Service Six

CONFIDENTIALITY AND DATA PROTECTION POLICY

Date: April 2017

Review Due By: April 2018

Lead Role/Manager: Chief Executive

Others involved in implementing: Executive Team, 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 Data Protection Act (1998); 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.

LINKS TO OTHER SPECIFIC THERAPEUTIC POLICIES, PROCEDURES & GUIDELINES

Clinical Risk Management Policy
Disclosure and Release of Information Policy

DEFINITIONS

Data Protection Act 1998

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.

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

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 Data Protection Act.

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

The Chief Executive acts as the Charity's Information 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.

Lead Therapist

In practice, responsibility for therapeutic decisions relating to disclosure of information is devolved to the Lead Therapist (who exercises responsibility similar to Caldicott Guardians). In addition, the Lead Therapist 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.

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 good 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.

IMPLEMENTATION

Rights of access to data

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 Data Protection Act. 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

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

Staff and 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

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's files are usually retained for a minimum period of 20 years after the case has been closed 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).

Disposal of Records

- Paper records of staff, affiliates and clients are scanned to a secure server 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 Data Protection Act, 1998, 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 you 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

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 Data Protection Act.

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.

Summary: Confidentiality Procedures for Administration

INTRODUCTION

Maintaining confidentiality applies to all communication with or about clients.

Discussion should be kept strictly to business matters, being polite and professional at all times, with both colleagues and clients.

If a client is known to you or you recognise a name, limit your involvement with that case and declare this knowledge to your line manager.

As a general principle, matters should only be discussed with or communicated directly to clients, unless there is clear permission to do otherwise.

COMMUNICATING BY PHONE

Always check the database contact details to see if it is OK to leave messages. If it is not OK to leave messages dial 141 before the full number.

Check that you have the right person, especially with 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, explain it will be passed on for action, take a contact number and ask if it is OK to leave a message.

Only request information as required for the purpose of passing on messages.

If you are unsure of the situation take the caller's number, always ask if it is OK to leave a message.

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, and write 'Only to be opened by the addressee' as the first line of the address.
Follow other procedures regarding careful storage of information and records.

COMMUNICATING WITH COUPLES OR PARENTS

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 who may be contacted and on which numbers.

If there is any doubt, check before proceeding.

Avoid using titles such as 'Mr & Mrs' and do not assume couples are of opposite sexes.

THIRD PARTY CONTACT

When a third party calls to re-arrange an appointment take the message but suggest the client calls when they are able, in order to re-arrange.

Any other requests for information from third parties, if it is not a normal part of your remit, take a message and pass it to the appropriate manager.

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. Do not give a therapist's contact information unless it is clear this is OK.

COMPLAINTS

Complaints need to be reported by the client concerned and using the Comments, Compliments and Complaints form and associated Policy.

Take the details and if it is something you can resolve immediately then do so. Explain that you are an administrator and what action you can take.

Note the details of the complaint and pass to your manager or appropriate person.

Do not discuss the complaint with others unless you are involved in the further investigation.

SCANNING PROCEDURE

The Data Protection Act 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.