Version History				
Version	Date	Detail	Author	Approved by Board
1.0	03/03/2013	Document created	Annie French	13 May 2013
1.1	09/08/2016	Amended	Hilary Ashton	
1.2	16/08/2016	Amended	Philip Bramson	
1.3	31/01/2017	Amended para 16	Hilary Ashton	31/01/2017
1.4	20/03/2017	Addition para 47	Hilary Ashton	
1.5	02/06/2017	Added Appendix 1	Katie Whitham	
1.6	29/09/2017	Addition of para 26	Hilary Ashton	

Confidentiality Policy

1.0 Advonet is aware that sharing information can be important for the organisation's effectiveness in achieving its goals.

2.0 In choosing when to share or not share information, and who to tell, we firstly and primarily consider the rights of the individual/s concerned.

3.0 The aim of this policy is to provide a framework for creating, and maintaining, a working environment within an atmosphere where individual personal dignity is supported and respected and to ensure that all service users are able to trust and have confidence in Advonet.

4.0 Advonet is a provider of independent advocacy and related support services. Advonet delivers services directly, sub contracts to other advocacy service providers and provides support services to the advocacy and wider voluntary sector in Leeds. This policy covers all of this work and sub contracted organisations will be required to adopt this or an equivalent policy.

5.0 Clients, paid staff, trustees and volunteers (hereafter referred to as *the individual*) have the right to expect that any information they impart:

- will only be used for the purpose for which it was given and
- not be divulged to any other people or organisations without their consent.

6.0 The policy applies to all staff, volunteers and members of the Board (hereafter referred to as *personnel*) and is intended to protect the rights of clients, members of staff, trustees, volunteers and the interests of the organisation.

7.0 This policy also covers the confidentiality of information on the internal workings and business affairs of the organisation.

8.0 All personnel have a responsibility to ensure that other personnel and service users are made aware of the confidentiality policy and understand the only circumstances where confidentiality can be breached.

9.0 Only information which is relevant and necessary should be obtained; and it should be used only for the purpose for which it was intended. It is not possible to guarantee that information will be handled solely by one member of staff but information will only be shared with other personnel on a 'need to know' basis and continue to be treated in a confidential manner.

10.0 Gossip will not be tolerated and all personnel should challenge other personnel who they believe are sharing information in this way within the organisation.

11.0 Consent may be restricted to the disclosure of specific information.

12.0 Information should **never** be shared if a wish for confidentiality is expressed in any way by an individual **except in cases where there is concern about the welfare of the person** (see Breach of Confidentiality below).

13.0 Whatever agreement is reached about sharing information, it is important that disclosure should only take place on those terms. It is vital therefore, that recipients of the information are made aware of this so they can act accordingly.

14.0 Breach of Confidentiality

15.0 Confidentiality will only be breached in exceptional circumstances where the failure to do so would place individuals in danger. In all cases individuals must be told that their confidentiality is going to be breached and given the reasons why.

16.0 Any breach of confidentiality by workers will be viewed as a disciplinary matter.

17.0 Any breach of confidentiality must be discussed and agreed with the Line Manager, a member of SMT, preferably the Office and Resources Manager (who is the Data Protection officer), or in the absence of all of these, a member of the Board. In the event of these being unavailable and the matter considered urgent the person making the decision will be required to provide high level evidence of reference to this policy.

18.0 A breach of confidentiality will only be considered in these limited circumstances:

- allegations of possible abuse,

- knowledge of criminal offences, and
- risk to the safety of the service user, volunteer, member of staff or others.

In addition there is an obligation to breach confidentiality when there is a danger of:

- injurious harm,
- fraud,
- serious crime,
- Adult or Children and Young People's Safeguarding concerns
- It is also an offence not to disclose any activities covered under the terms of the Terrorism Act 2006.

19.0 In the event of such information being disclosed the member of staff should state to the individual that it will be necessary to breach confidentiality. This will be recorded on Charity Log. Any documents pertaining to this breach in confidentiality will be uploaded to Charity Log, with permissions given to view only to the person recording the breach and their line managers. A note stating this has happened will be made in the client's history.

20.0 The individual should be given the reason why and to whom the information will be passed onto. However where for reasons of safety this is not feasible this should be discussed with the Line Manager, a member of SMT, preferably the Office and Resources Manager (who is the Data Protection officer), or in the absence of all of these, a member of the Board.

21.0 Procedure

22.0 All service users, workers and members of the Board of Trustees must be made aware of this policy at the earliest opportunity and of their right to complain if any aspect of their confidentiality is breached.

23.0 Although it is acceptable in certain situations such as team meetings, group supervisions etc to discuss particular situations or issues the identity of a particular service user should not be divulged.

24.0 Issues discussed during supervision sessions should remain confidential although staff are expected and should be enabled to discuss the details of service user's cases within supervision.

25.0 All records relating to individuals should be regarded as confidential and stored securely in the approved manner i.e. in locked filing cabinets in rooms which are locked when not in use and in accordance with the provisions of the Data Protection Act 1998. Records relating to clients will be stored on Advonet's secure database, Charity Log.

26.0 Other requirements for storing, transporting and emailing confidential information can be found in the Information Sharing Agreement, and staff party to such information should familiarise themselves with the requirements therein, the majority of which is contained in Appendix 1.

27.0 All records relating to individuals will only be available to those with the right to see them.

28.0 In accordance with the Data Protection Policy all records which are no longer required should be disposed of in the appropriate and approved manner. Records will be kept for a minimum of 7 years in line with the policy of the organisation.

29.0 Consideration should be given at all times to the physical environment in which verbal information is disclosed. In all cases it is preferable for this to take place in a designated private interview space.

30.0 All personnel should be aware of the need to ensure that telephone conversations remain as confidential as possible and with particular consideration to offices open to visitors of the public, or where telephone conversations may be overheard via other open telephone lines.

31.0 Any personal information held on the computer should not be kept longer than necessary in accordance with the Data Protection register.

32.0 Line Managers are responsible for both the day to day implementation and monitoring of this policy and the storage of confidential information within their projects in Advonet. Practices and procedures should be reviewed on a regular basis.

33.0 The need for confidentiality extends to the internal policies and business of the organisation.

34.0 Workers and members of the Board of Directors should receive a copy of the Confidentiality policy during their induction. The induction process should include training on all aspects of confidentiality and data protection and all such training should be reviewed and updated on an ongoing basis.

35.0 This policy covers all information whether obtained through face to face discussion, telephones, letters, emails and database etc.

36.0 In the event of personnel ceasing to be involved with the service there is a requirement that all records, paperwork and digital media be returned to the organisation, and access to work email accounts and the company database will be removed.

37.0 If a person is approached for information by an external organisation e.g. the police, the principle of confidentiality should be explained (i.e., that no information is given without the permission of the person it concerns). If pressed, personnel should discuss with their Line Manager or the Office and Resources Manager.

38.0 Case histories used in published articles, presentations etc shall not in any way reveal the identity of service users; pertinent details must be changed to preserve anonymity.

39.0 Photographs of individuals taken during events/activities shall not be publicised in any way without the expressed consent of the individual(s) involved.

40.0 Complaints about breaches of confidentiality can be made through Advonet's complaints procedure.

41.0 **Confidentiality in respect of personnel only**:

42.0 Commitments to confidentiality will be contained within the job descriptions and contracts for employment of all staff and within volunteer agreements.

43.0 Information requests regarding personnel will be dealt with in line with Advonet's Data Protection policy and procedures and will not be shared with third parties without that person's consent.

44.0 Personnel have a right to access their own personal details kept on record by Advonet. If a worker has left Advonet their requests should be made in writing to the Chair of the Board of Trustees and in accordance with Advonet's Data Protection policy and procedures.

45.0 Advonet may use written records when complying with any statutory obligations or Court Orders placed on it.

46.0 Discussion of personal and sensitive issues between workers and the Board of Directors may at times be necessary and is acceptable providing the information is contained within Advonet.

47.0 **Confidentiality and the Mental Capacity Act**

Information on the IMCA referral form will be shared with other agencies involved with the IMCA service in accordance with the Leeds Interagency Protocol for Sharing Information. A referral will require a decision-maker as defined by the Mental Capacity Act 2005. The IMCA will wish to talk to the decision maker about the decision to be made and the sources and types of information that the IMCA may wish to review. These discussions will be held within the parameters of this policy.

Appendix 1

Advonet
Providing Independent Advocacy & Related Support

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.