Data Protection Policy

Descriptor	Changes made	Date	Version
Policy first implemented	GDPR Compliant	21/2/18	2.0
Review no.1			
Review no.2			
Review no.3			

Name of policy being superseded (if applicable)	SDS Data Protection Policy
Related policies	
Related SOPs	
Related Guidance	
Equality Impact Assessment completed	No
Intended Audience	All Staff
Team responsible for policy	Data Protection Team
Policy owner contact details (email)	DPO@sds.co.uk
Policy due for review (date)	February 2020

Contents

1. Policy summary

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

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 Act covers all information about living individuals.

For SDS this covers:

- Clients (young persons, users of our services);
- 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 the Data Protection is the protection of the individual from having his/her personal data or privacy exploited or abused. This places the onus upon organisations and individuals 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.

GDPR Principles requires that personal data shall be:

- a) processed lawfully, fairly and in a transparent manner in relation to individuals;
- b) 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;
- c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- d) 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;
- e) 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 GDPR in order to safeguard the rights and freedoms of individuals; and
- f) 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 need to be understood:

- ***GDPR*** - is the EU General Data Protection Regulation which will replace the Data Protection Act 1998 in the UK and the equivalent legislation across the EU Member States.
- ***Personal Data*** – is information held about living, identifiable individuals, including expressions of opinion or intention about them;
- ***GDPR Controller*** – a controller determines the purposes and means of processing personal data.
- ***GDPR Processor*** – a processor is responsible for processing personal data on behalf of a controller
- ***Data Subjects*** – are individuals about whom the data is held;
- ***Processing*** – obtaining, recording or using the data, including organisation, adaptation, alteration, retrieval, disclosure, or erasure of it or any combination of these.

5. Scope

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

6. Policy detail

Roles and Responsibilities

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

The ***Information Governance Scrutiny & Innovation Group (IGSIG)*** are responsible for ensuring appropriate co-ordination and oversight is in place to ensure that SDS remains compliant with GDPR. The group commissions and approves Data Protection policies and procedures.

The ***Data Protection Officer (DPO)*** is mandatory designated role under GDPR and is responsible for managing a range of data protection activities at a corporate level. The 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.

- Coordinate and respond to Subject Access Requests responses received by SDS
- effective management of data breach investigation and internal reporting.
- breach notification to the Information Commissioner.

- expert advice and guidance to staff at all levels across SDS on data protection matters, including guidance on undertaking data protection impact assessments.

The ***Data Protection Team (DP Team)*** is the team who support the DPO in their role and provides support to the business for general queries. The team ensures that GDPR documentation set is maintained.

The ***EIS Information Assurance Team*** is responsible for ensuring Information Security policy's, processes and practices are in place to support the GDPR requirements to protect personal information from compromise. The Team will also support the DPO with investigations into electronic data breaches.

The SDS Legal Team are responsible for providing guidance on the interpretation of GDPR and Data Protection legislation in more complex cases and where there are issues around the interface of the DPA and other legislation.

Information Asset Owners must ensure that personal data is only processed and disclosed under the terms of the defined purposes, and that any new purposes for which personal data is processed or new classes of data subject or parties to whom disclosure will be made are notified to the Data Protection Officer for inclusion in an updated Information Asset Register. Information Asset Owners will engage with EIS to identify measures required on IS systems to protect their information.
Information Asset Owners are also required to co-ordinate and monitor compliance with Data Sharing Agreements.

All Employees are responsible for ensuring that they understand the implications of GDPR and this policy for their roles, and comply.

Human Resources are responsible for co-ordinating the response to Subject Access Requests where the requester is an employee or former employee.

Facilities Management are responsible for ensuring adequate secure storage is available for personal data in hard copy.

Compliance Requirements – All Employees

Gathering personal information

It is important that the person to whom the personal information relates to is aware of the following:

- Why we need it; ask only for what we need and not collect too much or irrelevant information;
- Protect it and make sure no unauthorised person has access to it;
- Let the data subject know if we will share it with other organisations and give them the opportunity to refuse;
- Make sure we don't keep it any longer than is necessary;
- Not make the data subjects personal information available for commercial use without their consent;
- Consider the data subjects request to stop processing data about them;
- Consider the data subjects request to delete data held about them

Obtain sufficient data for the purpose

Where items of personal data would be useful to us, but are not essential, obtain the data subject's consent or ensure that they are aware they have a choice about whether to provide them.

Do not collect excessive items of personal data on the basis that they might be useful for some unspecified purpose in the future.

Obtain or accept data only from sources which are lawfully allowed to supply it.

Processing personal information

Disclose the data only to parties who require it in relation to the purpose for which it was obtained. This includes both internal and external parties. Refer any requests for access to personal data held by the SDS from third parties (i.e. external parties who are not given access in the normal course of business or under the terms of an existing data sharing agreement) to the DPO for advice.

When disclosing personal data to third parties, take reasonable steps to confirm their identities. Be alert to the possibility of individuals attempting to obtain personal data by deception.

Ensure that further processing is compatible with the original purpose for which the data was obtained.

Seek the consent of the data subject for any new or non-obvious use or disclosure of the data.

Take reasonable steps to ensure that the data is accurate

Take reasonable steps to ensure that data is kept up to date. This can often be done by contacting the data subject periodically and asking them to confirm continued accuracy or provide any updates.

Make sure that any inaccuracies discovered are promptly corrected, including situations where the data subject points out inaccuracies.

Ensure erasure or destruction of the data is in line with the SDS Retention Schedules.

Data subjects are entitled to access personal data on them that is processed by SDS. The SDS Data Protection Subject Access Procedure details how SDS must handle requests for personal data.

Ensure personal data is properly classified in line with the SDS Information Classification and Handling Policy.

Provide other employees and/or contractors with access to personal data only as required in relation to the purpose for which it was obtained.

Ensure personal data is stored in a secure manner, whether on computer or in hard copy.

Ensure opinions and expressions of intent are recorded in a way that would not cause embarrassment in the event of the data subject requesting access.

Remember that any reference to individuals in e-mails or correspondence is covered by GDPR, and take appropriate care in relation to both content and who can see such communications.
Ensure data subjects have the opportunity to opt in of any proposed or potential direct marketing. This is an absolute right provided by GDPR in most situations, but does not apply to SDS statutory services to young people.

Sharing Personal Data with Consultants, Contractors and Partners

In all cases where consultants or contractors are granted access to personal data, whether the processing of that data is the main purpose of the contract or incidental to it, the contract must include reference to the consultant's or contractor's obligations under the GDPR, including their responsibility to maintain confidentiality. In addition, if the contractor is responsible for IS systems which process personal data on behalf of the SDS, mandatory specific reference in the contract to the need for adequate technical security over this data will be required. Advice on contract terms can be obtained from the Procurement team. Individual contractors engaged specifically for data processing roles involving the handling of personal data should be briefed on the implications of the GDPR and this policy.

Personal data may be shared with partner organisations where this is necessary in relation to the purpose for which the data was obtained, and in line with the relevant notification. Where a situation is identified where the sharing of personal data would be advantageous, but was not envisaged when the data was originally obtained, the consent of the data subjects should normally be obtained. Any new arrangements for sharing personal data with partners should be notified to the Data Protection Officer to ensure SDS's GDPR documentation set is updated.

Disclosure of Personal Data to the Police and Statutory Agencies

SDS may receive requests for the disclosure of personal data from the Police, the Child Support Agency, HMRC, Jobcentre Plus or other statutory agencies. In some cases, we may be obliged to provide the information and in others disclosure is permissible if certain conditions are met. All request should be passed to the DP team.

Transfer of Personal Data Abroad

Data should not be transferred to any country or territory outside the European Economic Area[1] unless that country or territory has legislation which offers adequate protection for data, or at least one of certain other conditions is met. The ones most likely to apply are the consent of the data subject or that the transfer is necessary under a contractual obligation. All transfers of data abroad must be notified and approved by the DPO.

[1] Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Republic of Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, The Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, UK.

Publishing

Images and recordings of identifiable individuals constitute personal data in terms of GDPR. Photographs, video and audio recordings of individuals should not be published in any material including promotional material or displayed on web sites, or in any other way made public without the consent of the individual concerned. In terms of GDPR, publishing on the internet is regarded as worldwide transfer. Further advice can be obtained from the Data Protection Officer.

Collection of Personal Data via the Internet

All SDS's websites must feature the corporate Privacy Statement. At any point where personal data is collected on-line there should be a link to this Privacy Statement.

The data collection screen should make mandatory only those fields which are necessary in relation to the purpose for which the data is being collected, and should make clear that completion of any other fields is optional. The screen, or a preceding screen, should make clear what will be done with the data, if this is not obvious. If it is intended to use the data for future marketing, an opt-in of such use must be provided. Further advice can be obtained from the Data Protection Officer.

HR Records

SDS HR records include Recruitment and Selection, Employment Records, Equal Opportunities and Monitoring Records and Information on Employee's Health, e.g. occupational health records. Employees have the right to access their HR record. The SDS Data Protection Subject Access Procedure details how SDS must handle requests for personal data.

Special category data

GDPR defines a category of data called Special Category data. This is because special category data is more sensitive, and so needs more protection. For example, information about an individual's:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation.

What are the additional conditions for processing special category data?

The conditions are summarised as:

(a) the data subject has given explicit consent
(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law;
(c) 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;
(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim;
(e) processing relates to personal data which are manifestly made public by the data subject;
(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
(g) processing is necessary for reasons of substantial public interest;
(h) 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;
(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices;
(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

In SDS it is anticipated that the conditions most likely to apply are explicit consent of the data subject, legal employment obligation, equal opportunities monitoring and other legislation (Post 16 Act).

In addition to ensuring that the pre-conditions are met, it is important to ensure appropriate security and confidentiality when processing special category data. In relation to equal opportunities monitoring, this involves limiting access to this data to the parties who undertake this monitoring. For example, in a recruitment situation monitoring data should be collected on a separate form which is not made available to the people making the selection of candidates for interview or carrying out the interviews.

New Uses of Personal Data

Whenever a new IT system or business process which involves personal data is established, the Information Asset Owner should notify the Data Protection Officer to ensure that the GDPR documentation set is updated accordingly.

Systems and process owners should also notify the Data Protection Officer if amendments are made to existing systems or processes involving the introduction of new classes of data subject or data, or new recipients of personal data.

The project SRO must consider privacy by design principles for new or amended system that process personal information. The SRO must complete a Privacy impact assessment screening questions checklist and provide to the DPO. If the assessment indicates that a PIA is required this must be done at the initiation of the project and the finding of the PIA shared with the DPO.

Personal Data Breach

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

The GDPR introduces a duty on all organisations to report certain types of personal data breach to the ICO. You must do this within **72 hours** of becoming aware of the breach, where feasible.

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. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

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.

If you become aware of a possible personal data breach you must contact the DP team immediately so that a decision on whether the ICO needs to be notified can be made.

7. Further guidance

Further information on GDPR:

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

Email the SDS Data Protection Officer:- **DPO@sds.co.uk**