job duties.

Processing personal data for any incompatible or unauthorised purposes could result in a breach of data protection law (e.g., using the company contacts database to find out a colleague's home address for private, non-work-related purposes). This may have potentially damaging consequences for all parties concerned, including disciplinary action.

If any employee needs to process personal data for a different purpose from that for which it was originally collected, they must check whether the individuals have been informed and, if not, consider whether the additional purpose is legitimate (in the context of the Company's business activities) and compatible with the original purpose.

If an employee is unsure about whether the purposes for processing are legitimate, they should contact the Data Protection Lead before going ahead with processing the data for the additional purpose.

MAKE SURE THAT PERSONAL DATA IS ADEQUATE, RELEVANT, AND LIMITED TO WHAT IS NECESSARY FOR LEGITIMATE PURPOSES

Data protection law requires the Company to ensure that, when it processes personal data, it is adequate, relevant to the purpose/s and limited to what is necessary for those purpose/s (also known as 'data minimisation'). In other words, the Company ask for the information it needs for legitimate business purposes but will not ask for more information than it needs in order to carry out business operations.

The Company should try to ensure that it only acquires and processes the personal data that it actually need for its legitimate and authorised purposes within the scope of individuals' roles.

The Company must ensure that it has sufficient personal data needed to be able to use it fairly and to take into account all relevant details.

If the Company is creating forms that collect personal data, it should be able to justify why each specific category of data is being requested.

The Company must also comply with instructions about data retention and storage, ensuring that personal data is only kept for as long as it is needed for any intended purpose.

KEEP PERSONAL DATA ACCURATE AND UP TO DATE

The Company must take steps to ensure that personal data is accurate and (where necessary) kept up to date. For example, the Company requests that employees provide changes in contact details or personal information via their manager through completion of the Employee Change Form. The

Company also take care that decisions impacting individuals are based on accurate and up-to-date information.

When the Company processes individuals' personal data in the course of employment, it must make reasonable efforts to be accurate and, where necessary, keep the relevant information updated. When collecting any personal data, a manager must confirm its accuracy at the outset. If the Company subsequently discovers any inaccuracies in the personal data that is being handled, these need to be corrected or deleted without delay.

Personal data should be held in as few places as possible to avoid the risk that duplicate copies are not updated and become out of sync. No employee should create additional copies of personal data but should work from and update a single central copy where possible (in accordance with standard company procedures on retention and storage of records).

KEEP PERSONAL DATA FOR NO LONGER THAN IS NECESSARY FOR THE IDENTIFIED PURPOSES

Records containing personal data should only be kept for as long as they are needed for the identified purposes. The Company has in place data retention, storage and deletion policies and internal processes/guidelines regarding various types of company records and information that contain personal data.

The Company take appropriate steps to retain personal data only for so long as is necessary, considering the following criteria:

- the amount, nature, and sensitivity of personal data.
- the risk of harm from unauthorised use or disclosure.
- the purposes for which the Company processes the personal data and how long it needs to keep the data to achieve these purposes.
- how long the personal data is likely to remain accurate and up to date.
- for how long the personal data might be relevant to possible future legal claims; and
- any applicable legal, accounting, reporting or regulatory requirements that specify how long certain records must be kept.

All employees must familiarise themselves with the Company's retention policies, processes, guidelines, and instructions that are relevant to their job and must ensure that, where it falls within the employee's responsibility, all information is destroyed or erased if the Company no longer requires it.

If an employee is not sure what retention guidelines/instructions apply to their role, or how to apply them to a particular type or item of personal data, the Data Protection Lead should be contacted.

TAKE ALL APPROPRIATE STEPS TO KEEP PERSONAL DATA SECURE

Keeping personal data safe and complying with the Company's security procedures to protect the confidentiality, integrity, availability, and resilience of personal data is a key responsibility for both the Company and employees.

The Company has an IT Policy & Procedures, which sets out its organisational and technical security measures to protect information, including personal data. The Company regularly evaluates and tests the effectiveness of these measures to ensure the security of our personal data processing activities as set out in this policy.

The Company also has a Technology and Communications Policy which sets out protocols for employees on the use of technology and communications systems, which also help to ensure appropriate security of personal data stored or communicated using such systems.

To assist the Company in maintaining data security and protecting the confidentiality and integrity of the personal data the Company handle in course of our employment, the Company requires employees to comply with this Policy, IT Policy & Procedures, IT Data & Hardware Disposal Policy and any company instructions regarding the processing and security of personal data. In particular, the Company require employees to:

- Save, store, and communicate personal data only within or using authorised information and communications systems.
- Restrict storage of personal data on personal devices or using personal communications facilities (or BYOD controls)
- Use password-protected and encrypted software for the transmission and receipt of emails.
- Lock files in a secure cabinet
- Never leave a laptop, other device or any hard copies of documents containing personal data in a public place
- Take care when observing personal data in hard copy or on-screen that such information is not capable of being viewed by anyone who does not have the right to that information, especially if the personal data is being viewed in a public place.
- When storing data on portable devices such as laptops, smartphones, or USB drives, ensure that the device is encrypted, and password protected.
- Ensure that information containing personal data is disposed of securely and permanently, using confidential waste disposal or shredding where necessary.
- Alert the Data Protection Lead to any personal data breaches immediately and in accordance with the company's breach management procedure (see below)
- Ensure that any sharing or disclosure of personal data is permitted on appropriate legal grounds and, where necessary, safeguards are in place (see below for further details of safeguards regarding overseas transfers or if sharing personal data with third party service providers)

TAKE EXTRA CARE WHEN SHARING OR DISCLOSING PERSONAL DATA

The sharing or disclosure of personal data is a type of processing, and therefore all the principles described in this Policy need to be applied.

INTERNAL DATA SHARING

The Company ensures that personal data is only shared internally on a 'need to know' basis.

EXTERNAL DATA SHARING

The Company will only share personal data with other third parties (including group entities) where the Company have a legitimate purpose, and an appropriate legal ground under data protection law which permits us to do so. Commonly, this could include situations where the Company is legally obliged to provide the information (e.g., to HMRC for tax purposes) or where necessary to perform contractual duties to individuals (e.g., provision of information to occupational pension providers).

The Company may appoint third party service providers (known as processors) who will handle information on its behalf, for example to provide payroll, data storage or other technology services. The Company remains responsible for ensuring that its processors comply with data protection law and this Policy in their handling of personal data. The Company must assess and apply data protection and information security measures prior to and during the appointment of processors. The extent of these measures will vary depending on the nature of the activities, but will include appropriate risk assessments and reviews, and contractual obligations.

The Company may only share or disclose the personal data it holds internally with an employee, agent, or representative of the Company if the recipient has a job-related need to know the information.

The Company may only disclose the personal data the Company hold to service providers or other third parties (including group entities) where:

- there is a legitimate purpose and an appropriate legal ground for doing so (e.g., it is necessary for them to process the personal data in order to provide a service to us, such as payroll, or if the Company is legally obliged to do so, e.g., HMRC).
- the individuals whose personal data is being shared have been properly informed (e.g., in an appropriate Privacy Notice).
- if the disclosure is to a service provider, the Company has checked that adequate security and data protection measures are in place to protect the personal data concerned.
- the service provider or third party has signed up to a written contract that contains the provisions required by data protection law (unless the Data Protection Lead has determined that this is not required in context); and
- the transfer complies with any overseas transfer restrictions, if applicable.

Routine disclosures of personal data to established recipients (e.g., payroll providers or group entities) which form a normal and regular part of a role and job duties will ordinarily satisfy the above requirements. However, if an employee is in any doubt as to whether the Company can share personal data with anyone else, they must contact the Data Protection Lead.

Do not transfer personal data to another country unless there are appropriate safeguards in place.

An overseas transfer of personal data takes place when the data is transmitted or sent to, viewed by, accessed by, or otherwise processed in, a different country. European Union data protection law restricts personal data transfers to countries outside of the European Economic Area to ensure that the level of data protection afforded to individuals is not compromised (as the laws of such countries may not provide the same level of protection for personal data as within the EEA).

To ensure that data protection is not compromised when personal data is transferred to another country, the Company assesses the risks of any transfer of personal data outside of the UK (considering the principles in this Policy, as well as the restrictions on transfers outside the EEA) and puts in place additional appropriate safeguards where required.

The Company do not currently transfer customer and supplier data to countries outside of the EEA.

If the Company is required to transfer individuals' personal data outside of the UK or EEA in the course of employment, adequate safeguards will need to be in place. Where these overseas transfers are a normal part of a role and job duties, the Company's current safeguards are likely to provide the required levels of data protection.

However, if an employee is transferring personal data overseas in alternative circumstances (e.g., for new types of processing activities which haven't previously formed part of the job scope and activities, or to countries with which an employee has not previously dealt with) they should contact the Data Protection Lead for further guidance before going ahead with the transfer.

.

DO NOT USE PROFILING OR AUTOMATED DECISION-MAKING UNLESS YOU ARE AUTHORISED TO DO SO

Profiling, or automated decision-making, occurs where an individual's personal data is processed and evaluated by automated means resulting in a major decision being taken in relation to that individual. This poses risks for individuals where a decision is based solely on that profiling or other automated processing.

One example of solely automated decision-making would be using an online psychometric test to automatically reject job applicants who do not meet a minimum pass mark (without any human oversight such as a review of the test results by a recruiting manager).

Data protection law prohibits decision-making based solely on profiling or other automated processing, except in very limited circumstances. In addition, where profiling or other automated decision-making is permitted, safeguards must be put in place and the Company must give individuals the opportunity to express their point of view and challenge the decision. The Company do not generally conduct profiling or other automated decision-making in respect of employees, customers', or suppliers' personal data.

If the Company conducts profiling or other automated decision-making at any time, the Company will familiarise itself with and implement any applicable safeguards.

If an employee is proposing to undertake any new automated decision-making or profiling activities in the course of employment, please contact the Data Protection Lead who will advise whether it is permitted and about the safeguards the Company need to put in place.

The Company does not currently use profiling or automated decision-making process.

INTEGRATE DATA PROTECTION INTO OPERATIONS

Data protection law requires the Company to build data protection considerations and security measures into all our operations that involve the processing of personal data, particularly at the start

of a new project or activity which may impact on the privacy of individuals. This involves considering various factors including:

- the risks (and their likelihood and severity) posed by the processing for the rights and freedoms of individuals.
- technological capabilities.
- the cost of implementation; and
- the nature, scope, context, and purposes of the processing of personal data.

The Company also seeks to assess data protection risks regularly throughout the lifecycle of any project or activity which involves the use of personal data.

If an employee is involved in the design or implementation of a new project or activity that involves processing personal data, they must give due consideration to all the principles of data protection set out in this policy.

The employee should assist the Data Protection Lead with regular reviews of projects or activities to ensure data protection risks continue to be addressed.
A useful tool for assessing data protection and privacy considerations is a Data Protection Impact Assessment or 'DPIA'. A DPIA will consider the necessity and proportionality of a processing operation and assess the risks to individuals and the measures that can be put in place to mitigate those risks. A DPIA must be carried out if a data processing operation is likely to give rise to a high risk to individual rights and freedoms.

If an employee is involved in the design or implementation of a new project that involves processing personal data, they must check whether it is necessary to conduct a DPIA or similar risk or compliance assessment by contacting the Data Protection Lead who will also be able to advise on how the Company expects to conduct, or otherwise contribute to, a DPIA or similar risk assessment.

INDIVIDUAL RIGHTS AND REQUESTS

Under data protection law, individuals have certain rights when it comes to how the Company handle their personal data. For example, an individual has the following rights:

- **The right to make a 'subject access request'.** This entitles an individual to receive a copy of the personal data the Company holds about them, together with information about how and why the Company processes it and other rights which they have (as outlined below). This enables them, for example, to check whether the Company is lawfully processing their data and to correct any inaccuracies.

- **The right to request that the Company correct incomplete or inaccurate** personal data that the Company holds about them.

- **The right to withdraw any consent** which they have given.

- **The right to request that the Company delete or remove personal** data that the Company holds about them where there is no good reason for it continuing to process it. Individuals also have the right to ask us to delete or remove their personal data where they have exercised their right to object to processing (see below).

- **The right to object to the processing** of their personal data for direct marketing purposes, or where the Company is relying on legitimate interest (or those of a third party), where the Company cannot show a compelling reason to continue the processing.

- **The right to request that the Company restrict the processing** of their personal data. This enables individuals to ask the Company to suspend the processing of personal data about them, for example if they want the Company to establish its accuracy or the reason for processing it.

- **The right to request that the Company transfer** to them or another party, in a structured format, their personal data which they have provided to the Company (also known as the right to 'data portability'). The applicability of this right depends on the legal grounds on which the Company process it.

- **The right to challenge a decision** based solely on profiling/automated processing, to obtain human intervention, and to express their point of view.

The Company is required to comply with these rights without undue delay and, in respect of certain rights, within a one-month timeframe.

Individuals also have rights to complain to the ICO about, and to take action in court to enforce their rights and seek compensation for damage suffered from, any breaches.

If a manager receives a request from an individual seeking to exercise a right in relation to their personal data or making an enquiry or complaint about the Company's use of their personal data, the manager must forward the request, enquiry, or complaint to the Data Protection Lead immediately so that it can be dealt with appropriately and within the applicable time limit in accordance with the Company's individual personal data rights procedures.

RECORD KEEPING

If an employee is processing individuals' personal data in the course of employment and the Company collect any new types of personal data or undertake any new types of processing activities, either through the introduction of new systems or technology or by amending existing ones, please inform the Data Protection Lead so that the Company can keep records up to date.

Retention of records. The Company follows the retention periods recommended by the Information Commissioner in its Employment Practices Data Protection Code.

You should therefore treat the following as guidelines for retention times in the absence of a specific business case supporting a longer period:

APPLICATION FORM	DURATION
References received	1 year
Payroll and tax information	6 years
Sickness records	3 years
Annual leave records	2 years
Unpaid leave/special leave records	3 years
Annual appraisal/assessment records	5 years
Records relating to promotion, transfer, training, disciplinary matters	1 year from end of employment
References given/information to enable references to be provided	5 years from reference/end of employment
Summary of record of service, e.g., name, position held, dates of employment	10 years from end of employment
Records relating to accident or injury at work	12 years

Any data protection queries should be addressed to your line manager or our Data Protection Officer.

COMPLIANCE

In order to comply, and demonstrate compliance, with data protection law, the Company keeps various records of data processing activities. These include a Record of Processing which must contain, as a minimum: the purposes of processing; categories of data subjects and personal data; categories of recipients of disclosures of data; information about international data transfers; envisaged retention periods; general descriptions of security measures applied; and certain additional details for special category data.

The Company must also comply with applicable processes/guidelines and any specific instructions that are given concerning the keeping of records about processing of personal data.

TRAINING, AWARENESS AND COMMUNICATION

Training will be provided for those employees who have a specific responsibility for implementing the Procedure or who may be involved in dealing with complaints which arise.

All employees will be informed of the Data Protection Policy.

The Data Protection Policy will be in employee's induction programmes, with a summary in the Company Handbook.

REPORTING AND MONITORING

If the Company discovers that there has been a personal data security breach that poses a risk to the rights and freedoms of individuals, the Company will report it to the ICO within 72 hours of discovery.

The Company also keep an internal record of all personal data breaches regardless of their effect and whether the Company reports them to the ICO. Additionally, the Company will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures the Company have taken.

If an employee becomes aware of any breach (or suspected breach) of this Policy (including, any security breach), they must report it to the Data Protection Lead immediately.

The Company takes any data protection breaches very seriously. These can include lost or mislaid equipment or data, use of inaccurate or excessive data, failure to address an individual's rights, accidental sending of data to the wrong person, unauthorised access to, use of or disclosure of data, deliberate attacks on the Company's systems or theft of records, and any equivalent breaches by the Company's service providers.

Where there has been a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to individuals' personal data, the Company will take immediate steps to identify, assess and address it, including containing the risks, remedying the breach, and notifying appropriate parties (see below). The Company has a Breach Management Procedure which sets outs its procedures for identifying, assessing, and addressing security breaches.

EXCEPTIONS OR WAIVERS

This Policy does not give contractual rights to any employees. It may be updated at any time.

This Policy supersedes all previous Data Protection Policies applicable to the UK.

REVIEW AND REVISION

The HR Manager / appropriate Director will be responsible for reviewing the Policy and Procedure.

CHANGE HISTORY

Date	Rev. No.	Revision by	Description of change
04/07/19	01	Ian Mallabone	First issue of the Policy
07/07/2021	02	Ian Mallabone	Policy formatting changed
01/04/2023	03	Ian Mallabone	Retention period table updated