Service Six

CONFIDENTIALITY AND DATA PROTECTION POLICY

April 2018

Content

What this policy Covers 3
Definitions 3
- GDPR 3
- Personal Data 4
- Sensitive Personal Data 4
- Processing 4
- Data Subject 5
- Data Controller 5
- Data Processor 5
- The Caldicott Principles 5
- Records 5

Roles & Responsibilities 5
- Information Officer 6
- Data Protection Officer 6
- Chief Executive 6
- Designated Safeguarding Officer 6
- Managers 6
- Practitioners 7

Policy on Handling Data 7
- Collection and maintenance of personal information 7
- Responsibilities for managing and handling personal information 7
- Ensuring security of personal information 8

Disclosures and sharing of client information 8
- Right to be informed 8
- Right of access to data 9
- Consent 10
- Data security 10
- Retention and disposal of data 10

Access to records 10
- Who can access 10
- Records of deceased 11
- Procedure for access to records 11
- Withholding access to records 11
- Rights to amend content of records 12

Release information handling process 12
Staff & Practitioners 13
Clients 14

Disposal of records 14
Guidance for Affiliate IT Security 14
- Introduction 14
- Password Management 14
- Safe Computing 15
- Internet and Email usage 15
- Mobile Computing 16
- Removable media 16
- Media disposal 17

Summary; Confidentiality Procedures for Administration 17
- Introduction 17
- Communicating by Phone 18
- Written Communication 18
- Communication with Couples or Parents 19
- Third party contact 19
- Therapist confidentiality 19
- Complaints 19
- Scanning procedure 19

Storing Data 20
Data Breaches 20

Date: April 2018

Review Due By: April 2019

Lead Role/Manager: Chief Executive

Others involved in implementing: Managers and Personnel

What this policy covers

In its operations, Service Six has to collect and use both personal and sensitive information about people with whom it works. These may include current, past and prospective employees, clients and customers, affiliate practitioners and other suppliers and contractors. The lawful and correct treatment of this personal and sensitive information is essential to the operation of Service Six's business and the proper delivery of its services. Such information must be handled and dealt with properly, however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means.

Service Six abides by the confidentiality provisions in the British Association for Counselling and Psychotherapy's (BACP) Ethical Framework for Good Practice in Counselling and Psychotherapy. Its operations are also governed by the General Data Protection Regulations (GDPR) 2018, the Access to Health Records Act (1990) and comply with NHS Codes of Practice and the business management standard ISO 9001:2008.

Service Six will endeavor to ensure that all people involved in the delivery of its services are aware and informed of their responsibilities to treat personal and sensitive information appropriately.

This policy also details your rights and obligations in relation to your personal data and the personal data of third parties that you may come into contact with during the course of your employment.

If you have access to the personal data of employees or of third parties, you must comply with this Policy. Failure to comply with the Policy and procedures may result in disciplinary action up to and including dismissal without notice.

LINKS TO OTHER SPECIFIC THERAPEUTIC POLICIES, PROCEDURES & GUIDELINES:

- Clinical Risk Management Policy
- Disclosure and Release of Information Policy
- Retention Periods for Records Policy

DEFINITIONS

General Data Protection Regulations (GDPR) 2018

GDPR stands for General Data Protection Regulation and replaces the previous Data Protection Directives that were in place. It was approved by the EU Parliament in 2016 and comes into effect on 25th May 2018.

GDPR states that personal data should be 'processed fairly & lawfully' and 'collected for specified, explicit and legitimate purposes' and that individuals data is not processed without their knowledge and are only processed with their 'explicit' consent.

GDPR covers personal data relating to individuals. Service Six is committed to protecting the rights and

freedoms of individuals with respect to the processing of children's, parents, visitors and staff personal data.

The Data Protection Act gives individuals the right to know what information is held about them. It provides a framework to ensure that personal information is handled properly.

Service Six is registered with the ICO (Information Commissioners Office) under registration reference: Z1997473 and has been registered since 16th November 2009. Certificates are on display on the Service Six's information boards at the offices; HQ-26 Rock Street, Wellingborough, Northamptonshire, NN8 4LW and Chapter House, Coffee Hall, Milton Keynes MK6 5EE.

The act states that anyone processing personal data must comply with eight principles of good practice. These principles require that personal information:

- shall be processed fairly and lawfully and in particular, shall not be processed unless specific conditions are met;
- shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes;
- shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed;
- shall be accurate and where necessary, kept up to date;
- shall not be kept for longer than is necessary for that purpose or those purposes;
- shall be processed in accordance with the rights of data subjects under the Act;
- shall be kept secure i.e. protected by an appropriate degree of security;
- shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

The Act provides conditions for the processing of any personal data. It also makes a distinction between personal data and 'sensitive' personal data.

Personal data

Personal data is defined as, information relating to an individual who can be identified from:

- the presenting data
- the presenting data and other information, which includes an expression of opinion about the individual and any indication of intentions in respect of the individual

Sensitive personal data

Sensitive personal data is defined as personal data consisting of information as to:

- Racial or ethnic origin; Political opinion; Religious or other beliefs; Trade union membership;
- Physical or mental health or condition; Sexual life;
- Criminal proceedings or convictions.

Processing

Processing, in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:

- organisation, adaptation or alteration of the information or data,
- retrieval, consultation or use of the information or data,
- disclosure of the information or data by transmission, dissemination or otherwise making available, or
- alignment, combination, blocking, erasure or destruction of the information or data

Data Subject

Data Subject means an individual who is the subject of personal data. In other words, the Data Subject is the individual whom particular personal data is about. The Data Protection Act does not count as a Data Subject an individual who has died or who cannot be identified or distinguished from others.
Data Subject within Service Six can be clients and employees.

Data Controller

The Data Controller means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.
Data Controller within Service Six can be Service Six.

Data Processor

Data Processor, in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the Data Controller. Data Processors are not directly subject to the Act. However, most Data Processors, if not all, will be Data Controllers in their own right for the processing they do for their own administrative purposes, such as employee administration or IT.
Data Processor within Service Six can be outsources services such as HR Mentor, FUSE Collaboration Services (IT) and Consultants.

The Caldicott Principles

All client-identifiable data is held in accordance with the six principles from the Caldicott guidelines:

1. justify the purpose for using confidential information
2. only use it where necessary
3. use the minimum that is required
4. access should be on a strict 'need to know' basis
5. everyone must understand his or her responsibilities
6. understand and comply with the law

Records

Within the Freedom of Information Act a health record is defined as consisting of information relating to the physical or mental health or condition of an identifiable individual, made by or on behalf of a practitioner in connection with the care of that individual.

The Act includes health records held for NHS, independent sector and practitioners private practice records. It also applies to employers who hold information relating to the physical or mental health of their employees if the record has been made by or on behalf of a practitioner in connection with the care of the employee.

A health record can be in digital or manual format. It may include hand written clinical notes, letters to and from practitioners, outcome measures and all records of telephone contacts.

ROLES & RESPONSIBILITIES

Service Six will follow procedures to ensure that all employees, practitioners, contractors, agents, consultants, or partners who have access to any personal data held by or on behalf of Service Six, are fully aware of and abide by their duties and responsibilities under the General Data Protection Regulations (GDPR) 2018.

All employees, practitioners, contractors, agents, consultants, or partners who have access to any personal information, whether paper based or electronic, must adhere to this policy and related procedures.

Information Officer

The Information Commissioner maintains a public register of data controllers and Service Six is registered as such.

Data Controller Name:	**Service Six**
Registration No:	**Z1997473**
Security No:	**10815990**

Data Protection Officer

The Chief Executive acts as the Charity's Data Protection Officer and is responsible for notifying, updating and renewing Service Six's registration details with the Information Commissioner's Office. The Chief Executive also has responsibility for overseeing the development of policies and procedures relating to non- clinical information.

Chief Executive

Service Six's Chief Executive has overall responsibility for policies and procedures relating to clinical information and for:

- Reviewing and updating this policy;
- The development of best practice guidelines and audits to ensure adherence and compliance with statutory duties
- Any breach of confidentiality or Data Protection must be reported to the Chief Executive immediately and then by the Chief Executive to the Board of Trustees.
- Audits to ensure adherence and compliance with statutory duties

Designated Safeguarding Officer (DSO)

In practice, responsibility for therapeutic decisions relating to disclosure of information is developed to the DSO (who excercises responsibility similar to Caldicott Guardians). In the absence of the DSO, responsibility will be delegated to the other members of the Designated Safeguarding team or to the Chief Executive.

In addition, the DSO is responsible for:

- ensuring the provision of confidentiality and data protection
- training for staff; ensuring that staff are aware of and adhere to relevant policy and procedures;
- monitoring the effectiveness of this policy and raising issues requiring further attention;
- consulting with the other managers, clinical supervisors and the Executive team as necessary to support compliance.

Managers

In practice, responsibility for decisions relating to disclosure and release of information is devolved to service managers (who exercise responsibility similar to Caldicott Guardians). In addition, service managers are responsible for:

- ensuring the provision of training for staff relating to managing information; ensuring that staff are aware of and adhere to relevant policy and procedures;
- monitoring the effectiveness of this policy and raising issues requiring further attention; consulting with the clinical governance manager or other management staff/Chief Executive as necessary to support compliance.

Service managers may deputize their role to a suitably trained and qualified member of staff, who will exercise due caution in making decisions, consulting with the Operations Manager, a designated clinical lead or other Manager as appropriate.

Practitioners

All employed personnel and practitioners are expected to consult with their line managers in matters relating to disclosure or release of client information.

Only when circumstances require an urgent response (i.e. to prevent immediate significant harm to the client or others) and the Operations Manager or any other member of the Designated Safeguarding team is not available, should the practitioner make the final decision to disclose information. In any event this should be in keeping with Service Six's policy in managing client risk.

In all cases of disclosure and release of client information, practitioners should make and retain careful notes about; when; what; and why decisions were taken.

POLICY ON HANDLING PERSONAL DATA

Collection and maintenance of personal information

Service Six will, through appropriate management and the use of strict criteria and controls follow the Caldicott Principles and in addition will:

- observe fully conditions regarding the fair collection and use of personal information;
- meet its legal obligations to specify the purpose for which information is used;
- collect and process appropriate information and only to the extent that it is needed to fulfill operational needs or to comply with any legal requirements;
- ensure the quality of information used;
- apply strict checks to determine the length of time information is held;
- ensure that the rights of people about whom the information is held can be fully exercised.

Responsibilities for managing and handling personal information

In addition, Service Six will ensure that:

- everyone managing and handling personal information understands that they are contractually responsible for following Service Six' data protection practice;
- everyone managing and handling personal information is appropriately trained to do so; everyone

managing and handling personal information is appropriately supervised;

- anyone wanting to make enquiries about handling personal information, whether a member of staff or a member of the public, knows what to do;
- queries about handling personal information are promptly and courteously dealt with; methods of handling personal information are regularly assessed and evaluated.

Ensuring security of personal information

Service Six will also ensure that personal data is kept secure at all times against unauthorized or unlawful loss or disclosure and in particular will ensure that:

- paper files and other records or documents containing personal/sensitive data are kept in a secure environment (i.e. in a lockable room with controlled access, or in a locked drawer or filing cabinet);
- personal data held on computers and computer systems is protected by the use of secure passwords which are changed regularly;
- individual passwords should be such that they are not easily compromised;
- where information is transmitted electronically, all sensitive information is referenced by case number and, if required, case number and name are sent under a separate communication;
- all contractors and temporary staff who have access to personal information supplied by Service Six sign a confidentiality agreement prior to commencement of employment and agree to abide by this policy and related procedures.

DISCLOSURE AND SHARING OF CLIENT INFORMATION

Where it is appropriate to share information about a client with other organisations, local protocols are in place to ensure as far as is reasonable that those receiving the information use it appropriately and respect confidentiality. These protocols differ according to the nature of the commissioning organisation (e.g. PCT, NHS or private) and care must be taken to follow the appropriate procedure for example in respect to release of information to a client's GP.

If it is necessary to share confidential information with others for the effective care of the client or where another person may be at risk of significant harm, this needs to be managed sensitively with the client. An explanation as to the reasons for the disclosure should be provided by the practitioner and the likely consequences should be given to the client. Where possible a client's written consent to release information is obtained.

Apart from exceptional circumstances involving risk of significant harm, the wishes of the client are taken into account as to information they do not want disclosed.

When information is disclosed, only as much as it is required for the purpose is released.

The decision to release information regarding a client, where it is believed to be in the "public best interest" is a matter for careful consideration with the service manager and other senior clinical staff as appropriate.

IMPLEMENTATION

Right to be informed

Service Six is a registered charity and as so, is required to collect and manage certain data. We need to know clients' full addresses, telephone numbers, email addresses, date of birth, GP contact details and the reason for their referral to our services. For clients who are children and young people we also require their parent's/carer's name and contact details and their school/college contact details. This is in respect of enabling us to process the referral and to provide a suitable service for the client.

We are also required to collect certain details of visitors to our Service Six offices. We need to know visitors' names, when and who they are visiting and where appropriate company name. This is in respect of our Health and Safety and Safeguarding Policies.

As an employer Service Six is required to hold data on its employees; including full names, addresses, email addresses, telephone numbers, date of birth, National Insurance numbers, Employment History, photographic ID such as passport and driver's license, bank details and next of Kin contact details. Some of this information is also required for Disclosure and Barring Service checks (DBS) and proof of eligibility to work in the UK.

Rights of access to data

Service Six is a charity registered with the Charity Commission for England and Wales. Registration No: 1132490.

Service Six is also a company registered in England & Wales. Registration No: 6740611.

Registered Office: 26 Rock Street, Wellingborough, Northamptonshire, NN8 4LW.

Telephone: (01933) 277520 or (01933) 273746.

At any point an individual can make a request relating to their data and Service Six will need to provide a response (within 40 days). Service Six can refuse a request, if we have a lawful obligation to retain data i.e. client information in relation to Safeguarding, but we will inform the individual of the reasons for the rejection. The individual will have the right to complain to the ICO if they are not happy with the decision.

Service Six staff and clients have the right to access any personal data, which is held by the Charity in electronic or manual format. Separate procedures govern the disclosure and release of such information.

Rules governing access to records applications:

- an individual Data Subject is entitled to apply to access their total record and are not required to give a reason for this;
- any person authorised by the Data Subject is entitled to apply;
- any parent or guardian who is responsible for a child Data Subject is entitled to apply;
- anyone who has lasting power of attorney, a court appointed deputy, or anyone acting as a mental health advocate on behalf of a Data Subject is entitled to apply;
- anyone appointed by the courts to manage a deceased person's affairs;
- anyone who may have a claim arising out of the person's death (e.g. next of kin).

Service Six must ensure that personal data is not disclosed to unauthorized third parties which includes family members, friends, government bodies, and in certain circumstances, the police. All staff should exercise caution when asked to disclose personal data held on another individual to a third party. This policy determines that personal data may be legitimately disclosed where one or more of the following conditions apply:

- If the individual has given their consent Service Six is legally obliged to disclose the data;

- protect the vital interests of the individual in the course of clinical work (e.g. in the management of risk of serious harm to the client or others)

Consent

Consent will always be sought explicitly if data is to be disclosed to a third party, subject to the conditions applying in 6.1.

By virtue of the services, Service Six provides, consent may not always be provided explicitly prior to personal information being provided to Service Six. By making use of Service Six's services a person may be providing sensitive information. This imposes an additional level of trust on Service Six and its staff to ensure that both personal and sensitive data is handled with due care. Where practicable, Service Six's staff will advise clients of the confidentiality provisions which apply.

Service Six's confidentiality policy is explicitly stated in the letter or statement of agreement provided at the first session. This also makes reference to Service Six's management of information in accordance with the General Data Protection Regulations (GDPR) 2018. Clients are actively encouraged to voice any hesitations they may have about Service Six's policy.

Data Security

Care should be taken to ensure that PCs and terminals are not visible except to authorised staff and that computer passwords are kept confidential. PC screens should not be left unattended without password protected screen-savers and manual records should not be left where unauthorized personnel can access them.

This policy also applies to staff who process personal data 'off-site'. Off-site processing presents a potentially greater risk of loss, theft or damage to personal data. Staff should take particular care when processing personal data at home or in other locations outside Service Six's premises.

Separate procedures relating to maintaining confidentiality are included in practitioner handbooks and guidance on data transfer.

Retention and disposal of data / Right to be erased

Service Six discourages the retention of personal data for longer than required.

You have the right to request the deletion of your data where there is no compelling reason for its continued use. However Service Six has a legal duty to keep clients' details for a reasonable time. For more information please see 'Service Six Retention Periods for Records Policy'

ACCESS TO RECORDS

Who can access records?

A client is entitled to apply for access to their total record as it stands at the time the record is made and they are not required to give a reason for their application. In addition the following can request a client's record:

- any person explicitly authorised by the client.
- parents or guardians with 'parental responsibility' in the case of a child (which may include estranged parents).
- anyone who has 'Lasting Power of Attorney', 'Court appointed Deputy' or is acting as an 'Independent Mental Capacity Advocate'.
- a request from a solicitor acting on behalf of a client is handled in the same way as a request from the client.

- In some cases, children under the age of 16 years who have the capacity and understanding to take decisions about their own treatment are also entitled to decide whether personal information may be passed on about something they do not wish their parents to know (i.e. a child who is 'Gillick Competent').
- At no time should a client's record be released to a solicitor or insurer without the knowledge of the service manager, as Service Six may be required to defend any litigation which may ensue. The service manager will seek further advice from their line manager in cases where a claim may arise.

Records of a deceased client

The Access to Health Records Act 1990 applies in this case, which allows the following rights of access to the records of a deceased client:

- a person appointed by the courts to manage the client's affairs following their death any person who may have a claim arising out the client's death (e.g. next of kin).
- where a party intending to make a claim on the estate of the deceased makes an application for access, that access should be limited to the relevant parts of the record only.

In keeping with Service Six's agreement with commissioning organisations, it may be necessary for information to be released as part of investigations into a serious untoward incident in such cases agreed protocols will be followed.

Procedure for access to records

Under the Freedom of Information Act 2000, the Data Subject has a general right of access to all types of recorded information (This is called a Subject Access Request) held by public authorities, unless particular exemptions apply. The Act aims to improve the openness and transparency of public authorities, and Service Six is committed to complying with this legislation.

Requests for access should be made in writing to the Data Protection Officer, who will confirm that the application being made is legitimate and the correct procedure to verify the right of access has been followed:

- Data Protection Officer @ info@servicesix.co.uk
- Attn: Service Six Data Protection Officer, 26 Rock Street, Wellingborough, Northamptonshire, NN8 4LW

Where in exceptional circumstances (notes have been destroyed after the retention period has elapsed) the request cannot be complied with the Data Subject is notified.

Information requested is usually free of charge and will usually be responded to within 40 days of submission, but we should aim to comply within 21 days as a matter of good practice. In some cases if a large volume of information is requested in hard copy Service Six may issue a fees notice for disbursement costs (printing and postage).

Should a request be made for a face-to-face meeting Service Six will arrange for the Data Subject to look through their file in the presence of a member of staff who can answer questions and note any changes they think should be made to their records.

Service Six staff who have contributed to the record are notified that an application for access has been made and informing them of the intention to release the record.

Copies of records should be provided, retaining the originals in the event of a further need for care.

Withholding access to records

Service Six policy is to be as open as possible, but some information may be withheld if we consider an exemption applies. Sometimes Service Six receives information from someone (e.g Doctor, Social Worker etc) that is written in confidence. When this happens Service Six have to obtain the agreement of the person providing the information before sharing it with the Data Subject. On very rare occasions Service Six might withhold some of the information because it could seriously harm the Data Subject to see it. References to other people might also be withheld.

If Service Six refuses to supply all or part of any information requested reasons for refusal will be provided. The reasons will be based on the exempted categories under the Freedom of Information Act 2000. If the Data Subject is unhappy with the way in which their request was handled they can request an internal review. A senior member of staff who was not party to the original decision on whether to release the information will review the manner in which the request was dealt and will either uphold or overturn the original decision.

Rights to amend contents of a health record

Where the Data Subject disagrees with a non-medical fact in the records, the Data Protection Officer can alter this.

Where the Data Subject disagrees with a medical or other professional entry, which the professional believes to be correct, this cannot be altered under any circumstances. In this case a note is added to the record to indicate the client's objection.

In some circumstances the Data Subject may request a note be added to the records indicating they do not wish access to be granted after their death. Where an application is made after the death of the person to whom the record refers, care should be taken to comply with the client's instruction.

Where possible, amendments to records should include notes of what has been amended which are signed by the Data Subject concerned and the Data Protection Officer.

RELEASE OF INFORMATION HANDLING PROCESS

A member of staff receives a request for records in writing, dates it then informs the Data Protection Officer as soon as possible.

The limit to comply with any request is 40 days from receipt but we should aim to comply within 21 days as a matter of good practice.

The Data Protection Officer ensures the following;

- The request is noted on the database Data Subject file and all subsequent actions are to be noted. The identification of the applicant is established.
- The request for the release of information is received directly from the applicant, or a third party on their behalf (e.g. solicitor, police) and is signed by the Data Subject.
- The relevant information or file is located and contents checked for accuracy and clarity.
- An assessment of what is required to comply with the request is made to establish whether:
  - confirmation of attendance and sessions would be adequate.
  - the whole record is to be supplied (ensuring any references to third parties is removed).

- a specific clinical report needs to be written (in which case the fee for an hour of practitioner's time may be chargeable).

- Inform the applicant of any problem in complying with the request, or if additional information is required. Any further actions should be communicated in writing, including requests for additional information.
- Consult with the practitioner concerned regarding information which is to be to be released.
- In the case of any unusual request from a third party, there should be consultation with another manager before information is released.
- Communications should be 'clean' of any information relating to Service Six processes.
- The information may be sent by registered post if it contains particularly sensitive information in which the Data Subject may be identified.
- If the information cannot be released consultation with the clinical governance manager will take place, for example when information:
  - may cause serious harm to the client or another person.
  - is not solely part of the client's record (e.g. mediation).
  - requires consent from others (e.g. couples).
  - has been requested previously within an unreasonably short period.

If there are any complications, the Data Protection Officer should consult with the Chief Executive or the Board of Trustees and detailed notes should be recorded of actions taken with reasons for decisions. Complex cases involving Social Services, the Police or other third party requests without client consent should always be referred for consultation

STAFF & PRACTITIONERS

When a member of staff leaves Service Six, it is not necessary to retain all their personal information. In general, electronic staff records containing information about individual members of staff are kept indefinitely and information typically includes name and address and, where appropriate positions held and leaving salary.

Other information relating to members of staff will be kept for 6 years from the end of employment. Information relating to Income Tax, Statutory Maternity Pay etc will be retained for the statutory time period (between 3 and 6 years).

Information relating to unsuccessful applicants in connection with recruitment to a post will be kept for 12 months from the interview date.

Brief records of individuals that have applied for, been short-listed, or interviewed for posts or affiliate status, may be retained indefinitely to aid management of the recruitment process

It is important that employers keep a clear and comprehensive summary of any allegations made,

Details of how the allegations were followed up and resolved and of any action taken and decisions reached. These should be kept in a person's confidential personnel file and a copy should be given to the individual. Such information should be retained on file, including for people who leave the organisation, at least until the person reaches normal retirement age, or for 10 years if that is longer.

The purpose of the record is to enable accurate information to be given in response to any future request for a reference. It will provide clarification in cases where a future DBS disclosure reveals information from the

police that an allegation was made but did not result in a prosecution or a conviction. It will also prevent unnecessary re-investigation if, as sometimes happens, allegations resurface after a period of time.

More information can be found it the retention Periods of Records Policy.

CLIENTS

Client records are retained for long enough to ensure that care is provided in a way that is consistent with regulations and clinical guidelines, including NHS requirements where applicable.

Adult client files relating to EAP or private work are usually retained for a minimum period of 6 years after the case has been closed and will then normally be destroyed.

Children and Young People's files are usually retained until the client's 25th birthday or 26th if young person was 17 at conclusion of service and will then normally be destroyed.

These periods may be extended in consideration of legal issues that may be raised in reference to a case (e.g. Serious Untoward Incident investigations).

More information can be found it the retention Periods of Records Policy.

DISPOSAL OF RECORDS

Paper records of staff, affiliates and clients are scanned to a secure system and attached to the database in accordance with procedures to ensure accuracy.

Care is taken to ensure that appropriate security measures are in place for the deletion or disposal of personal data.

Manual records are shredded and disposed of as 'confidential waste'.

Hard drives of redundant PCs are wiped clean and machines are destroyed rather than being re-conditioned for use outside Service Six, as secure electronic deletion is deemed to be an insufficient safeguard of personal data.

GUIDELINES FOR AFFILIATE IT SECURITY

INTRODUCTION

The General Data Protection Regulations (GDPR) 2018, requires that anyone handling personal and sensitive data must comply with the eight principles of the act. These include ensuring that all data is held, handled and transferred securely.

Much of the information entrusted to Service Six may be of a confidential, personal or sensitive nature, and it is important that the security of this information is preserved up to and including the point of disposal. The following briefly outlines potential IT risk issues and provides some guidance to ensure safe practice.

All affiliates working in Service Six services are required to read the following and to sign the attached agreement indicating compliance with minimum requirements:

PASSWORD MANAGEMENT: PURPOSE, CONSTRUCTION AND BEST PRACTICE

The purpose of a password is 'access control'. Passwords allow users to gain access to their own personal information or services electronically. Individual passwords can prevent unauthorized access to computer systems, online services, email accounts, electronic files and restricted premises. Overall passwords aim to keep information secure and confidential.

Do:

- password protect access to PCs, laptops, email and individual folders where client files are stored
- choose a password of at least six to eight characters long
- use a mixture of upper and lower case letters, numbers and keyboard symbols (i.e. ` ~ ! @ # $ % ^ & * ( ) _ + - = { } | [ ] \ : " ; ' < > ? , . /).
- change passwords regularly
- ensure passwords are kept secret
- change your password immediately if you suspect someone else knows it
- use memory tricks to remember passwords (e.g. make a password out of the first letters of each word in a memorable phrase)
- log off your computer or lock your computer screen with a password protected screen saver whenever you leave your desk unattended

Do not:

- use your user name, real name, or Charity name in your password or anything that is easy to work out with a little background knowledge (e.g. birthday, spouse's name)
- disclose your passwords to anyone else, even to family members
- recycle passwords (e.g. password2, password3)
- write passwords down

SAFE COMPUTING: SECURING AGAINST VIRUSES, MALWARE & EMAIL HOAXES

Secure computing has multiple issues that should be considered when constructing a safe operating environment. A common problem encountered is the issue of malicious software, or 'malware', which includes viruses, Trojans, worms and spyware.

Do:

- make sure that you have a firewall installed
- make sure you have anti-virus and anti-spyware software installed and that you keep it up to date
- make regular back-ups of data

Do not:

- open emails or attachments if you do not know the sender or if you suspect that the attachment is not what it seems

INTERNET AND EMAIL USAGE

The internet and email are the most common source of computer viruses, malware, spyware and other malicious code. Infected files could be unwittingly downloaded from the internet or contained in email

attachments and could be passed on.

Do:

- scan any email attachments for viruses before you open them
- include a relevant title for your email message (i.e. not using client names)
- follow the advice of the service on best practice in emailing client data (e.g. never incorporating names and addresses along with sensitive information)
- be careful to address emails accurately and include a footer after the signature e.g.:

"If you received this communication by mistake, please don't forward it to anyone else (it may contain confidential or privileged information), please erase all copies of it, including all attachments, and let the sender know it went to the wrong person. "

Do not:

- download files or open email attachments without being certain that you trust the sender and the content

MOBILE COMPUTING: THE SECURE USE OF LAPTOPS, PDAS AND OTHER MOBILE DEVICES

Mobile computing describes the use of any mobile device that can process data. Typically this will include items such as laptops, personal digital assistants (PDAs) and mobile email devices and even mobile telephones where these are capable of storing data. Mobile computing presents a further set of risks since devices are not restricted to a controlled office or home environment.

Do:

- make sure that your devices are physically secure when unattended
- keep the information you have on your device to a minimum and make sure that it is backed up
- encrypt and password protect devices and removable media that contain any client information
- be aware of the potential for opportunist or targeted theft of laptops and mobile devices in busy public places
- immediately report any actual or suspected loss, theft or unauthorized access/ disclosure.

Do Not:

- leave your mobile devices unattended, even for a short period (e.g.in a car)
- place devices in locations where they could easily be forgotten or left behind e.g. overhead racks and taxi boots
- hold more information than is necessary on mobile devices
- use laptops with removable media in places where that media could easily be left behind or misplaced

REMOVABLE MEDIA

Removable media is a term used to describe any kind of portable data storage device that can be connected to and removed from your computer (e.g. disk, USB stick). The data on removable media becomes portable, and therefore has less protection for security and confidentiality.

Do:

- use encryption or other protection methods for confidential, personal or sensitive information if you

intend to use portable storage devices.

Do not:

- copy client files to removable media such as passports provided

MEDIA DISPOSAL

Erasing electronic files and folders does not remove this from a computer's hard drive. At some point you will need to get rid of computer files, the computers themselves, disks and physical files. Disposal of IT media in the regular waste is not legal, for two reasons:

- The security of data: Compliance with data security and the Data Protection Act require that information, whether it is personal, the Charities or financial, is disposed of securely.
- Environmental protection issues: It is not lawful to dispose of magnetic media with household and general rubbish as it does not break down and decay.

Do:

- erase all folders, emails and files in connection with client work in accordance with the service requirements (usually after a month of submitting these)
- also erase the same folders, emails and files which may have been stored in back up versions, sent and deleted items
- destroy the hard drives of any obsolete equipment prior to safe disposal.
- obtain certificates of destruction for IT hardware disposed of using specialist services
- restrict any access IT specialists may have to client information when you submit equipment for upgrades, repair etc.

Do not:

- give or supply your computer equipment (even obsolete equipment) to a third party

SUMMARY; CONFIDENTIALITY PROCEDURES FOR ADMINISTRATION

INTRODUCTION

Confidentiality is a basic principle and essential element of providing a counselling service. Service Six follows the British Association for Counselling and Psychotherapy (BACP) ethical framework and guidelines regarding confidentiality, as well as the General Data Protection Regulations (GDPR) 2018.

The contract with clients clearly outlines our confidentiality policy and creates an expectation for the client; any leaking of information is a breach of this contract and is harmful to their confidence in our service.

As part of establishing, supporting and maintaining confidentiality, all of Service Six's administrative staff have a central role to play. They may be the first or most frequent point of contact for many clients, and therefore they help to create and continue to maintain the sense of what our confidentiality policy means in practice.

The following is an overview of areas where issues may arise for administrative staff. It is not intended to

cover every situation but to present a way for staff to feel confident in their role of receiving and passing on information without fear of being in breach of confidentiality.

Maintaining confidentiality has implications for all areas of Service Six's work. It applies not only to storing and maintaining records but also to all written communications. Likewise it applies to what is visible in our office environment. General chat about clients in corridors risks compromising confidentiality, with this in mind, discussion should be kept strictly to business matters, being polite and professional at all times, with both colleagues and clients. If you know a client or you recognise a name, limit your involvement with that case and declare this knowledge to your line manager, to discuss any further action required.

As a general principle, business matters should only be discussed with or communicated directly to clients and not any other person, unless there is clear permission to do so.

COMMUNICATING BY PHONE

Before contacting a client, always check the database contact details to see if it is OK to leave messages on the number you are calling; where this is not indicated then assume it is not OK. In these cases, always dial 141 before the full number, and do not leave a message. Check carefully that you have the right person, especially for landline numbers. If another person answers, only leave a discreet message with that person if it indicates that it is OK to leave messages.

When taking a message about a cancelled appointment, note the message and explain it will be passed on for action. Always ask for a contact number and whether it is OK to leave a message.

Only request information as required for the purpose of passing it on. It is not expected that you engage in a discussion, nor should you have to explore the database for details of the case.

If you are unsure of the situation or what the person is asking about, take the caller's number, always ask if it is OK to leave a message, and say that someone will call them back. Then check the case with your line manager as appropriate.

WRITTEN COMMUNICATION

Check that it is OK to write to the client at the address you have available.

All written communication should be marked ***'Private & Confidential'*** on the envelope. In addition it should have ***'Only to be opened by the addressee'*** as the first line of the address.

Take particular care to ensure that names and addresses are correct before sending, and that you have included only the information relevant to the client.

Be sure to follow other procedures in your particular work, regarding safe storage of information and records.

COMMUNICATING WITH COUPLES OR PARENTS

Administrative staff record initial information, and therapists may then clarify any special contact arrangements. In some cases, parents or partner's numbers may have been provided as a contact regarding payment, but there are limitations on further discussion.

In the case of children, assume all parental contacts on the database are OK to be contacted unless it states otherwise. Where contracts involve a couple, take care to check the database directions about who may be

contacted and on which numbers or addresses. Avoid using titles such as 'mr & mrs' and do not assume couples are of opposite sexes.

If there is any doubt about permission to discuss or make arrangements then check this before proceeding.

THIRD PARTY CONTACT

When a third party calls to re-arrange an appointment on behalf of a client, check whether the client is able to come to the phone, if not, take the message but suggest the client calls when they are able in order to re-arrange. For any other purposes we need to have direct contact with the client. There are always exceptions, so if a person is being difficult, explain that you will pass the matter on for further attention and seek advice from a manager.

Any other requests for information from third parties need careful managing.

Further policies regarding regular third party contacts with professionals supporting a client may apply in some cases, your manager will ensure you are aware of these.

THERAPIST CONFIDENTIALITY

If a client asks to speak directly to a therapist, say they are not available and take the detail to pass on. When cancelling sessions for a therapist, never give detailed personal information, simply state someone is ill or an emergency has arisen, as appropriate.

Do not give a therapist's contact information from the database unless it expressly states this is OK, in cases of emergency check with a manager.

COMPLAINTS

Complaints need to be reported by the client, individual or organisation concerned using the Comments, Compliments and Complaint form and associated policy.

If a client is dissatisfied or becomes angry or difficult, is anxious or in distress, try to remain calm and neutral and look after your own needs in the conversation. Acknowledge their response and explain that you will pass the matter on for further attention.

SCANNING PROCEDURE

The General Data Protection Regulations (GDPR) 2018 and the confidentiality provisions detailed by the British Association for Counselling and Psychotherapy in its Ethical Framework for Good Practice in Counselling and Psychotherapy govern Service Six's operations.

In order to ensure that complete and accurate records are maintained for the required period of time, this procedure must be implemented in all cases where documents are scanned and original copies are destroyed.

This process will apply to all records:

- Scan the original to its proper place on the server and attach to the database as appropriate
- If a file has been attached to the database, enter a final contact note saying, ***"Complete file scanned***

and attached".

- Count the pages in the original document and ensure that the same number of pages have been saved to the server and database file as appropriate.
- Check at least 10% (1 in every 10) of all documents that have been scanned, to ensure that every page is copied accurately (i.e. all pages are copied and legible).
- When scanning a single document, always check for accuracy.
- If any document is 20 pages or more always check 1 in every 10 pages for accuracy.
- The line manager should be informed of which documents have been scanned, so that they can carry out random checks for accuracy.
- If any omissions or problems arise in a batch being checked by the person scanning, or the line manager, the error should be corrected and a further 10% of documents should be checked. This procedure should be repeated until no errors are discovered in the sample.

Only when both the person scanning and the line manager, in accordance with the above, have checked a batch of scanning should the original paperwork be destroyed in accordance with confidential waste procedures.

STORING DATA

Personal data may be printed and secured in Service Six filing cabinets otherwise everything is on Service Six' secure IT and SAGE system. They are placed in our office that is secured by high level security and a monitored alarm system.

Personal data may also be stored electronically on our secure cloud based servers. Our back-up system is based in the UK. All Computers are protected by password and anti-virus program and can only be accessed by authorised staff.

Service Six holds Cyber Essential Accreditation, which demonstrates Service Six' commitment to cyber security.

More information about how long we keep records can be found in Service Six Retention Periods of Records Policy.

DATA BREACHES

Service Six has standards procedures to protect Data Subject's details against data breaches such as passwords for electronic files that are periodically changed, alarms and secure filing cabinets for physical documents.

We back-up all data by creating an electronic copy of each document that is securely stored on our cloud-based server system that is protected by passwords and anti-virus program.

Service Six understands the legal requirement to report a data breach to ICO (Information Commissioner's Officer) in maximum 72 hours from the event. We also commit to inform every person that has been affected by the data breach.