DATA PROTECTION POLICY

Including: Appendix 1 Data retention periods

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

DATA PROTECTION POLICY

1. Aim

The aim is to ensure compliance with the Data Protection Act 1998 which relates to the rights of individuals to gain access to personal information held by an organisation or individual within it, and the right to challenge the accuracy of the data held.

All staff and volunteers are required to ensure seAp's compliance with this policy when processing or communicating personal data.

The eight data protection principles require staff and others who process or use any personal information to ensure that they adhere to these principles that data should be:

- fairly and lawfully processed only if certain conditions are met
- processed for a specified and lawful purpose
- adequate, relevant and not excessive for those purposes
- accurate and kept up to date
- not kept for longer than is necessary
- processed in line with the data subject's rights
- kept safe from unauthorised access, accidental loss
- not transferred to a country outside the European Economic Area unless that country has equivalent levels of protection for personal data.

It is important that seAp has permission from the data subjects to process their data and is undertaking it for a registered purpose, in particular to ensure the rights of a data subject to access their personal data which the organisation holds, while protecting the rights of third parties.

2. Definitions

When this policy refers to "data", this applies to any information relating to an individual where the structure of the data allows information about the individual to be readily accessed. This will include written notes and records held in electronic and paper filing systems.

A "data subject" is a client, worker (employee, volunteer, placement student or agent temp) or other person or organisation that we may hold records on or communicate with.

Personal data is any data relating to a living individual (e.g. name, address, payroll details, etc.).

Sensitive data forms a subset of personal data and records such things as ethnic origin, religious beliefs, health criminal convictions, etc.

Data processing occurs whenever data is compiled, stored, or otherwise operated on.

Data controller is the person or organisation processing the data.

3. Registration

Under the Act seAp as a data controller is required to notify the Information Commissioner of certain details of the processing of personal data. Failure to keep the register entry up to date is a criminal offence.

Our registration entry Z9231372 summarises the reasons that we process data for advocacy and other services, the type of information we process, who this is about and with who we might share this information. Where we provide West Berkshire Healthwatch service a separate registration entry ZA144263 is held detailing the data held by this service.

4. General guidelines

4.1 Procuring personal data

Any permission to process client or staff information will be gained at the commencement of any contract, referral or agreement. This includes a completed client consent form and will include information on data protection and retention, advising clients of their rights including copies of data protection policies which are also published on the seAp website.

The Act does not allow an individual to prevent an organisation from making reasonable use of personal data in the interests of providing, for example, an advocacy service or employment.

Principle 3 of the Act requires that only necessary data should be collected i.e. that is necessary for the effective functioning of the service. Procedures should be reviewed periodically to ensure this is the case and that unnecessary information is not being requested or collected.

4.2 Storage of personal data

4.2.1 Electronic Data

All client data must be recorded on the Client Database which is a case management and reporting tool which stores all client notes and other records including uploading documents and correspondence. This is stored on seAp's central servers via secure network access.

seAp will ensure that all electronic data, including client database entries, emails and letters are accessed and secured by passwords, anti-virus, anti-spyware and firewall software. Personal data should not be stored on a local hard drive or laptop. All laptop are supplied with encryption software.

In line with the ICT policy, all database users are to keep passwords confidential. In extreme cases where it is necessary for the password to be shared, immediate steps should be taken to change the password.

As official documents, emails to any seAp staff or volunteer accounts may be accessed in the absence of the account holder by their manager for the necessary performance of work duties or as part of a Data Protection Access Request. Subject to an official request, emails may also be monitored for the purposes of quality and

monitoring performance or as otherwise specified in the ICT (Acceptable Use) Policy. All applications should be made to the ICT Manager.

4.2.2 Document Storage

Documents must be kept in a way that respects the information held:

- hard copies of data must be kept in a lockable filing cabinet or other secure storage compartment, however wherever possible documents should be uploaded to the Client Database and originals returned to the client or destroyed;
- staff must ensure that such data is not left in the sight of others and is filed when not in use;
- documents in transit should be carried securely for which lockable brief cases are provided to staff.

4.3 Updating personal data

Any changes to personal data, such as a new address, should be carried out at the first available opportunity to minimise the risk of using out of date information.

A check should be made to ensure correct personal details are current and accurate where a client reopens their case or a worker returns to the organisation after leaving.

4.4 Transferring data and use of secure email

Emails are a quick and convenient way of providing or responding to requests for information, although care must be exercised to ensure that confidential or sensitive information is kept secure, therefore it may be appropriate to use encrypted emails depending on the nature and circumstances of the communication. The email encryption system should be used where there are concerns about sending sensitive or confidential information by email. We should continue to respond to the needs of individual clients and communicate in the most appropriate way, and this is another device that allows us to respond to concerns about security or privacy.

Confidential or sensitive data should be transferred outside the organisation by safehaven fax, or for electronic data by encrypted memory stick sent by secure next day delivery post. Encrypted email should be used to send particularly sensitive client data.

4.5 Sharing data with third parties

Data must not be revealed to a third party without the data subject's express consent. However, there may be occasions where data is shared between seAp and selected partners which will be by client consent and should be formalised by agreeing any specific ground rules as illustrated in an Information Sharing: Protocol.

Requests for information should be in writing. This stipulation would only be breached in line with the specific reasons detailed in the Confidentiality Policy, for

example in order to protect the client in the event of a life-threatening situation or in issues relating to national security.

4.6 References

It is seAp's policy to provide references regarding the employment of current or past employees and volunteers when requested by another employer or potential lender. All references should remain factual and resist giving opinions of the referee or other staff members which cannot be backed up by evidence. Former or existing staff can request to see these references under the Data Protection Act. All reference requests should be directed to Human Resources for a response.

4.7 Data Protection Requests

Data subjects have the right to access personal data which is held by the organisation, both files and electronic data.

Where clients have an open file with seAp a copy of any relevant documents or of the complete file can be provided on request.

If the requests concern a closed case then an official request is needed, describing the exact request and providing proof of ID, seAp has 40 days to reply to such requests. No fee is charged for a request, although we reserve the right to make a charge where there have been multiple requests.

When fulfilling the request, seAp must take into consideration any data that has third party involvement. Data can be withdrawn if:

- the third party has not given consent for the data subject to see the data;
- the data would lead to the harm of the data subject or third party

Please refer to the Data Protection Subject Access Request Procedures, and in particular the:-
Subject Access Request Form
Subject Access Request Procedure and Guidelines

On the occasion that a relative, solicitor or other third party makes a subject access request on a subject's behalf, either because the subject lacks capacity or is deceased, seAp will require evidence that such a person is formally acting on their behalf.

Such requests will be reviewed on a case by case basis to determine whether such data can be released to the third party but will require proof of identity and a copy of power of attorney.

Where the data subject is deceased there is no automatic right to supply information, however where the individual can provide a copy of their own proof of identity and the grant of probate or certificated copy of the last will and testament, their request will be considered.

4.8 Protecting third parties

In meeting a data subject access request it is important that personal data relating to other identifiable individuals mentioned in the documents should not be revealed unless permission for disclosure is given by the individuals concerned. The data subject enquirer has a right to see comments made about them but the identity of the individual who made those comments should not be revealed without their express permission.

4.9 Secure file transfer

Transfers of sensitive information outside the organisation should normally be sent via encrypted email after first confirming the email address is the correct address of the intended recipient.

Transfers involving large amounts of data should be referred to the ICT department for support and will be via an appropriate secure file transfer method such as saving to an encrypted memory stick and couriered to the recipient, or by specific SSH Secure File Transfer set up for a specific transfer of data.

4.10 End of a contract

When a contract for services ends, there be a legal obligation on seAp to work with any new provider of the service, and seAp will work with them to ensure any open cases are transferred to the new provider providing the client or, for clients that lack capacity, the initial referrer, consents. Clients will receive written notice that a change is taking place and their consent to their data being transferred will be sought.

In the event of a loss of an existing contract or a new contract bid is successful, the terms of the contract may stipulate that the Transfer of Undertakings (Protection of Employment) Regulations 2006 (commonly known as TUPE) apply. In this situation, seAp is obliged to share/receive specific data about workers under these terms.

4.11 Data retention, archiving and destruction

Data is retained only for as long as the needs of the original consent for which it was collected and in line with any retention periods required in case of query, or to satisfy regulatory or contractual requirements.

By client information we mean any information that could identify the client as an individual or could be used to inform any decision about them.

When we no longer need to keep a client file we will delete the client's contact details, any associated documents, and any other information that could identify the client personally. We may keep other information about the case where this cannot identify the client personally but is required for contractual or operational reasons.

By deletion for electronic records we mean put "beyond use" as defined by the Data

Protection Information Commissioner's Office guidelines, and paper records are archived in secure storage and destroyed by shredding according to the time periods given in Appendix 1 – Data Retention Periods. .

5. Security breaches

Staff are required to report possible Data Protection breaches immediately to their line manager and the ICT Manager who acts as seAp's Data Protection Officer.

A Data Security Incident Reporting Form should be completed outlining the details of the incident.

seAp must report security breaches to the Information Commissioner (ICO) if it is believed that data is at risk of being misused as a result of the loss of data.

All possible breaches will be recorded by seAp. In line with the ICT and Information Security Policies, it is the employees' responsibility to inform the loss or possible loss of data to their line manager and the ICT Manager, or another senior manager within seAp.

6. 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.

7. 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.

Specific technical queries relating to ICT support should be addressed to the helpdesk ict@seap.org.uk or telephone 0845 2799007.

8. 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:

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.

Glossary of terms

Safehaven fax	A method of ensuring any personal information transmitted by fax is done so in a secure setting, i.e. the receiving fax machine is in a secure environment, or the person receiving the fax is alerted to its arrival, waits for it to arrive and confirms its receipt.
Encrypted email	An email transmitted using encryption software that is compliant with industry standards such as HIPAA (Health Insurance Portability Accountability Act) which is a United States standard for sending sensitive patient data by secure email.

Appendix 1: Data Retention Periods

seAp adheres to the statutory retention periods for worker, financial and health and safety data. Examples are outlined below:

Record	Retention period	Archiving period	Action
accident books, accident records/ reports	12 years for records relating to accident or injury at work	None	Destroy
accounting records	2 years	4 years	Destroy
Income tax and NI returns, HMRC records	2 years after the end of the financial year to which they relate	4 years	Destroy
Statutory Maternity Pay records, calculations, certificates (Mat B1s) or other medical evidence	2 years after the end of the tax year in which the maternity period ends	4 years	Destroy
Statutory Sick Pay records, calculations, certificates, self-certificates	2 years after the end of the tax year to which they relate	4 years	Destroy
Salary records (also overtime, bonuses, expenses)	2 years	4 years	Destroy

seAp also holds other data where the following retention period apply:

Record	Retention period	Archiving period	Action
Client files (21 and over)	18 Months after the closure of the file unless there is another case open with seAp or contractual requirements from funding bodies mean we have to keep this data for a longer period.	None	Destroy
Client files (under 21)	18 Months after the clients' 21st birthday if closed unless there is another case open with seAp or contractual requirements from funding bodies mean we have to keep this data for a longer period.	None	Destroy
Staff records	6 years after the worker has left	4 years	Destroy
Staff records (under 21)	6 years after the clients' 21st birthday if closed	4 years	Destroy
Grievance/disciplinary records	1 year from end of employment	5 years	Destroy
Application forms and interview notes	Duration of employment for successful application and 6 months for unsuccessful applicants	None	Destroy
Electronic timesheets/leave	3 years	None	Destroy

Meeting minutes (Board, Senior Management Team and Team)	3 years	Indefinitely	Archive store
Supervision notes	6 years after the worker has left	4 years	Destroy

Emails	1 year	2 years	Destroy
Emails (seAp Core Depts)	1 year	4 years	Destroy
Exceptional files (where criminal or other reason means they are excluded from this policy)	6 years	Indefinitely	Archive store