1.	**Policy, scope and objectives**
1.1	The Management of CSEP is committed to compliance with all relevant UK and EU laws in respect of personal data, and to protect the "rights and freedom" of individuals whose information CSEP collects in accordance with General Data Protection Regulation (GDPR). To that end the Management, Directors and Board of Trustees has developed, implemented, maintained and continuously improves a documented Personal Information Management Systems (PIMS) for CSEP.
1.2 Scope	The scope of the PIMS takes into account organisational structure, management responsibility, jurisdiction and geography. The PIMS may include the whole of CSEP or a defined part of CSEP.
1.3 Objectives of the PIMS	CSEP's objectives for the PIMS are that it should enable CSEP to: • meet its own requirements for the management of personal information; • support organisational objectives and obligations; • impose controls in line with CSEP's acceptable statutory, regulatory, contractual and/or professional duties; • protect the interest of individuals and other key stakeholders.
1.4	CSEP is committed to complying with data protection legislation and good practice including a. processing personal information only where this is strictly necessary for legitimate organisational purposes; b. collecting only the minimum personal information required for these purposes; c. providing clear information to individuals about how their personal information will be used and by whom; d. only processing relevant and adequate personal information; e. processing personal information fairly and lawfully; f. maintaining an inventory of the categories of personal information processed by CSEP; g. keeping personal information accurate and, where necessary, up to date; h. retaining personal information only for as long as is necessary for legal or regulatory reasons or, for legitimate organisational purposes; i. respecting individual's rights in relation to their personal information, including their right of subject access;

	j. keeping all personal information secure; k. only transferring personal information outside the EU in circumstances where it can be adequately protected; l. the application of various exemptions allowed by data protection regulation; m. developing and implementing a PIMS to enable the policy to be implemented; n. where appropriate, identifying internal and external stakeholders and the degree to which these stake holders are involved in the governance of CSEP's PIMS and; o. Identification of workers with specific responsibility and accountability for PIMS.
1.5 Notification	
2.	**<u>Background to the General Data Protection Regulation ('GDPR')</u>** The GDPR 2016 replaces the EU Data Protection Directives of 1995 and supersedes the laws of individual Member States that were developed in compliance with the Data Protection Directives 95/46 EC. Its purpose is to protect the "rights and freedom" of living individuals, and to ensure that personal data is not processed without their knowledge, and wherever possible, that it is processed with their consent.
3.	**<u>Definition used by the organisation (drawn from the GDPR)</u>** **Territorial scope** – the GDPR will apply to all controller that are established in the EU (European Union) who process the personal data of data subjects, in the context of that establishment. It will also apply to controllers outside the EU that process personal data in order to offer goods and services, or monitor the behaviour to data subjects who are resident in the EU. **Establishment** – the main establishment of the controller in the EU will be the place in which the controller makes the main decisions as to the purpose of its data processing activities. The main establishment of a processor in the EU will be its administrative centre. If a controller is based outside the EU, it will have to appoint a representative in the jurisdiction in which the controller operates, to act on behalf of the controller and deal with supervisory authorities. **Personal data** – any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one

who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identifiable number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special categories of personal data – Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data controller – the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Data subject – any living individual who is the subject of personal data held by an organisation.

Processing – any operation or set of operations which is performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Profiling – is any form of automated processing of personal data intended to evaluate certain personal aspect relating to a natural person, or to analyse, or predict that person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour. This definition is linked to the right of data subject to object to profiling and the right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

Personal data breach – a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or personal data transmitted, stored or otherwise processed. There is an obligation on the controller to report personal data breach to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject.

Data subject consent – means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he

	or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data. **Child** – the GDPR defines a child as anyone under the age of 16 years old. **Third party** – a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data. **Filing system** – any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.
4.	**Responsibilities under the GDPR**
4.1	CSEP is a data controller under the GDPR.
4.2	Top management and all those in management or supervisory roles throughout CSEP are responsible for developing and encouraging good information handling practices within the organisation; responsibilities are set out in individual job descriptions.
4.3	GDPR Owner, a member of the senior management team, is accountable to the Board of Directors/Management of CSEP for the management of personal information within CSEP and for ensuring that compliance with data protection legislation and good practice can be demonstrated. This accountability includes: • development and implementation of the PIMS as required by this policy; and • security and risk management in relation to compliance with the policy.
4.4	The Project Manager takes responsibility for CSEP's compliance with this policy on a day-to-day basis and, in particular, has direct responsibility for ensuring that CSEP complies with the GDPR, as do the Education Officer / Trustees / Directors) in respect of data processing that takes place within their area of responsibility.
4.5	The Data Protection Manager/GDPR Owner have specific

	responsibilities in respect of procedures such as the Subject Access Request Procedure (GDPR doc 2.2) and are the first point of call for members seeking clarification on any aspect of data compliance.
4.6	Compliance with data protection legislation is the responsibility of all members of CSEP who process personal information.
4.7	CSEP's Training Policy (GDPR doc 2.3) sets out specific training and awareness requirements in relation to specific roles and to members of CSEP generally.
4.8	Members of CSEP are responsible for ensuring that any personal data supplied by them, and that is about them, to CSEP is accurate and up-to-date.
5.	**Risk Assessment** Objective: To ensure that CSEP is aware of any risks associated with the processing of particular types of personal information. CSEP has a process for assessing the level of risk to individuals associated with the processing of their personal information. Assessment will also be carried out in relation to processing undertaken by other organisations on behalf of CSEP. CSEP shall manage any risks which are identified by the risks assessment in order to reduce the likelihood of a non-conformance with this policy. Appropriate controls will be selected from ISO 27001 and applied to reduce the level of risks associated with processing individual data to an acceptable level, by reference to CSEP's documented risk acceptance criteria and the requirements of GDPR.
6.	**Data protection principles** All processing of personal data must be done in accordance with the following data protection principles of the Regulation, and CSEP' policies and procedures are designed to ensure compliance with them.
6.1	Personal data must be processed lawfully, fairly and transparently. CSEP's Fair Processing Procedure

The GDPR introduces the requirement for transparency whereby the controller has transparent and easily accessible policies relating to the processing of personal data and the exercise of individuals "right and freedom". Information must be communicated to the data subject in an intelligible form using clear and plain language.

The specific information that must be provided to the data subject must as a minimum include:

6.1.1	The identity and the contact details of the controller and, if any, of the controller's representatives;
6.1.2	The contact details of the Data Protection Officer/GDPR Owner/Communication Lead, where applicable;
6.1.3	The purpose of the processing for which the personal data are intended as well as the legal basis for the processing;
6.1.4	The period for which the personal data will be stored;
6.1.5	The existence of the rights to request access, rectification, erasure or object to the processing;
6.1.6	The categories of personal data concerned;
6.1.7	The recipients or categories of recipients of the personal data, where applicable;
6.1.8	Where applicable, that the data controller intends to transfer personal data to a recipient in a third country and the level of protection afforded to the data;
6.1.9	Any further information necessary to guarantee fair processing.

6.2	Personal data can only be collected for specified, explicit and legitimate purposes.	
6.3	Personal data must be adequate, relevant and limited to what is necessary for processing.	
	6.3.1	Jacinth Martin is responsible for ensuring that information which is not strictly necessary for the purpose for which it is obtained, is not collected.
	6.3.2	All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must be approved by the Project Manager
	6.3.3	The Project Manager will ensure that on an annual basis all data collection methods are reviewed to ensure that collected data continues to be adequate, relevant and not excessive.
	6.3.4	If data is given or obtained that is excessive or not specifically required by CSEP's documented procedures, The Project Manager is responsible for ensuring that it is securely deleted or destroyed.
6.4	Personal data must be accurate and kept up to date.	
	6.4.1	Data that is kept for a long time must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate.
	6.4.2	The Project Manager is responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it.
	6.4.3	It is also the responsibility of individuals to ensure that data held by CSEP is accurate and up-to-date. Completion of an appropriate registration or application form etc. will be taken as indication that the data contained therein is accurate at the date of submission.

	6.4.4	Members should notify CSEP of any changes in circumstances to enable personal records to be updated accordingly. It is the responsibility of CSEP to ensure that any notification regarding change of circumstances is noted and acted upon.
	6.4.5	The Project Manager is responsible for ensuring that appropriate additional steps are taken to keep data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors.
	6.4.6	On at least an annual basis, the Project Manager will review all the personal data maintained by CSEP, by reference to the Data Inventory Register, and will identify any data that is no longer required in the context of the registered purpose and will arrange to have that data securely deleted/destroyed.
	6.4.7	The Project Manager is responsible for making appropriate arrangements that, where third party organisations may have been passed inaccurate or out-of-date personal information, of informing them that the information is inaccurate and/or out-of-date and is not to be used to inform decisions about the individuals concerned; and for passing any correction to the personal information to the third party where this is required.
6.5	<u>Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing.</u>	
	6.5.1	Where personal data is retained beyond the processing date, it will be minimised in order to protect the identity of the data subject in the event of a data breach.
	6.5.2	Personal data will be retained in line with the retention of records procedures and, once its retention date is passed, it must be securely destroyed.

	6.5.3 The Project Manager must specifically approve any data retention that exceeds the retention periods and must ensure that the justification is clearly identified.
6.6	Personal data must be processed in a manner that ensure security
6.7	Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data against accidental loss or destruction of, damage to, personal data.
6.8	Personal data shall not be transferred to a country or territory outside the European Union unless that country or territory ensures an adequate level of protection for the 'rights and freedom' of data subjects in relation to the processing of personal data.
6.9	Accountability The GDPR introduces the principle of accountability which states that the controller is not only responsible for ensuring compliance but for demonstrating that each processing operation complies with the requirement of the GDPR.
7	**Data subjects' rights** Data subjects have the following rights regarding data processing, and the data that is recorded about them:
7.1	To make subject access requests regarding the nature of information held and to whom it has been disclosed.
7.2	To prevent processing likely to cause damage or distress.
7.3	To prevent processing for purposes of direct marketing.
7.4	To be informed about the mechanics of automated decision-making

	processes that will significantly affect them.
7.5	Not to have significant decisions that will affect them taken solely by automated processes.
7.6	To sue for compensation if they suffer damage by any contravention of the GDPR.
7.7	To take action to rectify, block, erase, including the right to be forgotten, or destroy inaccurate data.
7.8	To request the ICO to assess whether any provision of the GDPR has been contravened.
7.9	The right for personal data to be provided to them in a structured, commonly used and machine-readable format, and the right to have the data transmitted to another controller.
7.10	The right to object to any automated profiling without consent. Data subject may make data access request as described in GDPR doc 2.2; this procedure also describes how CSEP will ensure that its response to the data access complies with the requirements of the regulation. <u>Complaints</u> Data subjects who wish to complain to CSEP about how their personal information has been processed may lodge their complaint directly with the Project Manager. Data subject may also complain directly to ICO and Project Manager and CSEP must provide appropriate contact details. Where data subjects wish to complain about how their complaint has been handled, or appeal against any decision made following a complaint, they may lodge a further complaint to the Project Manager (The right to do this should be included in the GDPR section of CSEP's complaints procedures).
8.	**<u>Consent</u>**

	CSEP understand 'consent' to mean that it has been explicitly and freely given, specific, informed and unambiguous indication of the data subject's wishes by which he/she by statement, or by a clear affirmative action, signifies agreement to the processing of personal data relating to him/her. The consent of the data subject can be withdrawn at any time. CSEP understand 'consent' to mean that data subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing. There must be some active communication between the parties which demonstrate active consent. Consent cannot be inferred from non-response to a communication. For sensitive data, explicit written consent of data subject must be obtained unless alternative legitimate bases for processing exists. In most instances consent to process personal and sensitive data is obtained routinely by CSEP using standard consent documents e.g. when registering a new member.
9.	**<u>Security of data</u>** All members are responsible for ensuring that any personal data which CSEP holds and for which they are responsible, is kept securely and is not under any condition disclosed to any third party unless that third party has been specifically authorised by CSEP to receive that information and has entered into a confidentiality agreement. All personal data should be accessible only to those who need to use it, and access may only be granted in line with the Access Control Policy. You should form a judgement based upon the sensitivity of the information in question, but personal data must be kept: • In a lockable room with controlled access; and/or • In a lockable drawer or filing cabinet; and/or • If computerised, password protected in line with corporate requirements in Access Control Policy; and/or • Stored on (removable) computer media which are encrypted. Care must be taken to ensure that PC screens and terminals are not visible except to authorised members of CSEP. All members are required to enter into an Acceptable Use Agreement before they are given access to organisational information of any sort. Manual records may not be left where they can be accessed by

	unauthorised personnel and may not be removed from business premises without explicit (written) authorisation. As soon as manual records are no longer required for the day-to-day member support, they must be removed. Processing of personal data 'off site' present a potentially greater risk of loss, theft or damage to personal data. Members must be specifically authorised to process data off-site.
10.	**Right of access to data** Data subjects have the rights to access any personal data (i. e. data about them) which is held by CSEP in electronic format and manual records which form part of a relevant filing system. This includes the right to inspect confidential personal references received by CSEP, and information obtained from third-party organisations about that person. Subject Access Requests are dealt with as described in GDPR doc 2.2.
11.	**Disclosure of data** CSEP must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the police. All members should exercise caution when asked to disclose personal data held on another individual to a third party (and will be required to attend specific training that enables them to deal effectively with any such risk). It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of CSEP's business. The GDPR permits certain disclosure without consent so long as the information is requested for one or more of the following purposes: • To safeguard national security; • Prevention or detection of crime including the apprehension or prosecution of offenders; • Assessment or collection of tax duty; • Discharge of regulatory functions (including health, safety and welfare of persons at work); • To protect the vital interest of the individual, this refers to life and death situations. All requests to provide data for one of these reasons must be

	supported by appropriate paperwork and all such disclosures must be specifically authorised by the Data Protection Manager/GDPR Owner.
12.	**<u>Retention and disposal of data</u>** Personal data may not be retained for longer than it is required. Once a member has left CSEP, it may not be necessary to retain all the information held on them. Some data will be kept for longer periods than others. CSEP's data retention and data disposal procedures will apply in all cases. **Disposal of records** Personal data must be disposed of in a way that protects the "rights and freedom" of data subjects (e. g. shredding, disposal as confidential waste, secure electronic deletion and in line with the secure disposal procedure.

Document Owner and Approval

Jacinth Martin is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the review requirement stated above.

A current version of this document is available to all members and on the CSEP website.

Issue	Description of change	Approval	Date Issue
1	Initial	Jacinth Martin	04/04/2019

Name: **Jacinth Martin, Project Manager**
Address: **CSEP, 32-34 Sydenham Rd, Croydon, CR0 2EF**
Telephone number: 0208 686 7865
Email: info@csep.org.uk