Version History				
Version	Date	Detail	Author	Approved by Board
1.0	3 March 2013	Document created	Annie French	13 May 2013
1.1	01 June 2016	Amended	Hilary Ashton / Katie Whitham	
1.2	31/01/2017	Amended para 25 and 77.	Hilary Ashton	31/01/2017
1.3	02/06/2017	Added Appendix 1	Katie Whitham	
1.4	04/07/2017	Amended para 14 and 15 Added para 87	Katie Whitham	
1.5	18/07/2017	Added para 88	Katie Whitham	

Data Protection and Personal Information Policy

1.0 Advonet complies fully with the Data Protection Act 1998 in respect of its management of personal data.

2.0 Advonet is a consortium of advocacy provider agencies. Advonet delivers direct advocacy services, sub contracts with service providers and provides support services to the advocacy and wider voluntary sector in Leeds. This policy refers to all of this work and sub contracted organisations will be required to adopt this policy.

3.0 The Board of Trustees ensures that Advonet is suitably registered with the Information Commissioner and that Advonet's Data Controller Registry information is maintained and updated when appropriate.

4.0 The Board of Trustees confirms that Advonet will only normally disclose personal data in respect of members of the public, current, past and prospective employees, volunteers, service users and customers, and suppliers to a legally

entitled recipient, with the explicit permission of the person or organisation concerned (data subject).

5.0 The Board of Trustees will ensure that personal data is only obtained and processed:

- Fairly and lawfully
- For specific and lawful purposes, in compliance with the registration with the Information Commissioner
- In a way that is adequate and relevant for the purpose
- Accurately and is maintained up to date
- For no longer than is necessary
- Respecting the right of data subjects to have due access to data held about them
- Securely, including secure storage
- By Advonet, as Data Controller, within the European Union and shall not be transferred to a country or territory outside the European Union, unless that country or territory ensures an adequate level of data protection.

6.0 The Board of Trustees confirms that personal data will only be shared without the consent of the data subject where this is justified on the basis that the benefits (supported by meaningful evidence and safeguards) outweigh the risks of negative effects. A Privacy Impact Assessment will be undertaken before personal data is shared other than in compliance with Advonet's registration.

7.0 The Office and Resources Manager of Advonet is the designated Information Officer with responsibility for ensuring that data is used in accordance with the designated policies, procedures and practices of Advonet and that a Privacy Impact Assessment is undertaken when required.

8.0 The Board of Trustees recognises that current and former service users, applicants, staff and volunteers have a right to reasonable access to information held about them by Advonet.

9.0 Definitions

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

11.0 **Personal data** is defined as data relating to a living individual who can be identified from:

- That data;
- That data and other information which is in the possession of, or is likely to come into the possession of the data controller and includes an expression of opinion about the individual and any indication of the intentions of the data controller, or any other person in respect of the individual.

- **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**: includes obtaining, disclosing, recording, holding, using, erasing or destroying personal information. The definition is very wide and covers virtually any action carried out on a computer.

12.0 Procedure

Handling of personal/sensitive information

13.0 Advonet will use appropriate management and strict criteria and controls including:

- 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 fulfil 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.
- Take appropriate technical and organisational security measures to safeguard personal information.
- Ensure that personal information is not transferred abroad without suitable safeguards.
- Ensure that the rights of people about whom the information is held can be fully exercised under the Act.
  The rights of individuals include:
    - The right to be informed that processing is being undertaken
    - The right of access to one's personal information within the statutory 40 days
    - The right to prevent processing in certain circumstances
    - The right to correct, rectify, block or erase information regarded as wrong information.

Responding to a request for Personal Information

14.0 The request by current and former service users, applicants, staff and volunteers to access any file held about them by Advonet must be made in writing:

- Most requests for personal information will not usually incur any cost from the applicant. However, a fee of up to £10 can be charged for responding to a request for personal information if Advonet estimates that the cost of complying with the request would exceed the appropriate limits as stated in the Freedom of Information Act 2000 Section 12-(1).
- The reply should include both the information held and details of the processing carried out.
- Information can only be withheld if it relates to or is from a third party who has not consented to access to this information or is subject to legal privilege.

15.0 Advonet will respond as soon as possible to the request and in all cases within 40 calendar days.

Responsibilities of Advonet

16.0 All members of the Board of Trustees are made fully aware of this policy and of their duties and responsibilities under the Act.

General responsibilities

17.0 Everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice and is appropriately trained to do so.

18.0 Everyone managing and handling personal information is appropriately supervised.

19.0 Anyone wanting to make enquiries about handling personal information, whether a member of personnel or a member of the public can be made aware of what to do.

20.0 Queries about handling personal information are promptly and courteously dealt with.

21.0 Methods of handling personal information are regularly assessed and evaluated.

22.0 Performance with handling personal information is regularly assessed and evaluated.

23.0 Data sharing is carried out under a written agreement, setting out the scope and limits of the sharing. Any disclosure of personal data will be in compliance with approved procedures.

24.0 Everyone has responsibility for reporting any data protection breaches or concerns to the Information Officer or to their Line Manager, who will inform the Information Officer.

Specific responsibilities

25.0 All personnel within Advonet will take steps to ensure that personal data is kept secure at all times against unauthorised 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
- Personal data held on computers and computer systems is protected by the use of secure passwords, which where possible have forced changes periodically
- Individual passwords should be such that they are not easily compromised.
- All representatives of Advonet must:
    - Ensure that they and all of their personnel who have access to personal data held or processed for or on behalf of Advonet are aware of this policy and are fully trained in and are aware of their duties and responsibilities under the Act. Any breach of any provision of the Act will be deemed as being a breach of any contract between Advonet and that individual, company, partner or firm.
    - Allow data protection audits by Advonet of data held on its behalf (if requested.
    - As far as possible, protect Advonet against any prosecutions, claims, proceedings, actions or payments of compensation or damages.
    - All representatives of Advonet who are users of personal information will be required to confirm that they will abide by the requirements of the Act.

Responsibility of Information Officer

26.0 Ensure that Advonet's registration with the Information Commissioner is maintained.

27.0 Review the Data Protection Register annually and notify the Information Commissioner of any changes.

28.0 Ensure the policy is implemented.

29.0 Ensure all workers and Board members are trained in data protection, at least by ensuring they have read and understand this policy.

30.0 Develop best practice guidelines on the gathering, use, storage, retention and sharing of personal information.

31.0 Carry out compliance checks to ensure adherence with the Data Protection Act throughout the organisation.

32.0 Deals with all requests from current and former service users, applicants and personnel to access information of files held about them by Advonet.

Sharing Personal Information

33.0 Information sharing must be supported by a sound business case and accompanied by a privacy impact assessment and risk assessment (including the risk of not sharing the information).

34.0 Information will only be shared under safeguarding procedures where there is a view that either a service user or a vulnerable person is at risk if the information is not shared.

Personal information and marketing

35.0 Marketing refers to promotional activities.

36.0 All individuals can stop their personal information being used for direct marketing. Requests must be complied with and within a reasonable period of time – no longer than three months and preferably 28 days.

37.0 Advonet must tell individuals what their personal information will be used for, and in particular:

- Who the organisation is
- What the information will be used for
- Anything else necessary to make sure the information is being used fairly – including whether marketing lists are passed to other organisations, and how people will be contacted (post, phone, mail or via a website or e-mail
- Advonet must give individuals the chance to opt out of receiving marketing on each occasion the organisation contacts them.

Privacy and Electronic Communications

38.0 *Telephone marketing* – do not make unsolicited calls to an individual or organisation who has told Advonet they do not want calls from Advonet. Do not make calls to any numbers on the Telephone Preference Service list unless the individual has told Advonet that they do not, for the time being, object.

39.0 *Automated calls* – do not make automated calls without getting the individual's permission first.

40.0 *Electronic mail* – do not send electronic mail marketing without obtaining the individual's permission first. (Applies only to messages sent to individuals).

41.0 *Fax marketing* – do not send to any number on the Fax Preference Service, any individual who has told Advonet they object or any individual unless they have told Advonet they agree, for the time being, to have faxes sent to them.

Identity and contact information

42.0 Identify Advonet in any marketing message

43.0 Provide appropriate contact details so that the individual or organisation receiving the message can contact Advonet. This should be a postal address, email address or telephone number.

44.0 For telephone marketing, identify Advonet. Give address or telephone number if asked for it.

Change

45.0 When told by an individual that they no longer want to receive marketing information, this must be dealt with promptly, preferably within 28 days.

Professional Opinion

46.0 All personal information should be accurate, and where necessary kept up to date. In relation to professional opinion this criterion will be met as long as the record made/kept accurately reflects professional opinion.

47.0 An opinion which contains factual information which is incorrect can be challenged.

48.0 A challenge to factual accuracy or reliability of an opinion may be recorded alongside it, since it will usually be important to maintain the original record. It is recommended that the fact that a challenge exists is made clear on the original record.

49.0 All personal information should be sufficient for its purpose and not include irrelevant material. This means that when the opinion is recorded it (or the context in which it is held) should contain enough information to allow a reader to be able to interpret it correctly. The opinion should explain the circumstances and include the evidence on which the opinion is based.

50.0 Advocacy records will usually contain opinions only of the service user and factual observations made by the advocate, although documents and records from other organisations may have been shared. If the record in the advocacy file is a summary of more detailed records held elsewhere, it is important that the reference to opinion includes enough information to allow these detailed records to be traced.

51.0 Personal information should not be kept for longer than is necessary to do the job it is intended for, unless that is a different and valid need to keep a comprehensive record.

52.0 Individuals may ask for an opinion to be deleted which they think is irrelevant or unjustified – this may be because they have obtained a second opinion which contradicts the first. In these circumstances Advonet will need to consider if it needs the information for the adequacy of the record and for its own purposes.

Security

53.0 Advonet will review the security of the personal information it controls by asking: Is processing carried out by Advonet or is any of it done by someone acting on behalf of the organisation? Consideration will be given to:

- How valuable, sensitive or confidential is the information.
- What damage or distress could be caused to individuals if there was a security breach
- What effect a security breach would have on Advonet – in cost to reputation and to the trust of clients
- The Office and Resources Manager / Information Officer must have day-to-day responsibility for security measures.

Security measures – the Information Officer

54.0 The Information Officer will:

- Discuss with senior colleagues what security measures should be adopted.
- Write procedures for workers to follow.
- Ensure training for personnel is organised.
- Check whether personnel are following procedures and that these work.
- Monitor change.
- Investigate any security incident.

55.0 Unless this is done, security will quickly become flawed and out of date.

Security measures – the organisation

56.0 Advonet will:

56.1 Carry out a risk assessment to take account of what needs to be protected, the type of security problems that could occur and the effectiveness of current security measures.

56.2 Use the risk assessment to inform the changes to be made.

56.3 Ensure the officer responsible has the standing and resources to make sure the job gets done.

56.4 Ensure the organisation has security procedures in place for personnel to follow.

56.5 Ensure there is co-ordination on security matters between key people in Advonet.

56.6 Check that personnel are taking their security responsibilities seriously.

56.7 Ensure that a procedure is in place to make sure that security incidents are investigated and lessons learned.

56.8 If access is given to anyone outside Advonet, e.g. for computer maintenance, ensure that security is in place to oversee what they do.

56.9 Using another organisation to process personal information often causes security problems. Steps are laid down in the Act which must be taken:

- Choose an organisation which offers guarantees about the security of information they are processing for Advonet.
- Have a written contract that sets out what Advonet allows the contractor to do with the information. This must be clear about use and disclosure, but must also have in place security measures equivalent to those which would be used by the organisation if doing the job internally.
- Take reasonable steps to check that the contractor is taking those security measures
- Make business continuity arrangements that identify how to protect and recover the personal information held by Advonet.
- Check compliance with legal obligations such as copyright and licensing requirements.

57.0 Carry out a periodic check of security arrangements to ensure that these are still appropriate and up to date.

Security issues – personnel

58.0 A high proportion of security incidents are shown to be personnel-related. Advonet will take all reasonable steps to ensure the reliability of personnel who have access to personal information.

59.0 At the recruitment stage, take reasonable steps to check the identity and reliability of personnel – obtain references; check that these and the person's qualifications are valid.

60.0 Include in the employment contract or in a confidentiality agreement what personnel can and cannot do with the personal information they handle.

61.0 Train personnel in their responsibilities about personal information. Make it clear what information is confidential and the restrictions as to how this should be used.

62.0 Ensure personnel are aware of the dangers of someone trying to trick them into revealing an address or disclosing information when the enquirer is not who they

say they are. Ensure personnel understand the proper procedure to identify a caller. Ensure personnel understand about possible 'phishing' attacks (via email) so that they can safeguard against data security breaches.

63.0 Ensure personnel understand that it is a criminal offence to deliberately give out personal information without the consent of Advonet. Ensure personnel know that they can commit a criminal offence if they try to access or obtain personal information without the authority of Advonet.

64.0 Physical security: emphasis is put on technical security measures to protect computerised information, but physical security is just as important.

65.0 Ensure that premises are secure with good quality doors and locks, and a well-lit exterior. The last person leaving Advonet offices should activate the alarm system.

66.0 Lock up paper-based information at night.

67.0 If on the ground floor prevent people being able to see the computers and screens form outside.

68.0 Ensure control of access to the premises is appropriate. Supervise visitors and consider keeping these to public areas.

69.0 Lock up laptops and other portable equipment and computer media like discs and memory sticks at night.

70.0 Dispose of paper waste containing personal information securely by shredding.

Computer security

71.0 This should be appropriate to the extent of the system and what it is used for. Measures do not have to be 'state of the art' but must be appropriate for the harm that could result and the nature of the information processed.

72.0 A networked system needs more controls than a stand-alone computer.

73.0 A stand-alone that is connected to the internet and email will need more protection than one that is not.

Managing security on the computer system:

74.0 Advonet will manage the operation of the computer system with procedures and document change.

75.0 Advonet will ensure that there are checks and balances in job roles to prevent unauthorised change or fraud.

76.0 We will note that servers need extra security and access to them must be limited. We will obtain specialist security advice and help to address these needs if this is required.

77.0 Advonet will ensure equipment is maintained to prevent against loss of or interruption to work.

78.0 Control access to the computer system through workers having their own password. We will ensure that no-one else is able to use this and require a password that will not be easily broken.

79.0 Advonet will control access to information that only certain people should see – for example by setting privileges to certain parts of the network.

80.0 There will be strategies to control access to computers when they are unattended e.g. By ensuring auto locking of inactive computers.

81.0 Advonet will obtain security updates for software to fix any vulnerability which has been discovered.

82.0 If laptops or portable media (memory sticks, discs etc) are taken out of the office containing personal information, they are to be transported with permission and securely. Consideration will be given to how sensitive the information available is and whether it could cause damage or distress to the people concerned. We will arrange for hard discs or individual documents to be encrypted to keep information secure, and use encryption of good quality. (See ICO views on encryption on the website)

83.0 Deletion procedures will be effective, especially on equipment which is being discarded.

84.0 We will take regular backups of information held on computer and store in another location in case of fire and test recovering information from the backup system to ensure that it works.

85.0 If using internet or email workers must ensure that firewall and virus protection is up to date. Advonet will ensure there are systems in place to use if the computers become infected or hacked into.

86.0 Advonet will warn personnel about the insecurity of email and ensure that any sensitive personal information sent electronically is encrypted or sent by other means.

Data Protection and the use of Interpreters

87.0 Interpreters are placed in a privileged position and as such are bound by Advonet's rules of confidentiality and data protection at all times. As with all Advonet staff and volunteers, any breach of confidentiality or misinformation would be dealt with through Advonet policies and procedures. Interpreters/Signers will: respect confidentiality/data protection at all times, in accordance with Caldicott guidelines and not seek to take advantage of any information disclosed during their work; act in an impartial and professional manner; not discriminate against parties, either directly or indirectly, on the grounds of race, colour, ethnic origin, age, nationality, religion, gender, sexuality or disability. Interpreters are an authorised third party, privy to personal and sensitive information, bound by common laws of confidentiality and provisions under the Data Protection Act 1998 in prior agreement with Advonet. Any agencies used to provide interpreting services for Advonet are responsible for training their staff in Data Protection and Confidentiality.

Escalating Concerns

88.0 If there are any concerns over any matter relating to Data Protection then the Information Officer should be informed. Complaints and concerns can be escalated through the Advonet Complaints Policy and Procedure. If the outcome of this is not satisfactory then they should approach the Information Commissioners Office.

Appendix 1

26 Roundhay Road, Leeds, LS7 1AB
Tel: 0113 244 0606 **Fax**: 0113 244 0178 **Email**: office@advonet.org.uk

Information Sharing Agreement Requirements and Equipment

The Information Sharing Agreement between Advonet and Leeds City Council requires that the following criteria be adhered to:

External mail

When sending personal/sensitive personal information via external mail services the sender of the information should:

- Ensure that the correspondence is addressed to the correct address.
- Ensure that the information being sent all relates to the correct individual.
- Ensure that a new envelope is being used
- Ensure that a secondary peer check takes place before the correspondence is sent out. The secondary peer check involves a colleague checking the correspondence address is correct and that the contents all relate to the correct individual.

Transporting documents

Personal/sensitive personal information in paper format must be transported safely and securely i.e.

- Carried in a secure bag i.e. a lockable, waterproof bag at all times
- Never left in a car for prolonged periods or overnight
- Stored apart from high valued devices such as tablets, laptops or mobile phones
- Never unattended, or left on show i.e. in a car or other vehicle
- Only transported if necessary and for the minimum period of time possible

Verbally

When personal/sensitive personal information is shared verbally care must be taken that the information is being shared in a secure environment i.e. the conversation cannot be overheard by any party who is not entitled to hear the information being discussed. Care must be taken before any personal/sensitive personal information is discussed that the correct person is being spoken to.

Fax

Fax is not considered to be a sufficiently secure method of sharing personal/sensitive personal information, and a more secure method of sharing should be used.

Use of email to share personal/sensitive personal information

Personal/sensitive information can only be shared using email if the information is being sent ***and*** received by a secure domain email address to ensure encryption of information in transit.

Confidential information should only be removed and stored away from the Advonet office according to processes agreed with your line manager.

Advonet Employee Agreement

I agree to abide by the above criteria when dealing with personal and sensitive information in the course of my work on behalf of Advonet. Specifically:

- I agree to store confidential documents in a secure location when away from the Advonet office.

- I agree to store confidential documents apart from high value devices such as tablets, laptops or mobile phones.

- I agree to return any confidential documents to the Advonet office at the next visit after case closure or as soon as the information is no longer required.

Signed …… Date …….

Name (Please print) ……..

For the purposes of the above I acknowledge receipt of:
……. x Lockable box(es)
……. x Lockable Document Pouch(es)

Signed …… Date …….

Name (Please print) ……..

The lockable box and document pouches remain the property of Advonet and must be returned at your employment with Advonet ceases.