SCLS Data Protection Policy (GDPR) 2023-2024

Date reviewed: July 2023
Next review date: July 2024

CONTENTS

1. INTRODUCTION 3

2. RESPONSIBILITIES 4-6

3. REPORTING A DATA BREACH …….6

3. DISCIPLINARY ISSUES …….....6

1. Introduction

To meet the General Data Protection Regulation (GDPR), which came into force in May 2018, all organisations handling personal data need to have the right governance measures in place.

Sefton Community Learning Service recognises that the correct handling of data is important to the reputation of the Service and will provide for a successful working environment. The Service's reputation and future growth are dependent on the way the Service manages and protects Personal Data.

The Service is under a legal obligation to keep all personal data secure and to only keep it for as long as it is required. As an organisation that collects and uses Personal Data, Sefton Community Learning Service takes seriously its obligations to keep that Personal Data secure and to deal with security breaches relating to Personal Data when they arise.

This Policy applies to all Service employees including consultants, contractors and temporary staff hired to work on behalf of the Service.

The Sefton Community Learning Data Protection Policy must be read and adhered to in conjunction to our Privacy Statement and Sefton MBC's Corporate Data Protection policy and procedures. These are available on the Intranet: (available from the office if you don't have access to intranet)

http://intranet.smbc.loc/our-council/data-protection-information-handling.aspx

This Policy (and the other policies and documents referred to in it) sets out the basis on which the Service will collect and use Personal Data. It also sets out rules on how the Service handles, uses, transfers and stores Personal Data.

This Policy applies to all Personal Data (any information that identifies or could be linked to an individual) stored electronically, in paper form, or otherwise. The types of individuals who may be in-scope include learners, prospective learners, employees and visitors. Data which does not include information about identifiable living individuals is not subject to data protection legislation.

All information relating to identifiable individuals must be kept secure at all times. Managers must take steps to ensure that office environments and working practices take account of the security necessary to prevent the loss, theft, damage or unauthorised access to data, subject and other personal information. The Service must ensure that all documents are stored appropriately and destroyed appropriately at the point that the funding bodies require this should be a minimum of six years from the end of the financial year the last payment is made.

2. Staff General Obligations

In line with Sefton MBC Corporate Data Protection policy, all staff must complete a mandatory yearly training programme which includes maintaining awareness of data protection, confidentiality and security issues for all staff. A compliance register will be maintained by the Safeguarding Lead.

Staff will receive a copy of this policy during their Induction process and may receive periodic revisions of this Policy. Any breach of these policies will be treated seriously and may result in disciplinary action being taken.

All staff is obliged to familiarise themselves and comply with the content of this policy and the content of Sefton Metropolitan Borough Council Corporate Data Protection policy and procedures to ensure that they keep confidential all Personal Data that they collect, store, use and come into contact with during the performance of their duties.

2.1 All staff must:

- keep up to date with data compliance regulations and legislation.
- complete adequate training in relation to data protection.
- be aware of their responsibilities regarding security, data protection and confidentiality issues
- not release or disclose any Personal Data without specific authorisation from their manager and the individual concerned. This includes by phone calls or in emails.
- take all steps to ensure there is no unauthorised access to Personal Data whether by colleagues who are not authorised to see such Personal Data or by people outside the Service, by checking the identity of individuals visiting premises, and locking away paper records when not in use.
- take extra care when transporting documents which include Personal Data. Staff must use a lockable case to transport enrolment/exam registration forms from outreach to/from the centre.
- use one of the Service's phones to contact learners. Mobile phones are available to use for this purpose. Learners' contact details are kept secured in a locked cabinet in the main office.
- dispose safely all documents containing personal data.
- use the BCC (blind copy) section if sending a global email to personal emails, so individual email addresses are not displayed.
- lock computer screens when leaving their desks (even for a short period of time)

- cover any documents containing personal data when leaving their desks unattended (even for a short period of time).
- store register folders, and any other documents with Personal Data, in a locked cabinet at the end of the day.
- not leave notes or note pads with personal data on their desks. Notes must be used, stored securely or destroyed.
- not leave notes/documents containing personal data on colleagues' desks when absent. If there is a message with personal contact details, this information must be emailed to the relevant person.
- not store Personal Data on unsecured removable media.
- not share passwords with others.
- report all actual and potential incidents to their line manager.

2.2 In addition, Main Office staff must:

- remove completed enrolment forms, and other documents with learners' details, from the register folders in a timely manner, and store them securely.
- maintain good levels of privacy when dealing with enquiries from the office window. Speak quietly and ask visitors to write down personal details.
- comply with Sefton Borough Council clear desk policy.
- ensure emails are sent to securely to the intended recipient/s, using Egress if attachments contain Personal Data.
- ensure Personal Data is securely archived.
- not keep personal data longer than is necessary for the purpose or purposes for which it was collected. When no longer needed, a shredder machine must be used to dispose of documents containing Personal Data.
- ensure copies of this policy and of the Service Privacy Statement are available in public display areas.

2.3 Tutors must:

- return register folders promptly to the main office where they will be stored securely in a locked cupboard.
- always keep documents with Personal Data secure, taking extra care when carrying folders. Tutors must use a lockable case to transport enrolment/exam registration forms from outreach to/from the centre.
- not keep learners' Personal Data on unsecured personal devices.
- make learners aware of this policy and of our Privacy Statement.

2.4 Managers must:

- ensure all staff have completed Data Protection training.
- assess the risk of the premises where their staff works which includes completing penetration tests annually and conducting regular checks on data security as part of Observations and Walkthroughs, taking immediate remedial action when needed.

3. Reporting a breach

Please note that at the first indication of a data breach or suspected data breach all personnel must contact their line manager immediately. Immediately after being informed of a data breach or suspected data breach by a member of staff managers must inform the Head of Service.

4. Disciplinary issues

A deliberate or reckless breach of this policy and data protection regulations could result in a member of staff facing disciplinary action. Managers must ensure that all staff familiarise themselves with the content of this policy.

All personal data recorded in any format must be handled securely and appropriately, and staff must not disclose information for any purpose outside their normal work role. Any deliberate or reckless disclosure of information by a member of staff will be considered as a disciplinary issue. Employees should be aware that it is a criminal offence deliberately or recklessly to disclose personal data without the authority of Sefton Council.