# SDS Data Protection Policy

| Descriptor | Changes made | Date | Version |
|---|---|---|---|
| Policy first implemented | GDPR Compliant | February 2018 | 1.0 |
| Internal DP Team review, redraft | General updates; updates to section 7 'Key Compliance Requirements'. | August 2020 | 1.1 |
| IGLG review | IGLG review, comments taken into account to inform minor updates. | September 2020 | 1.2 |
| Senior Director Review/approval | Policy reviewed and approved by Senior Director (Eugene Gallanagh). | December 2020 | 2.0 |
| Internal DP Team review, content approved | Point-in-time updates made to legislative references and description of the roles of particular teams and individuals. Small tweaks made to use more accessible language. | December 2022 | 3.0 |
| DP Team/CPPR review (correction) | Review date amended (typo in published version) | April 2024 | 3.1 |
| DP Team/Policy Working Group | Various updates for clarity and currency; new section on accessing SDS systems and data from outwith the UK. | August 2024 | 4.0 |

| | |
|---|---|
| Name of policy being superseded (if applicable) | N/A |
| Related policies | All found via the Policy Hub on Connect:<br>Code of Conduct<br>CCTV Policy<br>Employee Privacy Notice<br>Freedom of Information Policy<br>Information Access Control Policy<br>Physical Premises Security Policy<br>Policy on the Use of Protective Markings<br>Records Management Policy |

| | |
|---|---|
| | Social Media Policy<br>Using SDS IT Equipment and Systems Policy |
| Related SOPs | The following Data Protection processes and procedures can be found under the 'Data Protection Policies & Procedures' page on Connect:<br>- Data Breach handling process<br>- Data Subject Request handling process<br>- Microsoft Teams Recording request procedure |
| Related Guidance | Data Protection Guidance<br>Records Management Guidance (can be found under 'Records Management Guidance' page on Connect).<br>SDS Monitoring Guidance<br>Use of Generative Artificial Intelligence (AI) and Large Language Models (LLM): SDS Acceptable Use Guidance |
| Equality Impact Assessment completed | No (completed previously) |
| Intended Audience | All SDS colleagues; Information Asset Owners |
| Team responsible for policy | Data Protection Team |
| Policy owner contact details (email) | DPO@sds.co.uk |
| Policy due for review (date) | August 2026 |

## Contents

1. Policy summary ..... 3
2. Policy purpose and objectives ..... 4
3. Strategic context ..... 4
4. Definitions ..... 5
5. Scope ..... 5
6. Roles and Responsibilities ..... 6
7. Key compliance requirements ..... 7
8. Further guidance ..... 11

## 1. Policy summary

This policy sets out the framework for a consistent SDS wide approach to handling information relating to identifiable data subjects (Personal Data). Skills Development Scotland stores and processes personal data and information on behalf of its customers, partners and employees and has a duty to protect this information as mandated by Data Protection Legislation.

## 2. Policy purpose and objectives

SDS is committed to adopting best practice in protecting personal information. This policy sets out the approach adopted by SDS to comply with the legal requirements and maintain the trust of customers, partners and employees. The legislation covers any information that can identify a living person.

For SDS, this primarily covers personal data relating to:

- Customers (young persons; users of our services including businesses and employers);
- Employees and ex-employees of SDS and its predecessor companies; and
- Partners/Suppliers (information about directors, partners, sole traders or employees of the company or organisation is covered, including contact details).

## 3. Strategic context

The purpose of Data Protection is the protection of the individual ('data subject) from having their personal data or privacy exploited or abused. This places the onus upon organisations and individuals that are involved in processing such data to ensure that the processing is conducted in a fair, lawful and secure way. It is therefore of vital importance that all SDS employees comply with the requirements of this policy.

The core principles set out in Data Protection Legislation make it a requirement that personal data must be:

- *'processed lawfully, fairly and in a transparent manner in relation to data subjects*
- *'collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes*
- *'adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*
- *'accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay*
- *'kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of data subjects; and*
- *'processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.*

## 4. Definitions

The following key concepts and definitions need to be understood:

- ***Appropriate Policy Document*** - a document which outlines the compliance measures and retention policies for Special Category and/or Criminal Offence Data;
- ***Data Controller*** – a person or organisation that determines the purpose and means of processing personal data;
- ***Data Processor*** – a person who or organisation which processes personal data on behalf of a data controller;
- ***Data Protection Impact Assessment (DPIA)*** – a risk assessment process which helps to identify and reduce the data protection risks of processing personal data;
- ***Data Protection Legislation*** - the legislation relating to the processing of personal data currently in force in the United Kingdom, which includes the Data Protection Act (2018) and the UK GDPR;
- ***Data Sharing Agreement (DSA)*** – a document between organisations which details what data is being shared and how it is used;
- ***Data Subjects*** – the term used to describe an identified or identifiable living individual to whom personal data relates;
- ***DPA*** - the Data Protection Act (2018), the UK-specific legislation that incorporates the GDPR and creates certain exemptions and exceptions for the processing of personal data within the United Kingdom;
- ***Information Commissioner's Office (ICO)*** - the UK's independent regulatory body for Data Protection Legislation, who have powers to impose monetary penalties on organisations for non-compliance;
- ***Personal Data (or 'Personal Information')*** – information that relates to an identified or identifiable individual, including expressions of opinion or intention about them;
- ***Privacy Notice –*** information which is provided to Data Subjects about the collection and use of their personal data;
- ***Processing*** – any operation or set of operations which is performed on personal data, including obtaining, recording or using data, including its organisation, adaptation, alteration, retrieval, disclosure, or erasure of it or any combination of these;
- ***Record of Processing Activities (ROPA)*** - a document which records the overall processing activities concerning Data Subjects personal data;
- ***Special Category Data*** - specific category of data under Data Protection Legislation that is particularly sensitive and therefore requires a greater level of protection, so additional requirements apply to it;
- ***UK GDPR*** - the retained EU law version of the General Data Protection Regulation as it forms part of the law of England and Wales, Scotland and Northern Ireland.

## 5. Scope

This policy applies to all employees within SDS, also to individuals who are seconded into SDS from another organisation (or employed through an agency). Everyone involved in SDS business, including third party contractors and Board Members, has a responsibility to familiarise themselves and comply with this policy. **Non-compliance with this policy may be dealt with under our Disciplinary Policy and Procedure.**

## 6. Roles and Responsibilities

***All SDS Colleagues*** are responsible for ensuring that they understand the implications of Data Protection Legislation and of this policy for their roles and that they comply.

The ***SDS Board*** are accountable for SDS's compliance with Data Protection Legislation and for the appointment of a Data Protection Officer.

The ***Data Protection Officer (DPO)*** is a mandatory designated role under Data Protection Legislation. The DPO's primary focus is on monitoring and providing assurance to SDS's senior management and the Board on the organisation's compliance with all its statutory obligations under Data Protection Legislation. The DPO will also actively foster a positive culture of data protection across SDS and will provide expert advice and guidance to staff at all levels across SDS on data protection matters, including guidance on undertaking Data Protection Impact Assessments and, where appropriate, breach notification to the Information Commissioner.

The ***Data Protection Team (DP Team*** supports the DPO and the business to ensure SDS's organisational compliance with Data Protection Legislation and to deliver an effective data protection function. This includes:

- coordinating and responding to Data Subject Requests received by SDS;
- working with the business to carry out Data Protection Impact Assessments (DPIAs) in order to identify and mitigate risks of activities that involve the use of personal data;
- maintaining such technical documentation as is required for compliance with Data Protection Legislation e.g. Privacy Notices, Register of Processing Activities (ROPA) and an 'Appropriate Policy Document' among others;
- preparation of Data Sharing Agreements to support the business in sharing data with external organisations;
- management of requests from Data Subjects regarding their personal data that is held by SDS (including requests to access personal data, or have it deleted);
- investigation, resolution and internal reporting of data breaches affecting personal data held by SDS;
- ensuring colleagues understand the importance of data protection and responding to any queries relating to the use of personal data;
- engaging with external partners on data protection matters.

The ***EIS Cyber Security Team*** is responsible for ensuring information security policies, processes and practices are in place to support the requirements as set out in Data Protection Legislation to protect personal information and data from compromise. The EIS Team will also support the DP Team with investigations into electronic data breaches.

***The SDS Legal Team*** are responsible for providing guidance on the interpretation of UK GDPR and Data Protection Legislation in more complex cases.

The ***SDS Business Continuity & Resilience*** team is responsible for managing incidents which disrupt SDS services, including major data breach incidents.

***Human Resources*** directorate are responsible for supporting the Data Protection team regarding Data Subject requests under Data Protection Legislation that are made by

employees or former employees, in line with agreed processes and procedures.

# 7. Key Policy Requirements

This section focuses on key requirements of Data Protection Legislation and this policy, and how to demonstrate good practice in data protection. This will help SDS colleagues to carry out their role at SDS whilst keeping personal data secure and ensuring that individuals' rights relating to their data are respected.

Please note that there is separate guidance, available on Connect, that colleagues must familiarise themselves with if they are involved in:

- Collecting or receiving personal data from customers
- Using personal data as part of a wider project or piece of work
- Transferring personal data to an external organisation
- Transferring personal data outside of the UK

**Understanding the types of data relevant to Data Protection**

## 7.1 Personal data

Personal data is any piece of information that can directly or indirectly identify a living individual. The ICO website provides detailed guidance as to whether information can be considered personally identifiable or not.

PRACTICAL EXAMPLE

- David Smith gets in touch with you through his email address David.Smith@companyname.co.uk.
- His email address is still personal data, even though it is his work email address, as it includes his name 'David Smith'.

## 7.2 Special category data

Under the UK GDPR, there is a specific category of personal data called 'special category data'. Special category data is particularly sensitive and therefore requires a greater level of protection. This relates to the following:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health (e.g. information relating to a disability);
- sex life; or
- sexual orientation.

**Additional conditions that must be met when processing special category data**

In processing special category data, SDS must ensure it is compliant with the terms of Article 9 of the UK GDPR. This sets out the different legal bases under which you are permitted to process special category data.

For SDS, the bases under which we process special category data are the following:

- when we have the explicit consent of the individual (e.g. information on an individual's disability, for use in a case study published on our website, or when using biometric data).
- when we have a legal obligation to ask for this information and report on it (i.e. our obligations under the Equality Act 2010;
- when doing so is in the public interest in the area of public health (e.g. processing health/sickness related information in response to a pandemic);
- when doing so is in the substantial public interest (e.g. receiving special needs data related to school pupils so we can provide relevant CIAG support);
- processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
- processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
- when processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services;
- when it is for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

For any of the scenarios above where SDS would process special category data, it is of paramount importance that it is stored in a secure location and that only a limited number of colleagues that require access to it, for a justified business purpose, can do so.

It is important to note that special category data does not include data that has been **anonymised**. For example, if you have produced a report that includes a high-level, anonymised breakdown of Modern Apprentices and their racial/ethnic backgrounds (and provided that the numbers of this report aren't low enough to potentially identify any data subjects) then that is not personal data and therefore it is not special category.

However, if the data was personally identifiable at the point you collected or received it (e.g. you could see it was Jane Smith that answered a certain way to a question on racial/ethnic background), you still need to define a purpose and legal basis for processing this data and ensure that it complies with the legislation and this policy. You may then later anonymise this data (which greatly reduces the risk attached to it), but you still need a purpose and legal basis for collecting it in the first place.

For any large-scale processing of special category data, particularly when it is planned to be collected or received as part of a new project, piece of work or process, the Data Protection Team at DPO@sds.co.uk must be consulted at an early stage of the planning phase to ensure that a Data Protection Impact Assessment (DPIA) is carried out. This will ensure that the risks of the processing are identified and assessed and that appropriate mitigating actions are agreed and implemented.

### 7.3 How to handle and store personal data securely

Once personal data has been collected or received, it must be handled in a manner that is compliant with Data Protection Legislation. Handling and storage of personal data must also be compliant with the SDS policies on the Use of Protective Markings and Information Access Control. Compliance with these policies and their associated guidance will minimise the risk of a data breach.

Personal data must be stored in a secure location, only accessible to colleagues who require access for the purposes of carrying out their role. Access must be reviewed where colleagues join SDS, move teams in SDS and leave SDS, so that only those colleagues with a legitimate business purpose can access a certain file, folder or system.

### 7.4 How to identify and respond to a Personal Data Breach

All staff are required to understand how to recognise a Personal Data breach and the steps they require to take in response.

An organisation and/or its employees can be held criminally liable for offences leading from data breaches that are held to be intentional or arising from negligence. A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

If you become aware of a possible personal data breach you must contact the DP team at DPO@sds.co.uk as soon as possible (**no later than 48 hours after discovering the breach**) so that a decision can be made on whether the ICO needs to be notified. This is particularly important as organisations are legally required to report certain types of personal data breach to the ICO. The Data Protection team must report certain kinds of data breaches within **72 hours** of **the organisation becoming aware of the breach**.

This does mean that if you discover a possible personal data breach on a Friday afternoon, it is important to notify the Data Protection Team at DPO@sds.co.uk before the close of business that day and inform us of what may have happened so that the Data Protection Team can make a decision on whether this should be reported to the ICO.

At this point you may not have all the details to hand, but the earliest possible notification gives the Data Protection Team the best chance to investigate the breach and take prompt action.

Personal data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

### 7.5 How to recognise and handle Data Subject Requests

You may be contacted by an individual regarding their rights under Data Protection Legislation. This could be, for example, a customer, partner/stakeholder or fellow colleague. The full list of rights available to data subjects can be found on the ICO website, however, common requests you may receive are:

- Requests to obtain a copy of personal data that SDS holds on them (e.g. an excerpt of an HR record, a copy of a CSS or FIPS record)
- Requests to erase personal data that SDS holds on them (e.g., deletion of their customer record on CSS, FIPS or their My World of Work account)
- Stating a withdrawal of consent for a particular processing activity

If you receive such a request from an individual, you must pass this as soon as possible to the Data Protection Team at DPO@sds.co.uk (this is the point of contact for all data subjects). As previously noted with data breaches, SDS has a specific timeframe in which to respond to all Data Subject requests. **For these requests, SDS has 1 calendar month to comply.** This clock starts as soon as SDS receives the request.

Data Subject requests can be verbal, written or made through social media. They do not have to be addressed to the Data Protection Officer or Data Protection Team to be valid. They also do not have to be titled 'data subject request' to be valid. All that is required is a clear indication or message that an individual is wishing to enact one of their rights.

You may be more likely to receive a request if you are working in CIAG or closely with Data Subjects, as you may be seen as a first point of contact. Whilst we advise Data Subjects to contact the Data Protection Team directly regarding these requests (from our website's privacy notice) a request made to any colleague in SDS is still a valid request.

### 7.6 How to assess data protection/privacy risks (Data Protection Impact Assessments)

The purpose of a DPIA is to identify and reduce the data protection risks of processing personal data. You must do a DPIA for processing that is likely to result in high risk to individuals. To assess the level of risk, you must consider both the likelihood and the severity of any impact on individuals.

Examples (although these are not exhaustive) of when, you must do a DPIA are as follows:

- Process Special Category or Criminal Offence data;
- Use systematic and extensive profiling or automated decision-making to make significant decisions about people;
- Procure new software that may involve the Processing of Personal Data;
- Process Personal Data without providing a Privacy Notice directly to the individual;
- Process Personal Data in a way that involves tracking individuals' online or offline location or behaviour;
- Process children's Personal Data (under the age of 18);
- Combine, compare or match Personal Data from multiple sources;
- Process personal data on a large scale;
- Process personal data for evaluation and scoring.
- Carry out systematic monitoring of people or public areas

If you are unsure whether you require to complete a DPIA, contact the SDS Data Protection Team.

### 7.7 Accessing SDS Systems (and Data) from outwith the UK

Accessing business systems and software applications (and the data held in them, including personal data) from outside the UK can create additional cyber and information security risk exposure and make a data breach more likely. To reduce this risk there are additional controls in place for SDS colleagues, as set out in the Using SDS Equipment & Systems Policy. This requires that where intending to access our systems from abroad, colleagues must seek appropriate approval and give prior notification to EIS and to the DP team (contact DPO@sds.co.uk).

## 8. Further guidance

Further information on the UK GDPR and data protection requirements is available from the Information Commissioner's Office: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

Or you can email the SDS Data Protection Officer/SDS Data Protection Team: **DPO@sds.co.uk**