



## DATA PROTECTION POLICY

Owner: John Vago, ICT Manager

Approver: Management Team

Date	Document Version	Draft / Final	Distribution	Comment
2009	2.1	Final	All staff & volunteers	
Feb 2010	2.2	Final	All staff & volunteers	Add email monitoring section
April 2013	2.3	Final	All staff & volunteers	Minor update
August 2014	3.0	Final	All staff & volunteers	Rewritten
Nov 14	3.1	Final	All staff & volunteers	Encryption information
Oct 17	4.1	Final	All staff & volunteers	Updated
Jun 2018	5.0	Final	GDPR working party	Rewritten
Jul 2018	5.1	Final	All staff & volunteers	Minor update

# DATA PROTECTION POLICY

## 1. Aim

seAp Advocacy obtains, uses, stores and otherwise processes personal data relating to potential, current and former staff, volunteers and clients, contractors, website users and other contacts, collectively referred to in this policy as data subjects. When processing personal data, seAp is obliged to fulfil individuals' reasonable expectations of privacy by complying with GDPR and other relevant data protection legislation (data protection law), and aims to treat all personal information with the respect.

This policy therefore seeks to ensure that we:

1. are clear about how personal data must be processed and the seAp's expectations for all those who process personal data on its behalf;
2. comply with the data protection law and with good practice;
3. protect the seAp's reputation by ensuring the personal data entrusted to us is processed in accordance with data subjects' rights
4. protect seAp from risks of personal data breaches and other breaches of data protection law.

The main terms used are explained in the glossary at the end of this policy (Appendix 3).

## 2. Scope

This policy applies to all personal data we process regardless of the location where that personal data is stored (e.g. on an employee's own device) and regardless of the data subject. All staff and others processing personal data on the seAp's behalf must read it. A failure to comply with this policy may result in disciplinary action.

Information compliance staff - seAp's Data Protection Officer (DPO) is John Vago, ICT Manager, contacted at [info@seap.org.uk](mailto:info@seap.org.uk). Day to day administration of data protection issues is handled by the Data Support Officer. Clarification on any issues relating to this policy can be provided by either post holder or the Resources Manager.

## 3. Information Commissioner's Office

seAp is registered with the Information Commissioner's Office (Registration No. Z9231372) and information about data privacy rights can be found on the Commissioner's website.

## 4. Personal data protection principles

When you process personal data, you should be guided by the following principles, which are set out in the GDPR. seAp is responsible for, and must be able to demonstrate compliance with, the data protection principles listed below:

Those principles require personal data to be:

1. processed lawfully, fairly and in a transparent manner (Lawfulness, fairness and transparency). Detail on how to achieve this can be found in Appendix 1.
2. collected only for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes (Purpose limitation). Detail on how to achieve this can be found in Appendix 2.

3. adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data minimisation). Detail on how to achieve this can be found in Appendix 2.
4. accurate and where necessary kept up to date (Accuracy). Detail on how to achieve this can be found in Appendix 2.
5. not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the personal data is processed (Storage limitation). Detail on how to achieve this can be found in Appendix 2.
6. processed in a manner that ensures its security, using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage (Security, integrity and confidentiality). Detail on how to achieve this can be found in Appendix 2.

## **5. Data Subjects' Rights**

Data subjects have rights in relation to the way we handle their personal data. These include the following rights:

1. where the legal basis of our processing is Consent, to withdraw that Consent at any time;
2. to ask for access to the personal data that we hold (see below);
3. to prevent our use of the personal data for direct marketing purposes
4. to object to our processing of personal data in limited circumstances
5. to ask us to erase personal data without delay:
  - a. if it is no longer necessary in relation to the purposes for which it was collected or otherwise processed;
  - b. if the only legal basis of processing is Consent and that Consent has been withdrawn and there is no other legal basis on which we can process that personal data;
  - c. if the data subject objects to our processing where the legal basis is the pursuit of a legitimate interest or the public interest and we can show no overriding legitimate grounds or interest;
  - d. if the data subject has objected to our processing for direct marketing purposes;
  - e. if the processing is unlawful.
6. to ask us to rectify inaccurate data or to complete incomplete data;
7. to restrict processing in specific circumstances e.g. where there is a complaint about accuracy;
8. to ask us for a copy of the safeguards under which personal data is transferred outside of the EU;
9. the right not to be subject to decisions based solely on automated processing, including profiling, except where necessary for entering into, or performing, a contract, with seAp; it is based on the data subject's explicit consent and is subject to safeguards; or is authorised by law and is also subject to safeguards;
10. to prevent processing that is likely to cause damage or distress to the data subject or anyone else;

11. to be notified of a personal data breach which is likely to result in high risk to their rights and freedoms;

12. to make a complaint to the Information Commissioner's Office (ICO) the independent authority set up to uphold data privacy for individuals.

13. in limited circumstances, receive or ask for their personal data to be transferred to a third party (e.g. when a new provider takes on an existing contract provided by seAp) in a structured, commonly used and machine readable format.

You must verify the identity of an individual requesting data under any of the rights listed

Requests (including for data subject access – see below) must be complied with, usually within one month of receipt. You must immediately forward any Data Subject Access Request you receive to the Data Support Officer. A charge can be made for dealing with requests relating to these rights only if the request is excessive or burdensome.

## **6. Accountability**

seAp must implement appropriate technical and organisational measures in an effective manner to ensure compliance with data protection principles. seAp is responsible for, and must be able to demonstrate compliance with, the data protection principles.

We must therefore apply adequate resources and controls to ensure and to document GDPR compliance including:

- (a). appointing a suitably qualified Data Protection Officer (DPO);
- (b). implementing Privacy by Design when processing personal data and completing a Data Protection Impact Assessment (DPIA) where processing presents a high risk to the privacy of data subjects;
- (c). integrating data protection into our policies and procedures, in the way personal data is handled by us and by producing required documentation such as Privacy Notices, Records of Processing and records of Personal Data Breaches;
- (d). training staff on compliance with Data Protection Law and keeping a record accordingly; and
- (e). regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, and where improvements can take place.

## **7. Responsibilities**

### **7.1. seAp responsibilities**

seAp is responsible for establishing policies and procedures in order to comply with data protection law either as a Data Controller or Data Processor dependent upon the activity being performed and any contract that provides the lawful basis for that activity.

### **7.2. Data Protection Officer (DPO responsibilities)**

The DPO is responsible for:

- (a) advising seAp and its staff of its obligations under GDPR
- (b) monitoring compliance with this Regulation and other relevant data protection law, seAp's policies with respect to this and monitoring training and audit activities relate to GDPR compliance

- (c) to provide advice where requested on data protection impact assessments
- (d) to cooperate with and act as the contact point for the Information Commissioner's Office
- (e) the data protection officer shall have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

### 7.3. Staff responsibilities

Staff members who process personal data about clients, staff, or any other individual must comply with the requirements of this policy. Staff members must ensure that:

- (a) all personal data is kept securely;
- (b) no personal data is disclosed either verbally or in writing, accidentally or otherwise, to any unauthorised third party;
- (c) personal data is kept in accordance with seAp's retention schedule and any specific contract for services under which the data has been collected;
- (d) any queries regarding data protection, including subject access requests and complaints, are promptly directed to the Data Protection Officer;
- (e) any data protection breaches are swiftly brought to the attention of the Data Protection Officer and that they support Information Compliance staff in resolving breaches;

Staff who are unsure about who are the authorised third parties to whom they can legitimately disclose personal data should seek advice from their line manager or Information Compliance staff.

### 7.4. Third-Party Data Processors

Where partners are used to process personal data on behalf of seAp, responsibility for the security and appropriate use of that data remains with seAp.

Where a third-party data processor is used:

- (a) a data processor must be chosen which provides sufficient guarantees about its security measures to protect the processing of personal data;
- (b) reasonable steps must be taken that such security measures are in place;
- (c) a written contract establishing what personal data will be processed and for what purpose must be set out;
- (d) a data processing agreement, available on the Infostore, must be signed by both parties.

For further guidance about the use of third-party data processors please contact Information Compliance staff.

### 7.5. Contractors, Placements and Volunteers

SeAp is responsible for the use made of personal data by anyone working on its behalf. Managers who employ contractors, short term or voluntary staff must ensure that they are appropriately vetted for the data they will be processing and complete the appropriate confidentiality and other documents. In addition, managers should ensure that:

- (a) any personal data collected or processed in the course of work undertaken for seAp is kept securely and confidentially;

(b) all personal data is returned to seAp on completion of the work, including any copies that may have been made. Alternatively, that the data is securely destroyed and seAp receives notification in this regard from the contractor or short term / voluntary member of staff;

(c) seAp receives prior notification of any disclosure of personal data to any other organisation or any person who is not a direct employee of the contractor;

(d) any personal data made available by seAp, or collected in the course of the work, is neither stored nor processed outside the UK unless written consent to do so has been received from seAp;

(e) all practical and reasonable steps are taken to ensure that contractors, short term or voluntary staff do not have access to any personal data beyond what is essential for the work to be carried out properly.

## **8. Data Subject Access Requests**

Data subjects have the right to receive copy of their personal data which is held by seAp. In addition, an individual is entitled to receive further information about seAp's processing of their personal data as follows:

1. the purposes
2. the categories of personal data being processed
3. recipients/categories of recipient
4. retention periods
5. information about their rights
6. the right to complain to the ICO,
7. details of the relevant safeguards where personal data is transferred outside the EEA
8. any third-party source of the personal data

You should not allow third parties to persuade you into disclosing personal data without proper authorisation. For example, clients' parents do not necessarily have an automatic right to gain access to their son's or daughter's data.

The entitlement is not to documents per se but to such personal data as is contained in the document.

You should not alter, conceal, block or destroy personal data once a request for access has been made. You should contact ICT staff before any changes are made to personal data which is the subject of an access request.

In order to verify a Data Subject Access Request we require certain information – see the Subject Access Request Form which includes the relevant guidelines. Completion of the form itself by the data subject is not necessarily required providing we can verify their identity.

## **9. Reporting a personal data breach**

The GDPR requires that we report to the Information Commissioner's Office (ICO) any personal data breach where there is a risk to the rights and freedoms of the data subject. Where the Personal data breach results in a high risk to the data subject, the ICO also has to be notified unless subsequent steps have been taken to ensure that the risk is unlikely to materialise, security measures were applied to render the personal data unintelligible (e.g. encryption) or it would amount to disproportionate effort to inform the data subject directly. In the latter circumstances, a public communication must be made or an equally effective alternative measure must be adopted to inform data subjects, so that they themselves can take any remedial action.

seAp has put in place procedures to deal with any suspected personal data breach and will notify data subjects or the ICO where we are legally required to do so. Reports should be made using the Data Security Incident Report Form for the Data Protection Officer to access any requirements to report externally.

If you know or suspect that a personal data breach has occurred, you should immediately contact the ICT Manager and follow the instructions in the Information Security Breach Policy. The Data Support Officer will maintain a record of such breaches, as required by the GDPR.

## **10. Limitations on the transfer of personal data**

The GDPR restricts data transfers to countries outside the EU in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. We will not transfer personal data outside the EU and wherever possible look to retain data in the UK.

## **11. Record Keeping**

The GDPR requires us to keep full and accurate records of all our data processing activities and for client data this should be solely on the Microsoft Dynamics CRM. These should reflect our processing activities, including records of data subjects' Consents and procedures for obtaining Consents, where Consent is the legal basis of processing.

These records should include the name and contact details of seAp as Data Controller and the DPO, clear descriptions of the personal data types, data subject types, processing activities, processing purposes, third-party recipients of the personal data, personal data storage locations, personal data transfers, the personal data's retention period and a description of the security measures in place. They will normally be found in the specification for a particularly service and the description by seAp of how these activities are carried out.

Records of personal data breaches must also be kept, setting out:

1. the facts surrounding the breach
2. its effects; and
3. the remedial action taken

## **12. Training and Audit**

We are required to ensure that all staff undergo adequate training to enable them to comply with data protection law. We must also regularly test our systems and processes to assess compliance.

You must undergo all mandatory data privacy related training.as available on Moodle.

You must regularly review all the systems and processes under your control to ensure they comply with this policy.

Data privacy by design and default and Data Protection Impact Assessments (DPIAs)

(see Privacy Impact Statement SOP)

We are required to implement privacy-by-design measures when processing personal data, by implementing appropriate technical and organisational measures (like pseudonymisation) in an effective manner, to ensure compliance with data-protection principles. SeAp must ensure therefore that by default only personal data which is necessary for each specific purpose is processed. The obligation applies to the volume of personal data collected, the extent of the processing, the period of storage and the accessibility of the personal data. In particular, by default, personal data should not be available to an indefinite number of persons. You should ensure that you adhere to those measures.

As well as complying with seAp-wide practices designed to fulfil reasonable expectations of privacy, you should also ensure that your own data-handling practices default to privacy to minimise unwarranted intrusions in privacy e.g. by disseminating personal data to those who need to receive it to discharge their duties.

SeAp must also conduct DPIAs in respect of high-risk processing before that processing is undertaken.

You should conduct a DPIA (and discuss your findings with the DPO) in the following circumstances:

1. the use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);
2. automated processing including profiling;
3. large scale processing of sensitive (special category) data; and
4. large scale, systematic monitoring of a publicly accessible area.
5. A DPIA must include:
  6. a description of the processing, its purposes and the Data Controller's legitimate interests if appropriate;
  7. an assessment of the necessity and proportionality of the processing in relation to its purpose;
  8. an assessment of the risk to individuals; and
  9. the risk-mitigation measures in place and demonstration of compliance.

### **13. Direct Marketing**

We are subject to certain rules and privacy laws when marketing to our clients, Advocacy Training participants, and any other potential user of our services. We would not generally market directly to clients of our advocacy services.

A data subject's prior Consent is required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing customers (e.g. current clients) known as "soft opt in" allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar services (e.g. a post-graduate course or a professional qualification), and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

The right to object to direct marketing must be explicitly offered to the data subject in an intelligible manner so that it is clearly distinguishable from other information.

A data subject's objection to direct marketing must be promptly honoured. If a data subject opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

#### **14. Sharing Personal Data**

In the absence of Consent, a legal obligation or other legal basis of processing, personal data should not generally be disclosed to third parties unrelated to seAp (e.g. clients' family members, or other professionals). Normally a client will authorise any relevant correspondence with third parties.

However for non-instructed advocacy an advocate takes affirmative action with or on behalf of the client to uphold their rights and there is a legal basis under the Mental Health Act or the Mental Capacity Act to give specific powers to an advocate in these circumstances.

Partners working on the same contract to provide advocacy services will be covered by the original consent where we are working under a common brand name for the service and it is explained to the client that we are working with the partners.

Some bodies may have a statutory power to obtain information (e.g. regulatory bodies or the police). However, without a warrant, the police have no automatic right of access to records of personal data, though voluntary disclosure may be permitted for the purposes of preventing/detecting crime or for apprehending offenders. You should seek written assurances from the police that the relevant exemption applies.

Some additional sharing of personal data for research purposes may also be permissible, subject to certain safeguards

#### **15. Copyright Information**

Copyright is a legal right to control the use and exploitation of original creative material. Copyright in a work is usually owned by its creator. We need be aware of this when using non-original material such as photo and permission sought for its use. This includes consent to use a contribution from a client or other person. Copyright material such as photos, newspaper articles or other documents should not be reproduced.

#### **16. Queries about this policy**

Employees should address any enquiries relating to this policy to their line manager. In the event that a line manager is unable to resolve a query, a response should be sought from the Data Support Officer.

## **17. Accessibility, review timetable and feedback**

The current version of this policy is kept on the Infostore under Policies and Procedures/Operations and is available to all staff and volunteers. It is covered in staff and volunteer mandatory induction training and updates are communicated to staff and volunteers via the Intranet and through Staff Consultative Council (SCC) representatives and local team meetings.

It is the intention of seAp that policies and procedures remain current and 'fit for purpose' to reflect changes in legislative, organisational, operational and management arrangements. The Data Protection Policy will be reviewed annually.

If an employee has any concerns about this policy or wishes to provide feedback on the process of policy development this can be addressed either through their SCC rep or via email to the ICT Manager.

Applicable policies include those listed below. This list is not exhaustive, and will be subject to change:

Subject Access Request

Data Security Incident Report Form

Privacy Impact Statement SOP

Information Security Policy – detailing procedures followed to protect information security.

Information Security Breach Management Plan – procedures to follow in the event of an information security breach.

Confidentiality and Non-Disclosure Statement – signed by all employees and volunteers, including password security.

Confidentiality Policy – confidentiality principles and procedures to follow in the circumstances where it may be breached due to potential harm befalling the client.

ICT Acceptable Use Policy – safeguards particularly on email and social media.

Data Privacy Policy – outlines to referrers, clients, and other users of our services how we collect data and what we do with it to keep it secure, and information on their rights.

Home working Policy – safeguards for home workers.

## Appendix 1

### Principle 1 of GDPR – Processing personal data lawfully, fairly and transparently

#### 1. Lawfulness and fairness

You may only process personal data fairly and lawfully and for specified purposes. These restrictions are not intended to prevent processing, but ensure that we process personal data for legitimate purposes without prejudicing the rights and freedoms of data subjects. In order to be justified, seAp may only process personal data if the processing in question is based on one (or more) of the legal bases set out below. Section 4.3 below deals with justifying the processing of sensitive personal data. Including special category data.

The legal bases for processing non-sensitive personal data are as follows:

1. the data subject has given his or her Consent
2. the processing is necessary for the performance of a contract with the data subject (e.g. assessments carried out by Advocacy Training in order to provide the relevant qualification for which the staff member has enrolled)
3. to meet our legal compliance obligations (e.g. advocates may have specific responsibilities under the Mental Health Act).
4. to protect the data subject's vital interests (e.g. safeguarding)
5. to pursue our legitimate interests (or another's legitimate interests) which are not overridden because the processing prejudices the interests or fundamental rights and freedoms of data subjects. The specific legitimate interest or interests that seAp is pursuing when processing personal data will need to be set out in relevant Privacy Notices.

You must identify the legal basis that is being relied on for each processing activity, which will be included in the Privacy Notice provided to data subjects.

#### (a) Consent

You should only obtain a data subject's Consent if there is no other legal basis for the processing. Consent requires genuine choice and genuine control.

A data subject consents to processing of his/her personal data if he/she indicates agreement clearly either by a statement or positive action to the processing. Silence, pre-ticked boxes or inactivity are therefore unlikely to be sufficient. If Consent is given in a document that deals with other matters, you must ensure that the Consent is separate and distinct from those other matters.

Data subjects must be able to withdraw Consent to processing easily at any time. Withdrawal of Consent must be promptly honoured. Consent may need to be renewed if you intend to process personal data for a different and incompatible purpose which was not disclosed when the data subject first consented, or if the Consent is historic.

You will need to ensure that you have evidence of Consent and you should keep a record of all Consents obtained so that we can demonstrate compliance.

Consent is required for some electronic marketing and some research purposes.

#### (b) Legal bases for Processing Sensitive Personal Data, including Special Category Data

Special Category Personal Data is data revealing:

1. racial or ethnic origin
2. political opinions
3. religious or philosophical beliefs,
4. trade union membership,

It also includes the processing of:

5. genetic data
6. biometric data for the purpose of uniquely identifying a natural person,
7. data concerning health
8. data concerning a natural person's sex life or sexual orientation

Personal data relating to criminal convictions and offences including the alleged commission of offences or proceedings for offences or alleged offences should be treated in the same way to special category data.

The processing of sensitive personal data by seAp must be based on one of the following (together with one of the legal bases for processing non-sensitive personal data as listed above):

1. the data subject has given explicit Consent (requiring a clear statement, not merely an action,
2. the processing is necessary for complying with employment law;
3. the processing is necessary to protect the vital interests of the data subject or another person where the data subject is physically or legally incapable of giving Consent;
4. the processing relates to personal data which are manifestly made public by the data subject;
5. the processing is necessary for the establishment, exercise or defence of legal claims;
6. the processing is necessary for reasons of substantial public interest (provided it is proportionate to the particular aim pursued and takes into account the privacy rights of the data subject)
7. the processing is necessary for the purposes of preventive or occupational medicine, etc. provided that it is subject to professional confidentiality
8. the processing is necessary for reasons of public interest in the area of public health, provided it is subject to professional confidentiality;
9. the processing is necessary for archiving purposes, for instance in the public interest, or statistical purposes, if it is subject to certain safeguards (i.e. pseudonymisation or anonymisation where possible, the research is not carried out for the purposes of making decisions about particular individuals (unless it is approved medical research) and it must not be likely to cause substantial damage/distress to an individual and is in the public interest).

Examples of sensitive personal data processed by seAp will include:

1. details of racial/ethnic origin, sexual orientation, religion/belief for the purposes of equality monitoring.
2. details of health records for the purposes of health complaints advocacy
3. checks conducted by the Disclosure and Barring Service for the purposes of assessing eligibility of staff or clients to engage in work with children and vulnerable adults,
4. details of disability either for the purposes of monitoring client access to services or for assessing and implementing reasonable adjustments to seAp's policies, or practices

Processing sensitive personal data represents a greater intrusion into individual privacy than when processing non-sensitive personal data. You must therefore take special care when processing sensitive personal data and ensure that you comply with the data protection principles and with this policy, in particular in ensuring the security of the sensitive personal data.

## **2. Transparency (notifying data subjects)**

Under the GDPR seAp is required to provide detailed, specific information to data subjects depending on whether the information was collected directly from data subjects or from elsewhere. That information must be provided through appropriate Privacy Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a data subject can easily understand what happens to their personal data.

Whenever we collect personal data directly from data subjects, for example for the recruitment and employment of staff and for the referral and triage of clients, at the time of collection we must provide the data subject with all the prescribed information which includes:

1. SeAp's details
2. Contact details of DPO
3. Purposes of processing
4. Legal basis of processing
5. Where the legal basis is legitimate interest, identify the particular interests (e.g. marketing, fundraising)
6. Where the legal basis is Consent, the right to withdraw
7. Where statutory/contractual necessity, the consequences for the Data Subject of not providing the data of non-provision

When personal data is collected indirectly (for example, from a third party or publically available source), you must also provide information about the categories of personal data and any information on the source. The data subject must be provided with all the information required by the GDPR as soon as possible after collecting/receiving the data. You must also check that the personal data was collected by the third party in accordance with the GDPR and on a basis which contemplates our proposed processing of that personal data (rather than for an entirely different reason).

## **Appendix 2**

### **Principle 2 of GDPR - Purpose Limitation**

Personal data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.

You cannot therefore use personal data for entirely new, different or incompatible purposes from those disclosed when it was first obtained unless you have informed the data subject of the new purposes. Where the further processing is not based on the data subject's Consent or on a lawful exemption from data-protection law requirements, you should assess whether a purpose is incompatible by taking into account factors such as:

1. the link between the original purpose/s for which the personal data was collected and the intended further processing
2. the context in which the personal data has been collected – in particular seAp to data subject relationship. You should ask yourself if the data subject would reasonably anticipate the further processing of his/her personal data
3. the nature of the personal data in particular whether it involves special categories of personal data (i.e. sensitive) or personal data relating to health conditions, etc.
4. the consequences of the intended further processing for the data subjects
5. the existence of any appropriate safeguards e.g. encryption or pseudonymisation.

Provided that prescribed safeguards are implemented, further processing for statistical or research purposes will not be regarded as incompatible. Safeguards include ensuring data minimisation (e.g. pseudonymisation or anonymisation where possible), the research will not be carried out for the purposes of making decisions about particular individuals and it must not be likely to cause substantial damage/distress to an individual.

### **Principle 3 of the GDPR – Data minimisation**

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. You should not therefore amass large volumes of personal data that are not relevant for the purposes for which they are intended to be processed. Conversely, personal data must be adequate to ensure that we can fulfil the purposes for which it was intended to be processed.

You may only process personal data when performing your job duties requires it and you should not process personal data for any reason unrelated to your job duties.

You must ensure that when personal data is no longer needed for specified purposes, it is deleted or anonymised in accordance with seAp's data retention policy and schedule.

### **Principle 4 of the GDPR - Accuracy**

Personal data must be accurate and, where necessary, kept up to date. You should ensure that personal data is recorded in the correct files.

Incomplete records can lead to inaccurate conclusions being drawn and where there is such a risk, you should ensure that relevant records are completed.

You must check the accuracy of any personal data at the point of collection and at regular intervals thereafter. You must take all reasonable steps to destroy or amend inaccurate records without delay and you should up-date out-of-date personal data where necessary (e.g. where it is not simply a historical record).

Where a data subject has required his/her personal data to be rectified, you should inform recipients of that personal data that it has been rectified..

### **Principle 5 of the GDPR – Storage limitation**

You must not keep personal data in a form that allows data subjects to be identified for longer than needed for the legitimate business purposes or other purposes for which seAp collected it. Those purposes include satisfying any legal, accounting or reporting requirements. Records of personal data can be kept for longer than necessary if anonymised.

You will take all reasonable steps to destroy or erase from seAp's systems all personal data that we no longer require in accordance with the records retention schedules and policies.

You will ensure that data subjects are informed of the period for which their personal data is stored or how that period is determined in any relevant Privacy Notice.

### **Principle 6 of the GDPR – Security, Integrity and Confidentiality**

seAp is required to implement and maintain appropriate safeguards to protect personal data, taking into account in particular the risks to data subjects presented by unauthorised or unlawful processing or accidental loss, destruction of, or damage to their personal data. Safeguarding will include the use of encryption and pseudonymisation where appropriate. It also includes protecting the confidentiality (i.e. that only those who need to know and are authorised to use personal data have access to it), integrity and availability of the personal data. We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our processing of personal data.

You are also responsible for protecting the personal data that you process in the course of your duties. You must therefore handle personal data in a way that guards against accidental loss or disclosure or other unintended or unlawful processing and in a way that maintains its confidentiality. You must exercise particular care in protecting sensitive personal data from loss and unauthorised access, use or disclosure.

You must comply with all procedures and technologies we put in place to maintain the security of all personal data from the point of collection to the point of destruction.

You must comply with all applicable aspects of our Information Security Policy, and comply with and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the Data Protection Law standards to protect personal data.

You may only transfer personal data to third-party service providers (i.e. data processors) who provide sufficient guarantees to implement appropriate technical and organisational measures to comply with Data Protection Law and who agree to act only on seAp's instructions. Data processors should therefore be appointed subject to seAp's standard contractual requirements for data processors.

Where we act as data processor for a third party such as a local authority care should be taken that we follow any specific instructions on how the data should be processed and inform the data controller in line with any reporting requirements.

## Appendix 3

### Glossary of Terms

**Anonymisation:** replacing information that directly or indirectly identifies an individual with blank spaces or meaningless data entries so that the person, to whom the data relates, cannot be identified.

**Automated Decision-Making (ADM):** when a decision is made which is based solely on automated processing (including profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not automated processing.

**Profiling:** any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, etc.

**Consent:** agreement which must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the processing of personal data relating to them.

**Data Controller:** the person or organisation that determines when, why and how to process personal data. It is responsible for establishing practices and policies in accordance with the GDPR. SeAp is the Data Controller of all personal data relating to it and used delivering advocacy and training, conducting research and all other purposes connected with delivering services.

**Data Subject:** a living, identified or identifiable individual about whom we hold personal data.

**Data Protection impact assessment (DPIA):** tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programs involving the processing of personal data.

**Data Protection Officer (DPO):** the person appointed as such under the GDPR and in accordance with its requirements. A DPO is responsible for advising seAp on its obligations under Data Protection Law, for monitoring compliance with data protection law, as well as with seAp's policies, providing advice, cooperating with the ICO and acting as a point of contact with the ICO.

**Personal Data:** any information identifying a data subject or information relating to a data subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal data includes sensitive personal data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

**Personal Data Breach:** any breach of security resulting in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or unauthorised access to, personal data, where that breach results in a risk to the data subject. It can be an act or omission.

**Privacy by Design:** implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

**Privacy Notices:** notices setting out information that may be provided to data subjects when seAp collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee, and donor privacy notices or the website privacy policy) or they may be stand-alone, one-time privacy statements covering processing related to a specific purpose.

**Processing:** any activity that involves the use of personal data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties. In brief, it is anything that can be done to personal data, including both creation and destruction.

**Pseudonymisation:** replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.