Centre For Self Managed Learning

Information Security Policy

POLICY DOCUMENT 7	
Title	**Information Security Policy**
Approved by	Board of Trustees
Date approved	31 August 2023
To be reviewed	Every 2 years, on legislative changes or in the event of a serious incident
Review history	31 August 2023
Owner	Chair of Trustees
Where to be published (website/private)	Website

1.0 Purpose

1.1 This policy describes how all data is managed, see the Data Protection Policy for compliance with the General Data Protection Regulation.

1.2 The Chair of Governors or delegated person (hereafter referred to as "the Chair"), is responsible for ensuring the Self-Managed Learning College (hereafter referred to as “the College”) adheres to this policy. The Chair of Trustees is responsible for data maintained for purposes unrelated to the college.

2.0 Policy Statement

2.1 The aim of this policy is:

- To make sure the charity knows what its information assets are and where they are stored.
- To keep the information secure and accessible only to those who need it.
- To have processes in place so that data is not lost in the event of a system or device failure.

3.0 Information Asset Register

3.1 Information used by the charity for its main projects and regular activities are valuable assets. A list of the assets is maintained, as a minimum this must be:

- The Data Processing Register (see the Data Protection Policy)
- Finance and employment records
- Any data relating to the day to do running of the charity or charity project.

4.0 Information Classification

4.1 For the purposes of information security, the charity has chosen to classify its information in the following way:

- Public: available to any member of the public without restriction.
- Open: available to any authenticated member of the College.
- Confidential: available only to specified members, with appropriate authorisation.
- Sensitive and Confidential: available to only a very small number of members, with appropriate authorisation.

4.2 Any information which is disclosable under the Freedom of Information Act 2000 will be classified as public.

4.3 Any data which is classified as sensitive personal data by legislation will be classified as confidential.

4.4 Any information which is not explicitly classified will be classified as open, by default.

5.0 Using, storing and transferring information

5.1 Charity information will be protected and kept safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

- Preference is given to storing and transferring data using secure electronic means.

- Where possible personal information is stored on the SML College online administration platform.
- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing personal data must not be left on office and classroom desks, pinned to notice/display boards, or left anywhere else where there is general access. An exception to this may be where the well-being of the student outweighs the individual rights e.g. specific allergy information – provided documentation exists to justify this decision then this is allowable.
- Where personal information in paper format needs to be taken off site, Learning Advisers must notify the Learning Support Officer and/or Chair.
- Computer screens on which confidential or sensitive information is processed or viewed will be sited in such a way that they cannot be viewed by unauthorised persons and all computers will be locked while unattended.

6.0 Electronic Device Security

6.1 Any stakeholders who have access to confidential data must confirm the following on an annual basis:

- They have a Firewall switched-on on all the device(s) they use to access charity data.
- They have anti-virus operational on all the devices they use to access charity data and that the software is automatically updated.
- All the devices and software they use to store and transfer data uses end to end encryption
- They follow good practices for creating and maintaining passwords, https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/use-a-strong-and-separate-password-for-email

7.0 Data Backup and Disaster Recovery

7.1 It is the charities policy to use reputable cloud-based systems where data backup and disaster recovery is managed by the service provider.

7.2 Where data is not stored in such a system as described in 7.1 an alternative backup and system recovery must be put in place. Where backups are stored off site, appropriate security measures must be taken to protect against unauthorised disclosure or loss. This process is documented and referenced in the Information Asset Register,

8.0 Disposal of records

8.1 Confidential data that is no longer needed will be disposed of securely. Confidential data that has become inaccurate or out of date will also be disposed of securely, where there is not a need to rectify or update it.

8.2 Paper-based records will be shredded or incinerated.

8.3 Electronic files will be overwritten or deleted.

8.4 When PC, Laptop, Mobile Phone, USB sticks or other electronic equipment is disposed of the hard drives and memory components must be re-formatted to permanently erase the data. Just deleting files in not sufficient for disposing of confidential information.

9.0 Data Breach

9.1 For data breaches involving personal data follow the procedure in the Data Protection Policy.

9.2 Data breach that do not involve personal data it must be reported to the Chair of Trustees within 72 hours. Following a risk assessment of the breach it may be reported to the following organisations:

a. Action Fraud https://www.actionfraud.police.uk/
b. ICO https://ico.org.uk/for-organisations/report-a-breach/
c. Charity Commission https://www.gov.uk/guidance/how-to-report-a-serious-incident-in-your-charity

10.0 Ransomware Policy

10.1 All infected devices are to be wiped and data restored following disaster recovery processes if required.

11.0 Related Policies

- 17 Data Protection Policy
- 18 Privacy Notice

12.0 Review

12.1 This policy will be reviewed as and when the legislation changes or after a significant change in operations of the Charity or a significant incident, but no less frequently than every 2 years.