Centre For Self Managed Learning

Data Protection Policy

POLICY DOCUMENT 17	
Title	**Data Protection Policy**
Approved by	Board of Trustees
Date approved	22 July 2021
To be reviewed	Every 3 years, on legislative changes or in the event of a serious incident
Review history	28 July 2020
Owner	Chair of Trustees
Where to be published (website/private)	Website

1.0 Purpose

1.1 The use of all personal data by the Centre for Self Managed Learning Limited (hereafter referred to as "the Charity") is governed by The General Data Protection Regulation (GDPR) and UK Data Protection Act 2018 (DPA)

1.2 This policy applies to all personal data, regardless of whether it is in paper or electronic format.

1.3 The Self-Managed Learning College (hereafter referred to as "the College") is the primary project of the charity, the procedures specific to the college are detailed in the Appendices:

1. Key Information
2. Subject Access Requests
3. Data Processed on the basis of Consent
4. Personal Data Breach Procedure

1.4 This policy applies to all individuals working (paid or voluntary) on behalf of the charity and/or college (hereafter referred to as "adult stakeholders"). Those who do not comply with this policy may face disciplinary action and/or breach of contract penalties.

1.5 This document is based on the following source material:

- https://www.nicva.org/resource/data-protection-policy
- https://gdpr.algolia.com/
- https://ico.org.uk/

2.0 Policy Statement

2.1 GDPR is based on six data protection principles that must be complied with. This policy sets out how the Charity aims to comply with these principles. The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

2.2 Personal data will only be processed when there is one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- processing is necessary for compliance with a legal obligation to which the controller is subject;
- processing is necessary in order to protect the vital interests of the data subject or of another natural person;

- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

2.3 The vast majority of data collected or processed by the charity will fall within the "performance of a contract" basis. This is the data needed by the College to be able to provide our contractual services to others. It is also the data needed to receive contractual services from others.

2.4 If the charity wishes to collect or process data that is not required to fulfil a contractual obligation, then consent should be obtained and used as the legal basis. (e.g. detailed information about siblings of a student, surveys to past students, marketing questionnaires to prospective students). See appendix 2 Data Processed on the basis of Consent, for more details.

2.5 If the charity plans to collect or process data under one of the remaining 4 lawful bases, specialist advice must be sought.

3.0 Defining the terms and scope

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: ● Name (including initials) ● Identification number ● Location data ● Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: ● Racial or ethnic origin ● Political opinions ● Religious or philosophical beliefs ● Trade union membership ● Genetics ● Health – physical or mental ● Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.

Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4.0 Responsibilities

4.1 All members of adult stakeholders must comply with these procedures for processing or transmitting personal data.

4.2 If you have access to personal:

- Always treat people's personal information with integrity and confidentiality. Don't hand out personal details just because someone asks you to.
- Know what the data protection principles are and apply them
- Store hard copies securely and transfer them directly to recipients
- Use your encrypted USB drives to store and transfer data where needed
- If you have an organisational email address and remote access, always use it rather than personal email or taking copies of data.
- Be alert to cyberattacks and report suspicious emails or calls
- Contact the person responsible for Data Protection (see section 4.3.1 and 4.4) in the following circumstances:
    - You have any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - You are aware that this policy is not being followed
    - If you are unsure whether or not they have a lawful basis to use personal data in a particular way
    - Immediately, if there has been a data breach

4.3 The Charity

4.3.1 The Board of Trustees has overall responsibility for ensuring compliance with all relevant data protection obligations.

- The Chair of Trustees is the person responsible for Data Protection relating to the Charity
- The Trustees will monitor compliance with the GDPR and DPA across the charity
- The Trustees will be the first point of contact for the ICO and for individuals whose data is processed directly by the Charity

4.4 The College

4.4.1 The Board of Trustees delegates responsibility for ensuring the colleges compliance with all relevant data protection obligations.

- The Chair of Governors or delegated person (hereafter referred to as "the Chair"), is responsible for Data Protection relating to the college
- The Chair will monitor compliance with the GDPR and DPA within the college
- The Chair will be the first point of contact for individuals whose data is processed directly by the college.
- The Chair will escalate data protection risks and concerns to the Board of Trustees

5.0 The Data Processing Register

5.1 The Charity and the College will maintain a Data Processing Register as required by Article 30 of the GDPR to document regular processing activities. The register is maintained at the highest appropriate level and must contain:

- A description of the personal data
- The classification level (public, open, confidential, strictly confidential)
- The lawful basis on which the data is held and processed
- The purpose for which it was collected
- How the data will be kept up to date
- How it will be determined that it is no longer needed and is to be deleted.
- Where it is stored and the security of the location
- The internal roles or individuals who have access to it
- External organisations with whom it is shared with on a regular basis (for each organisation confirmation that they adhere to GDPR and DPA is maintained)

6.0 Sharing Personal Data

6.1 The charity nor the college will not normally share personal data with anyone else, but may do so where:

- There is an issue with a data subject that puts their safety, or the safety of those around them, at risk
- There is a need to liaise with other agencies. Consent will be sought before doing this, unless there is a legal requirement for us to share the data, this includes for:
    - The prevention or detection of crime and/or fraud
    - The apprehension or prosecution of offenders
    - The assessment or collection of tax owed to HMRC
    - In connection with legal proceedings
    - Where the disclosure is required to satisfy safeguarding obligations
    - Research and statistical purposes, as long as personal data is sufficiently anonymised
- Suppliers or contractors need data to enable the charity to provide its contractual obligations, for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide reasonable guarantees that they comply with data protection law

- Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data shared between us
- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with the Charity

7.0 Information Security

Personal data must be protected and kept safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage. All adult stakeholders must adhere to the guidance in the Information Security Policy.

8.0 Related Policies

- 17 Information Security Policy
- 18 Privacy Notice

9.0 Review

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.

APPENDICES

APPENDIX 1: Subject Access Requests

SUBJECT ACCESS REQUESTS

The information in this procedure must be read in partnership with section 9 “Your Rights” of the Privacy Notice.

Individuals have a right to make a ‘subject access request’ to gain access to personal information that SML College holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this is not possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests must be submitted in writing to the Chair. A request should include:

- Name of individual
- Contact details to be able to respond to the request (correspondence address/email address/phone number)
- Details of the information requested

If Learning Advisers receive a subject access request, they must immediately forward it to the C Chair

CHILDREN AND SUBJECT ACCESS REQUESTS

Personal data about a child belongs to that child, and not the child’s parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests for this age range from parents or carers of these students may be granted without the express permission of the student.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of Students at SML College may not be granted without the express permission of

the pupil. This is not a rule and a student's ability to understand their rights will always be judged on a case-by-case basis.

RESPONDING TO SUBJECT ACCESS REQUESTS

When responding to requests, the College:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is
- complex or numerous. We will inform the individual of this within 1 month, and explain why the
- extension is necessary

Information will not be disclosed if it:

- Might cause serious harm to the physical or mental health of the student or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, the College may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information.

When refusing a request, the individual will be told why and that they have the right to complain to the ICO.

OTHER DATA PROTECTION RIGHTS OF THE INDIVIDUAL

In addition to the right to make a subject access request (see above), and to receive information when College is collecting their data about how it is used and processed, individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask for their personal data to be rectified, erased, restricted in its processing, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances

- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

PARENTAL REQUESTS TO SEE THE STUDENT/CHILD'S RECORD

Parents, or those with parental responsibility, may make a request for access to their child's record for students under the age of 18. SML College defines the data held on a child's educational record as:

- Records of any academic achievements
- Correspondence concerning the student from adults within SML College, local authorities, employees and educational psychologists engaged by SML College.
- Information from the pupil and their parent(s).

It does not include information about the student

- That the college employees or Learning Advisers keep solely for their own use.
- Provided by the parent of another child.

It should be noted that:

- there is no automatic right to see records;
- requests are not covered by the Data Protection Act and are separate from Subject Access Requests;

Information will not be disclosed if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

the law relating to such requests is not regulated by the ICO.

Response times and format:

- a response will be given without delay and normally within 15 working days of receipt of the request;
- responses will be given via email.

Requests specifically relating to student records must be submitted in writing to the Chair of Governors. A request should include:

- Name of pupil/student
- Contact details of the parent/carer to be able to respond to the request (correspondence address/email address/phone number)
- That the request is for a student record

APPENDIX 2: Data Processed on the basis of Consent

At the point of the first collection of personal data directly from individuals, the relevant information required by data protection law will be provided (e.g. the privacy notice).

The following processes are followed when data is collected under the basis of consent.

PHOTOGRAPHS AND VIDEOS

College activities may include photographing and recording images of individuals. Consent will be obtained from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. This will be immediately requested via our online e-forms available on Care Monkey

It will be clearly explained how the photograph and/or video will be used to both the parent/carer and pupil. Uses may include:

- Within SML College on display boards and any published newsletters, etc.
- Outside of SML College by external agencies such as any hired photographer, newspapers, campaigns
- Online on the SML Website or the SML social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, photographs or video will be deleted and not distributed further.

Photographs and videos used in this way will not be accompanied with any other personal information about the child, to ensure they cannot be identified.

APPENDIX 3: Personal Data Breach Procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

When appropriate, the data breach will be reported to the ICO within 72 hours of the moment a breach is identified, including weekends and holidays. Such breaches may include, but are not limited to:

- Safeguarding information being made available to an unauthorised person
- The theft of a SML College laptop containing non-encrypted personal data about pupils
- The loss or theft of paper files or USB containing any personal data

PROCEDURE

- On finding or causing a breach, or potential breach, any adult or Learning Adviser must immediately notify the Chair of Governors
- The Chair of Governors will investigate the report and determine whether a breach has occurred. To decide, they will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- The Chair of Governors will alert the Board of Trustees
- The Trustees will advise on all reasonable measures to contain and minimise the impact of the breach, assisted by relevant adults or data processors where necessary.
- The Chair of Governors will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The Chair of Governors, along with the Trustees will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, they will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

If it is likely that there will be a risk to people's rights and freedoms, the Trustees must notify the ICO.

- The Trustees will document the decision (either way) in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions will be securely stored
- Where the ICO must be notified, the Trustees will do this via the 'report a breach' page of the ICO website within 72 hours. As required, this will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
    - The name and contact details of the Chair of Governors, as well as the relevant Trustees
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and
    - mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the Trustees will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when they expect to have further information. The trustees will submit the remaining information as soon as possible
- The Trustees will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the Trustees, along with the Chair of Governors, will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the those monitoring.
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The Trustees will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.
- The Chair of Governors, along with the Trustees will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more
    - robust processes or providing further training for individuals)
- The Chair of Governors, along with the Trustees will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

ACTIONS TO MINIMISE THE IMPACT OF DATA BREACHES

All actions to mitigate the impact of different types of data breach will be taken, focusing especially on breaches involving particularly risky or sensitive information. The effectiveness of these actions will be reviewed and amended as necessary after any data breach.