

Serco Education / Adult Skills for Work Data Protection Policy

Version history				
Version	Date	Reason for release / version update	Amendments	Issued by
1.0	15.09.2021	First release		Emmanuelle Masquelier-James
2.0	17.08.2022	Annual review	N/A	Emmanuelle Masquelier-James

Document approval		
Job Role	Name	Date approved
Head of Serco Education	Anne Thomas	17 th August 2022

This policy should be read in conjunction with the following Serco Group's Standard Operating Procedures:

Doc Ref:	Title	Location
SMS GSOP-S1-3	Data Protection	MySerco

This policy should also be read in conjunction with Serco Education's *Information Classification, Handling, Retention and Disposal* policy.

Policy Statement

Serco Education and ASW need to collect and use certain types of applicants about applicants, learners, employers, employees and other stakeholders for a variety of business purposes.

This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards and comply with the Data Protection Act 1998 and General Data Protection Regular (GDPR) from May 2018.

Scope

This policy applies to all Serco Education and ASW staff.

This policy supplements other Serco policies relating to information classification, data protection and internal and email use.

Procedures

Fair and lawful processing

Serco Education and ASW will process personal data fairly and lawfully in accordance with individuals' rights. This generally means that we should not process personal data unless the individual whose details we are processing has consented to this happening.

The Data Protection Officer's Responsibilities

- Keeping the Serco board updated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures and policies on a regular basis
- Arranging data protection training and advice for all staff members
- Answering questions on data protection from staff, board members and other stakeholders
- Responding to individuals such as clients and employees who wish to know which data is being held on them by Serco Education and/or ASW

Responsibilities of the IT Manager

- Ensure all systems, services, software and equipment meet acceptable security standards
- Checking and scanning security hardware and software regularly to ensure it is functioning properly
- Researching third-party services, such as cloud services the company is considering using to store or process data

Responsibilities of the Marketing Manager

- Approving data protection statements attached to emails and other marketing copy
- Addressing data protection queries from clients, target audiences or media outlets
- Coordinating with the DPO to ensure all marketing initiatives adhere to data protection laws and the company's Data Protection Policy

Responsibilities of Coaches

- To support the learner to evidence the apprenticeship standard in a way which does not include sensitive information, such as business or client confidential information, customer personal data, or recordings of customer observation
- In the event of a learner submitting documentation that has not been de-sensitised, to ensure that the documentation is removed from the system and deleted confidentially
- To ensure the learner is not disadvantaged by the End Point Assessment Organisation due to the removal of such information

Processing of all data must be

- Necessary to deliver our services
- In our legitimate interests and not unduly prejudice the individual's privacy
- In most cases this provision will apply to routine business data processing activities.

Our website contains a Privacy Notice on data protection ([Serco Employment, Skills and Enterprise - privacy policy \(serco-ese.com\)](https://www.serco-ese.com/privacy-policy)).

The notice

- Sets out the purposes for which we hold personal data
- Highlights that our work may require us to give information to third parties
- Provides that customers have a right of access to the personal data that we hold about them

Sensitive Personal Data

In most cases where we process sensitive personal data, we will require the data subject's explicit consent to do this unless exceptional circumstances apply or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work or safeguarding). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

Accuracy and Relevance

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the DPO.

Staff Personal Data

All staff must take reasonable steps to ensure that the personal data we hold about you is accurate and updated as required. For example, if your personal circumstances change, please inform your Line Manager so that they can update your records.

Data security

All staff must keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the DPO will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third party organisations.

Storing Data Securely

- In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it
- Printed data should be shredded when it is no longer needed

- Data stored on a computer should be protected by strong passwords that are changed regularly. We encourage all staff to use a password manager to create and store their passwords.
- Data stored on CDs or memory sticks must be locked away securely when they are not being used
- Data should only be stored on designated drives and servers, and should only be uploaded on approved cloud computing services
- Servers containing personal data must be kept in a secure location, away from general office space
- Data should be regularly backed up in line with the company's backup procedures
- Data should never be saved directly to mobile devices such as laptops, tablets or smartphones
- All servers containing sensitive data must be approved and protected by security software and strong firewall.

Data Use

- When working with personal data, employees should ensure the screens of computers are locked when left unattended
- Personal data should not be shared informally. In particular, it should never be sent by e-mail, as this form of communication is not secure
- Data must be encrypted before being transferred electronically
- Personal data should never be transferred outside of the European Economic Area
- Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data

Data retention

Serco Education and ASW staff must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines.

Our contracts with the Education and Skills Funding Agency stipulate specific timeframes that data must be held for auditing purposes.

Data Accuracy

The law requires Serco Education and ASW to take reasonable steps to ensure data is kept accurate and up to date. The more important it is that the personal data is accurate, the greater the effort Serco Education and ASW will make into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

Subject access requests

Under the Data Protection Act 1998, individuals are entitled, subject to certain exceptions, to request access to information held about them. Such as

- Ask what information the company holds about them and why
- Ask how to gain access to it
- Be informed how to keep it up to date
- Be informed how the company is meeting its data protection obligations

Subject access requests from individuals should be made by email and addressed to the DPO.

The DPO can supply a standard request form, although individuals do not have to do this. Individuals will be charged £10 per subject access request. The DPO will aim to provide the relevant data in 14 days.

The DPO will always verify the identity of anyone making a subject access request before handing over any information.

Processing data in accordance with the individual's rights

All staff should abide by any request from an individual not to use their personal data for direct marketing purposes and notify the DPO about any such request.

Please contact the DPO for advice on direct marketing before starting any new direct marketing activity.

Staff Training

All staff receive training on GDPR and how to protect our information. New employees receive training as part of the induction process. Further training is on an annual basis or whenever there is a substantial change in the law or our policy and procedure.

Training is provided through in-house CBTs.

General Staff Guidelines

- The only people able to access data covered by this policy should be those who need it for their work
- Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below:
 - In particular, strong passwords must be used and they should never be shared.
 - Personal data should not be disclosed to unauthorised people, either within the company or externally.
 - Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.

- Employees should request help from their line manager or the DPO if they are unsure about any aspect of data protection

GDPR Provisions

Privacy Notice

Being transparent and providing accessible information to individuals about how we will use their personal data is important for our organisation. The following are details on how we collect data and what we will do with it:

- What information is being collected?
- Who is collecting it?
- How is it collected?
- Why is it being collected?
- How will it be used?
- Who will it be shared with?
- Identity and contact details of any data controllers
- Details of transfers to third country and safeguards
- Retention Period

Conditions for processing

We will ensure any use of personal data is justified using at least one of the conditions for processing and this will be specifically documented. All staff who are responsible for processing personal data will be aware of the conditions for processing. The conditions for processing will be available to data subjects in the form of a privacy notice.

Justification for personal data

We will process personal data in compliance with all six data protection principles. We will document the additional justification for the processing of sensitive data and will ensure any biometric and genetic data is considered sensitive.

Consent

The data that we collect is subject to active consent by the data subject. This consent can be revoked at any time.

Criminal record checks

Any criminal record checks are justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject.

Data portability

Upon request, a data subject should have the right to receive a copy of their data in a structured format. These requests should be processed within one month, provided there is no

undue burden and it does not compromise the privacy of other individuals. A data subject may also request that their data is transferred directly to another system. This must be done for free.

Right to be forgotten

A data subject may request that any information held on them is deleted or removed, and any third parties who process or use that data must also comply with the request.

International data transfers

No data may be transferred outside of the EEA without first discussing it with the data protection officer.

Specific consent from the data subject must be obtained prior to transferring their data outside the EEA.

Data audit and register

Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

Reporting breaches

All members of staff have an obligation to report actual or potential data protection compliance failures.

This allows us to investigate the failure and take remedial steps if necessary.

Monitoring

Everyone must observe this policy. The DPO has overall responsibility for this policy. They will monitor it regularly to make sure it is being adhered to.