STRIDE TREGLOWN

Data Protection Policy

1.1 Introduction

At Stride Treglown, we collect and process information about individuals (i.e. 'personal data') for business purposes, including employment and HR administration, provision of our services, marketing, and business administration. This includes personal data relating to our staff, clients, suppliers and other third parties.

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

If an Employee routinely handles individuals' personal data, they will be given specific training and instructions regarding data protection procedures in relation to their particular team. This training will supplement their obligations as set out in this Policy.

There will also be other policies which will impact on how Employees deal with personal data and data protection. The main ones are our Equipment Use Policy (which describes the acceptable use of company equipment, and personal equipment for business purposes), our Social Media Policy and our Data Security Policy (which sets out its organisational and technical security measures to protect information, including personal data).

We expect Employees to comply with these where relevant.

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

1.2. Who does this Policy apply to?

This Policy applies to all Stride Treglown employees, workers, contractors, agency workers, consultants, interns, volunteers, partners and directors (together referred to as 'Employees').

1.3. Who is responsible for data protection at Stride Treglown?

The Board is ultimately responsible for Stride Treglown's compliance with applicable data protection law. Stride Treglown has appointed a Data Security Team who are responsible for overseeing advising Stride Treglown on and administering compliance with this Policy and data protection law. The Data Security Team consists of representatives from IT, Marketing / BD, HR and the Board. Representatives from other areas of the business will be co-opted as necessary.

All Employees at Stride Treglown have some responsibility for ensuring that personal data is kept secure and processed in a lawful manner although certain Employees will have particular responsibilities, of which they will be aware and in respect of which they may receive specific instructions.

If an Employee is in any doubt about how they should handle personal data, or if they have any concerns or questions in relation to the operation (or suspected breaches) of this Policy, they should seek advice from the Data Security Team (DataSecurity@StrideTreglown.com).

1.4. Why is data protection compliance important?

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 Stride Treglown and, in some cases, individual Employees to serious legal liabilities. These can include criminal offences and fines of up to EUR20 million (approximately £18 million) or 4% of total worldwide annual turnover, whichever is higher. In addition, an individual may seek damages from us in the courts if we breach their rights under data protection law. Breaches of data protection law can also lead to serious damage to Stride Treglown's brand and reputation.

In addition to our legal obligations, Stride Treglown's policy is to support a culture where we process data professionally, responsibly and respectfully. This supports our values of collaboration, trustworthiness and respect. These values enable us to interact better with clients, Employees, partners and suppliers which in turn, makes our organisation more effective.

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

Pierre Wassenaar (Chair)
3rd January 2023

Darren Wilkins (Managing Director)
3rd January 2023

Last Reviewed: 3rd January 2023

Data Protection Policy

1.5. 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) in particular by reference to an identifier (e.g. name, NI number, Employee number, email address, physical features). Relevant individuals can include Employees' 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.

Personal data may be automated (e.g. electronic records such as computer files or in emails) or in manual records which are part of a filing system or are intended to form part of a filing system (e.g. structured paper files and archives).

1.6. 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.

2. Data Protection Obligations

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

We have set out below the key obligations under data protection law and details of how Stride Treglown expects Employees to comply with these requirements.

2.2. Process personal data in a fair, lawful and transparent manner

2.2.1 Legal grounds for processing

Data protection law allows us 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. a contract for services with an individual client or an Employee's terms and conditions of employment);
- acting in Stride Treglown 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).

Occasionally, we may also hold and use personal data: in the public interest for the detection or prevention of crime; or where needed to protect somebody's vital interests.

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

In most cases, consent is also not required for other standard business activities involving use of client or supplier data, but it may be needed for activities which are not required to manage the main business relationship, such as direct marketing activities.

2.2.2 Transparency

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

We usually provide individuals with basic information about how we use their data on forms which collect data (such as application forms or website forms), and in longer privacy notices setting out details including: the types of personal data that we hold about them, how we use it, our legal grounds for processing the information, who we might share it with and how long we keep it for. For example, we provide information about our processing of Employees' personal data in the Stride Treglown Employee Privacy Notice.

We supplement these notices, where appropriate, with reminders or additional information at the time particular processing activities take place or become relevant for an individual (for example when they sign up for a new service or event).

2.2.3 What Employees need to do:

By processing personal data only in accordance with their lawful job duties and Stride Treglown instructions, ordinarily, Employees will be processing personal data fairly and lawfully.

The standard privacy notices and statements that we issue, for example, to Employees, clients and the public, should normally be sufficient to ensure that individuals have appropriate information about how our Employees are handling their personal data in the course of their employment. However, Employees should consider whether reminders or additional information may be appropriate at the time particular processing activities take place. This is particularly important if an Employee 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 Security Team.

If an Employee has any concerns about the legal grounds for processing personal data or if they are unsure whether individuals have been provided with appropriate information (in particular in relation to any new processing activities), then we ask the Employee to please check with the Data Security Team.

2.3. Take extra care when handling 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 us to have (as well as one of the legal grounds described in section 1), 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 (*) would be 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. (As well as the requirements for consent outlined in section 1 above, this requires an express statement from the individual that their special category of data may be used for the intended purposes.)

2.3.2 What Employees need to do:

If an Employee is handling special category personal data in the course of their employment, they need to take extra care regarding compliance with data protection law.

In particular, they must try to ensure that:

- any processing activities are strictly in accordance with their lawful job duties and Stride Treglown instructions;
- there are appropriate legal grounds for processing the data (both basic grounds under section 2.1 and additional grounds under this section 2.2) which have been assessed for their 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 data (e.g. when Stride Treglown is managing sickness absence and/ or making adjustments to job duties for Employees with disabilities or serious illness, we may provide additional ad hoc privacy notices to supplement the Employee Privacy Notice);
- they apply additional security and confidentiality measures, taking into account 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 section 2.7 below (Take appropriate steps to keep personal data secure); and
- if they are relying on consent as a legal ground for processing, they obtain advance approval of any consent wording from the Data Security Team.

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

However, if alternative circumstances apply (e.g. they are involved in a new project or updating an existing system which involves new types of processing of special category data), please contact the Data Security Team to ensure that the correct compliance procedures are followed.

Similarly, if an Employee has any concerns over the legal grounds that apply when they are processing special category data or any concerns over the appropriate information to be provided to individuals, then we ask the Employee to get in touch with the Data Security Team.

2.4. Only process personal data for specified, explicit and legitimate purposes

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

2.4.2 What Employees need to do:

Employees must only use the personal data that they process in the course of their duties for Stride Treglown's legitimate and authorised purposes. They must not process personal data for any purposes which are unrelated to their 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 an Employee finds that they need 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 Stride Treglown'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 Security Team who will undertake a Legitimate Interests Assessment (LIA) before the Employee goes ahead with processing the data for the additional purpose.

2.5. Make sure that personal data is adequate, relevant and limited to what is necessary for Stride Treglown's legitimate purposes

Data protection law requires us to ensure that, when we process personal data, it is adequate, relevant to our purposes and limited to what is necessary for those purposes (also known as 'data minimisation'). In other words, we ask for the information we need for our legitimate business purposes, but we won't ask for more information than we need in order to carry out our business operations.

2.5.2 What Employees need to do:

Employees should try to ensure that they only acquire and process the personal data that they actually need for Stride Treglown's legitimate and authorised purposes within the scope of their role.

They must ensure that they have sufficient personal data needed to be able to use it fairly and to take into account all relevant details.

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

They must also comply with Stride Treglown's instructions about data retention and storage, ensuring that personal data is only kept for as long as it is needed for any intended purpose.

2.6. Keep personal data accurate and (where necessary) up-to-date

Stride Treglown must take steps to ensure that personal data is accurate and (where necessary) kept up-to-date. For example, we request that Clients or Suppliers inform their Stride Treglown contact or the Marketing team. We ask Employees to provide us with any change in contact details or personal information by informing their office manager or contacting the HR team. We also take care that decisions impacting individuals are based on accurate and up-to-date information.

2.6.2 What Employees need to do:

When Employees process individuals' personal data in the course of their employment, they must make reasonable efforts to be accurate and, where necessary, keep the relevant information updated.

When collecting any personal data, Employees must try to confirm its accuracy at the outset. If they subsequently discover any inaccuracies in the personal data that they are handling, 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. Employees should not create additional copies of personal data, but should work from and update a single central copy where possible (in accordance with standard Stride Treglown procedures on retention and storage of records).

Data Protection Policy

2.7. 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. Stride Treglown 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.

We take appropriate steps to retain personal data only for so long as is necessary, taking into account the following criteria:

- the amount, nature, and sensitivity of the personal data;
- the risk of harm from unauthorised use or disclosure;
- the purposes for which we process the personal data and how long we need the particular 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.

2.7.2 What Employees need to do:

Employees must familiarise themselves with our retention policies, processes, guidelines and instructions that are relevant to their job. They must ensure that, where it falls within their responsibility, they destroy or erase all information that they no longer require in accordance with these.

If an Employee is not sure what retention guidelines/instructions apply to them in their role, or they are unsure of how to apply them to a particular type or item of personal data, then the Employee should contact the Data Security Team.

2.8. Take appropriate steps to keep personal data secure

Keeping personal data safe and complying with Stride Treglown's security procedures to protect the confidentiality, integrity, availability and resilience of personal data is a key responsibility for Stride Treglown and its workforce.

Stride Treglown has a Data Security Policy, which sets out its organisational and technical security measures to protect information, including personal data.

Stride Treglown also has an Equipment Use Policy which describes the acceptable use of company equipment, and personal equipment for business purposes The Equipment Use Policy helps to ensure appropriate security of personal data stored or communicated using our systems.

We regularly evaluate and test the effectiveness of our measures to ensure the security of our data processing activities (including personal data) and we are annually audited to maintain our Cyber Essential Plus certification as a minimum but often go beyond this, for example with further penetration testing.

2.8.2 What Employees need to do:

To assist Stride Treglown in maintaining data security and protecting the confidentiality and integrity of the personal data Employees handle in the course of their employment, we require Employees to comply with this Policy, our Equipment Use Policy, our Data Security Policy and any Stride Treglown instructions regarding the processing and security of personal data.

2.9. 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.

2.9.2 Internal data sharing

Stride Treglown mandates that personal data is only shared internally on a 'need to know' basis.

2.9.3 External data sharing

Stride Treglown will only share personal data with other third parties (including group entities) where we 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 we are legally obliged to provide the information (e.g. to HMRC for tax purposes) or where necessary to perform our contractual duties to individuals (e.g. provision of information to our occupational pension providers).

2.9.3.2 We may appoint third party service providers (known as processors) who will handle information on our behalf, for example to provide technical services such as payroll, data storage, planning applications, system and application support etc.

2.9.3.3 Stride Treglown remains responsible for ensuring that its processors comply with data protection law and this Policy in their handling of personal data. We must assess and apply data protection and information security measures prior to and during the appointment of a processor. 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.

2.9.3.4 Details of the recipients or categories of recipients of personal data (including processors and other third parties) should be set out in privacy notices as described in section 2.1 (particularly section 2.1.2 Transparency) above (Process personal data in a fair, lawful and transparent manner).

2.9.4 What Employees need to do:

2.9.4.1 Employees may only share or disclose the personal data we hold internally with an Employee, agent or representative of Stride Treglown if the recipient has a job-related need to know the information.

Employees may only disclose the personal data we 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 we are legally obliged to do so);
- 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, Stride Treglown 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 Security Team 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 an Employee's role and job duties will ordinarily satisfy the above requirements. Employees should always ensure they comply with any particular Stride Treglown instructions they are given. However, if they are in any doubt as to whether they can share personal data with anyone else, first contact the Data Security Team.

2.10. 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, accessed or otherwise processed in, a different country. European Union data protection law restricts, in particular, personal data transfers to countries outside of the European Economic Area (EEA – this is the European Union plus Norway, Liechtenstein and Iceland), 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, Stride Treglown assesses the risks of any transfer of personal data outside of the UK (taking into account the principles in this Policy, as well as the restrictions on transfers outside the EEA) and puts in place additional appropriate safeguards where required.

We do not normally transfer personal data outside the UK.

2.10.2 What Employees need to do:

If an Employee is required to transfer individuals' personal data outside of the UK or EEA in the course of their employment, adequate safeguards will need to be in place. Where these overseas transfers are a normal part of their role and job duties, Stride Treglown'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 their job scope and activities, or to countries with which they haven't previously dealt) they should contact the Data Security Team for further guidance before going ahead with the transfer.

2.11. Report any data protection breaches without delay

Stride Treglown 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 Stride Treglown's systems or theft of records, and any equivalent breaches by Stride Treglown'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, Stride Treglown will take immediate steps to identify, assess and address it, including containing the risks, remedying the breach, and notifying appropriate parties (see below).

This will usually involve appointing a board director-led breach management team who will produce and execute a breach management plan. The breach management team is not the same as the data security team although it is likely that at least one member of the data security team will join the breach management team in an advisory and/or executive capacity. The members of the board carry overall responsibility for personal data processing and to limit the possible consequences, it is essential that breaches are dealt with immediately that they are discovered.

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

We also keep an internal record of all personal data breaches regardless of their effect and whether or not we report them to the ICO.

If a personal data breach is likely to result in a high risk to the rights and freedoms of individuals, we will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures we have taken. All of these actions will be included in the breach management plan.

2.11.2 What Employees need to do:

If an Employee becomes aware of any breach (or suspected breach) of this Policy (including, in particular any security breach), they must report it to the Data Security Team immediately via email to DataSecurity@StrideTreglown.com. The data security team will immediately escalate it to a board director.

If the discovery is outside of normal office hours then the employee who becomes aware of it should also immediately escalate it to a board member who will put together a breach management team to start to create and execute a breach management plan. It is vital that the discoverer of the breach escalates this to the board immediately and the time of the discovery is noted so that we can comply with our data breach reporting obligations within the strict time scales laid down by the Act.

2.12. 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 an important decision being taken in relation to that individual. This poses particular 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 we must give individuals the opportunity to express their point of view and challenge the decision.

We do not currently conduct profiling or other automated decision-making in respect of Employees', clients', prospective clients', suppliers', partners' or other individuals' personal data.

2.12.2 What Employees need to do:

If an employee conducts profiling or other automated decision-making in the course of their role, they must familiarise themselves with and implement any applicable safeguards. Stride Treglown recommends that automated decision making is never used in isolation and that some manual oversight is also put in place.

If an Employee is proposing to undertake any new automated decision-making or profiling activities in the course of their employment, they must first contact the Data Security Team, who will advise them whether it is permitted and about the safeguards they need to put in place.

2.13. Integrate data protection into operations

Data protection law requires Stride Treglown to build data protection considerations and security measures into all of 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 taking into account 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.

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

2.13.2 What Employees need to do:

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 Security Team with reviews of projects or activities where necessary 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 Security Team. The Data Security Team will also be able to advise the Employee on how we expect them to conduct, or otherwise contribute to, a DPIA or similar risk assessment.

3. Individual Rights and Requests

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

- **The right to make a 'Subject Access Request' (SAR).** This entitles an individual to receive a copy of the personal data we hold about them, together with information about how and why we process it and other rights which they have (as outlined below). This enables them, for example, to check we are lawfully processing their data and to correct any inaccuracies.

- **The right to request** that we correct incomplete or inaccurate personal data that we hold about them.

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

- **The right to request that we delete or remove personal data** that we hold about them where there is no good reason for us 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 our processing of their personal data** for direct marketing purposes, or where we are relying on our legitimate interest (or those of a third party), where we cannot show a compelling reason to continue the processing.

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

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

We are 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.

3.1.2 What Employees need to do:

If an Employee receives a request from an individual seeking to exercise a right in relation to their personal data, or making an enquiry or complaint about our use of their personal data, they must forward the request, enquiry or complaint to the Data Security Team immediately so that it can be dealt with appropriately and within the applicable time limit in accordance with Stride Treglown's individual personal data rights procedures. The Employee's assistance may be needed to address and respond to the request, enquiry or complaint.

Data Protection Policy

4. Record Keeping

In order to comply, and demonstrate our compliance, with data protection law, Stride Treglown keeps various records of our data processing activities. These include a Record of Processing Employee data and an external contacts database 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.

4.1 What Employees need to do:

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

If an Employee is processing individuals' personal data in the course of their employment and they 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, they must inform the Data Security Team so that we are able to keep our records up-to-date.

5. Training

We require all Employees to undergo some basic training to enable them to comply with data protection law and this policy. Additional training may be required for specific roles and activities involving the use of personal data.

To this end, we provide training as part of our induction process for new joiners to Stride Treglown and operate an ongoing training programme to make sure that Employees' knowledge and understanding of what is necessary for compliance in the context of their role is up-to-date. Attendance at such training is mandatory and will be recorded.

6. Departures from this Policy

There are some very limited exemptions from data protection law, which may permit departure from aspects of this Policy in certain circumstances.

Employees will be given specific instructions if any exemptions are relevant to their role.

If an Employee thinks they should be able to depart from this Policy in any circumstances, they must contact the Data Security Team before taking any action.