GDPR / Data Protection Policy

Our Commitment:

Skills Office Network (SON) is committed to the protection of all personal and sensitive data for which it holds responsibility as the Data Controller and the handling of such data in line with the General Data Protection (GDPR) and Data Protection Act 2018

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

Changes to data protection legislation shall be monitored and implemented in order to remain compliant with all requirements.

The member(s) of staff responsible for data protection is James Neilands, Director.

SON is also committed to ensuring that its' staff are aware of GDPR & data protection policies, legal requirements and adequate training is provided to them.

The requirements of this policy are mandatory for all staff employed by SON and any third party contracted to provide services within the organisation.

Notification:

Our data processing activities will be registered with the Information Commissioner's Office (ICO) as required of a recognised Data Controller. Details are available from the ICO: https://ico.org.uk/about-the-ico/what-we-do/register-of-data-controllers/

Changes to the type of data processing activities being undertaken shall be notified to the ICO and details amended in the register.

Breaches of personal or sensitive data shall be notified immediately to the individual(s) concerned and the ICO.

Personal and Sensitive Data:

All data within SON's control shall be identified as personal, sensitive or both to ensure that it is handled in compliance with legal requirements and access to it does not breach the rights of the individuals to whom it relates.

The definitions of personal and sensitive data shall be as those published by the ICO for guidance: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

The principles of the GDPR & Data Protection Act shall be applied to all data processed by SON to ensure that it is:

1. **Processed fairly and lawfully.**
   SON will make all reasonable efforts to ensure that individuals who are the focus of the personal data (data subjects) are informed of the identity of the data controller, the purposes of the processing, any disclosures to third parties that are envisaged; given

an indication of the period for which the data will be kept, and any other information which may be relevant.

2. **Obtained only for lawful purposes and is not further used in any manner incompatible with those original purposes.**
   SON will ensure that the reason for which it collected the data originally is the only reason for which it processes those data, unless the individual is informed of any additional processing before it takes place.

3. **Accurate and, where necessary, kept up to date.**
   SON will not seek to collect any personal data which is not strictly necessary for the purpose for which it was obtained. Forms for collecting data will always be drafted with this mind. If any irrelevant data are given by individuals, they will be destroyed immediately.

4. **Adequate, relevant and not excessive in relation to the purposes for which it is processed**.
   SON will review and update all data on a regular basis. It is the responsibility of the individuals giving their personal data to ensure that this is accurate, and SON should be notified if, for example, a change in circumstances mean that the data needs to be updated. It is the responsibility of SON to ensure that any notification regarding the change is noted and acted on.

5. **Not kept for longer than is necessary for those purposes.**
   SON will not retain personal data for longer than is necessary to ensure compliance with the legislation, and any other statutory requirements. SON will undertake a regular review of the information held and implement a data weeding process.

   SON will dispose of any personal data in a way that protects the rights and privacy of the individual concerned (e.g. secure electronic deletion, shredding and disposal of hard copy files as confidential waste).

6. **Processed in accordance with the rights of data subjects under the Data Protection Act 2018 & GDPR Regulations, in respect of receiving privacy information, and access, rectification, deletion and portability of personal data.**
   SON will only process personal data in accordance with individuals' rights, in line with legislation, including rights to:
   - be told the nature of the information SON holds and any parties to whom this may be disclosed.
   - prevent processing likely to cause damage or distress.
   - prevent processing for purposes of direct marketing.
   - be informed about the mechanics of any automated decision-making process that will significantly affect them.
   - not have significant decisions that will affect them taken solely by automated process.
   - sue for compensation if they suffer damage by any contravention of the legislation.
   - take action to rectify, block, erase or destroy inaccurate data.
   - request that the Office of the Information Commissioner assess whether any provision of the Data Protection Act has been contravened.

7. **Protected by appropriate technical and organisational measures against unauthorised or unlawful processing and against accidental loss, destruction or damage.**
   All members of staff are responsible for ensuring that any personal data which they hold is kept securely and not disclosed to any unauthorised third parties.

   SON will ensure that all personal data is accessible only to those who have a valid reason for using it and will have appropriate security measures in place e.g.
   - keeping all personal data in a lockable cabinet with controlled access.
   - password protecting personal data held electronically.
   - archiving personal data which are then kept securely.
   - ensuring that PC screens are not left unattended without a password protected screensaver being used.

8. **Not transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection of the personal information.**
   SON will not transfer data to such territories without the explicit consent of the individual.

   This also applies to publishing information on the Internet. SON will always seek the consent of individuals before placing any personal data (including photographs) on its website.

   If SON collects personal data in any form via its website, it will provide a clear and detailed privacy statement prominently on the website, and wherever else personal data is collected.

To ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, SON shall implement appropriate technical and organisational measures, employing the following approach recommended by the ICO as appropriate:

- We undertake an analysis of the risks presented by our processing and use this to assess the appropriate level of security we need to put in place.

- When deciding what measures to implement, we take account of the state of the art and costs of implementation.

- We have an information security policy (or equivalent) and take steps to make sure the policy is implemented.

- Where necessary, we have additional policies and ensure that controls are in place to enforce them.

- We make sure that we regularly review our information security policies and measures and, where necessary, improve them.

- We have put in place basic technical controls such as those specified by established frameworks like Cyber Essentials.
- We understand that we may also need to put other technical measures in place depending on our circumstances and the type of personal data we process.
- We use encryption and/or pseudonymisation where it is appropriate to do so.
- We understand the requirements of confidentiality, integrity and availability for the personal data we process.
- We make sure that we can restore access to personal data in the event of any incidents, such as by establishing an appropriate backup process.
- We conduct regular testing and reviews of our measures to ensure they remain effective, and act on the results of those tests where they highlight areas for improvement.
- Where appropriate, we implement measures that adhere to an approved code of conduct or certification mechanism.
- We ensure that any data processor we use also implements appropriate technical and organisational measures.

Fair Processing / Privacy Notice:

We shall be transparent about the intended processing of data and communicate these intentions via notification to staff, learners and organisations prior to the processing of individual's data.

Notifications shall be in accordance with ICO guidance and, where relevant, be written in a form understandable by those defined as young adults or adults under the legislation.
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

When processing sensitive data, SON ensure that individuals are fully informed of the intended processing and obtain agreement without having any undue influence exerted upon them. Consent obtained on the basis of misleading information will not be a valid basis for processing. Consent cannot be inferred from the non-response to a communication.

The intention to share data relating to individuals to an organisation outside of our organisation shall be clearly defined within notifications and details of the basis for sharing given. Data will be shared with external parties in circumstances where it is a legal requirement to provide such information.

Any proposed change to the processing of individual's data shall first be notified to them.

Data Security:

In order to assure the protection of all data being processed and inform decisions on processing activities, we shall undertake an assessment of the associated risks of proposed processing and equally the impact on an individual's privacy in holding data related to them.

Risk and impact assessments shall be conducted in accordance with guidance given by the ICO:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

Security of data shall be achieved through the implementation of proportionate physical and technical measures. Nominated staff shall be responsible for the effectiveness of the controls implemented and reporting of their performance.

The security arrangements of any organisation with which data is shared shall also be considered and these organisations shall provide evidence of the competence in the security of shared data.

Data Access Requests (Subject Access Requests):

All individuals whose data is held by us, has a legal right to request access to such data or information about what is held. We shall respond to such requests within 40 days and they should be made in writing to: James Neilands, Director at Skills Office Network

A charge may be applied to process the request.

https://ico.org.uk/media/for-organisations/documents/1131/definition-document-colleges-of-further-education.pdf

Photographs and Video:

Images of staff and learners may be captured at appropriate times and as part of training activities. Consent of use of any images will be obtained and a record of consent stored.

Unless prior consent from learners or staff has been given, we shall not utilise such images for publication or communication to external sources.

It is our policy that external parties may not capture images of staff or learners during such activities without prior consent.

Data Disposal:

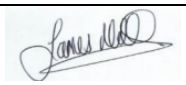
Our organisation recognises that the secure disposal of redundant data is an integral element to compliance with legal requirements and an area of increased risk.

All data held in any form of media (paper, tape, electronic) shall only be passed to a disposal partner with demonstrable competence in providing secure disposal services.

All data shall be destroyed or eradicated to agreed levels meeting recognised national standards, with confirmation at completion of the disposal process.

Disposal of IT assets holding data shall be in compliance with ICO guidance: https://ico.org.uk/media/for-organisations/documents/1570/it_asset_disposal_for_organisations.pdf

When required Skills Office Network will identify a qualified source for disposal of IT assets and collections and make the required individuals aware.

Version Number	V4
Approved by (Director Name)	James Neilands
Director Signature	
Date	24/01/2024