STRIDE Data Protection & GDPR Policy

Stride UK

Version	Date Approved	Actions
1.0	January 2022	Policy internally reviewed & revised accordingly
2.0	January 2023	Internally Reviewed by DM
Reviewed:	January 2023	
Review frequency:	Annually	
Next review:	September 2024	

Stride Data Protection Policy

1. Introduction
As a data controller STRIDE is committed to protecting the privacy and security of employees, staff and service users personal information and is responsible for deciding how personal information about its employees is held and used.

2. Principles
This policy sets out the basis by which the personal information of our employees is collected, used and disclosed, as well as individual rights in respect of such personal information.
In collecting and processing personal information, the business will comply with the data protection law in force at the time. This requires that the personal information held must be:
• Used lawfully, fairly and in a transparent way
• Collected only for valid purposes and not used in any way that is incompatible with those purposes
• Relevant to the purposes communicated and limited only to those purposes
• Accurate and kept up to date
• Kept only as long as necessary for the purposes we have identified
• Kept securely

3. The type of information held about employees / staff and service users, how and when it will be used
The business may collect the following types of personal information:
• Name, address, email address, telephone number and other contact information that allow the business to meet organisational and statutory obligations
• Driving licence details;
• Details of family members and Next of Kin details
• Bank details;
• Right to work documentation and other screening information
• Discipline and. grievance records
• Absence records
• Medical/occupational health information

Some of the information may include sensitive personal information for example:
• Ethnicity, sexual orientation, marital status, religion
• Medical information;
• Criminal records

4. Using personal information
Personal information may be used in the following ways:
• To ensure that the information held about an individual is kept up-to-date
• To deal with any employee/employers related disputes that may arise
• For assessment and analysis purposes to help improve the operation of, and manage the performance of the business
• To prevent, detect and prosecute fraud and other crime
• For any other purpose for which an individual gives consent to use personal information
• To comply with legal obligations e.g. HMRC, pensions

5. How is personal information collected?
The business may collect personal information in several ways, for example when an individual:
• Contacts HR either via telephone or email
• Registers for recruitment and vacancy updates
• Completes satisfaction surveys that are used for performance purposes
• Enters a competition
• Applies for a vacancy internally or externally
• Is involved in the application of any HR policies e.g. Disciplinary
• Places contact details on the company's internal staff personnel file
• Uses any HR services

The business may also collect personal information from third parties, for example recruitment agencies or previous employers as well as in the course of managing an individual's employment.

6. If an employee fails to provide personal information
Without certain information the business may not be able to perform the contract agreed with an employee (such as paying them or providing a benefit), or it may be prevented from complying with legal obligations (such as to ensure the health and safety of workers and checking an individual's right to work in the UK for example).

7. Change of purpose
Personal information will only be used for the purposes for which it was collected, unless it is reasonably considered that it is needed for another reason and that reason is compatible with the original purpose.
If personal information needs to be used for an unrelated purpose, the employee will be notified and the legal basis which allows it explained. The business may process personal information without the employee's knowledge or consent in compliance with the above rules where this is required or permitted by law.

8. Consent to use sensitive information
Consent is not required if personal information is used in accordance with this policy to carry out legal obligations or exercise specific rights in the field of employment law.
In limited circumstances, written consent may be sought to allow the processing of certain particularly sensitive data (for example, medical information). In this case full details of the information required and the reasons for needing it will be communicated, so that employees can carefully consider whether they wish to consent.
Employees should be aware that it is not a condition of their contract of employment that they agree to any request for consent.

9. Sharing personal information with third parties
The business might have to share personal information with third parties, including third party service providers, where it is required by law, where it is necessary to administer the working relationship with an individual or where there is another legitimate interest in doing so.
Personal information may be shared:
• With STRIDE partners (e.g. schools and community venues where STRIDE delivers its projects)

• With third party contractors who provide services to the business; (e.g. DBS Umbrella Partners)
• Where there is a legal obligation to do so, for example sharing information under statute, to prevent fraud and other criminal offences or because of a Court Order for example HRMC, the police.

Some of the above grounds for processing will overlap and there may be several grounds which justify the use of personal information.
Third party service providers are not allowed to use personal information for their own purposes, they are only permitted to process personal information for specified purposes.

10. Data security
The business has appropriate security measures in place to prevent personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. Access to personal information is limited to those who have a business need to know.
Individuals and any applicable regulator will be notified of any suspected data security breach where legally required to do so.

11. Data retention
Personal information will only be retained for as long as necessary to fulfil the purposes it was collected for, including for the purposes of satisfying any legal, accounting or reporting requirements.
In some circumstances personal information may be anonymised so that it can no longer be associated with an individual, in which case it may be used without further notice to the individual.

12. Employee duties
It is important that personal information held about employees is accurate and up to date. Employees are required to inform the business of any changes to personal information during their employment.

13. Employee rights
Employees have specific rights in certain circumstances to:
• Request access to personal information (commonly known as a 'data subject access request' This enables the individual to receive a copy of personal information held about them and to check that the business is lawfully processing it
• Request corrects to personal information held about them
• Request erasure of personal information where there is no good reason for the business to continue processing it. Employees also have the right to request for information to be deleted where they have exercised their right to objecting against personal information being processed
• Object to processing of personal information where the business relies on a legitimate interest and there is something about the employee's particular situation which makes them want to object processing on this ground. The right to object also extends to the business processing personal information for direct marketing purposes
• Request the suspension of processing personal information if an employee wants to establish the accuracy or the reason for processing it
• Request the transfer of personal information to another party

14. Complaints
Employees have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.

16. Changes to this privacy notice
The business update this Privacy Notice from time to time and will communicate an up to date copy of the Privacy Notice via Google Drive.