Data Protection and Personal Information Policy

Scope

Advonet is the lead partner in a consortium of advocacy provider agencies. Advonet delivers direct advocacy services, works in partnership with other advocacy providers and provides support services to the advocacy and wider voluntary sector in Leeds. This policy refers to all of Advonet's work and sub contracted and consortium organisations will be required to adopt this policy.

This policy applies to all staff and volunteers of Advonet and its partners.

Policy Statement

- Advonet complies fully with the Data Protection Act 2018 in respect of its management of personal data. This policy sets out how we seek to protect personal data and ensure that staff understand the rules governing their use of personal data to which they have access in the course of their work.

- General Data Protection Regulation ('GDPR') provisions came into effect from 25 May 2018.

- 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.

- 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).

- The Board of Trustees will ensure that personal data is only obtained and processed in line with seven key principles set out in the GDPR. All personal data will be:

- Processed fairly and lawfully and in a transparent way. We will be clear how and why we use the personal data we obtain;

- Obtained in a clear and open way so individuals are clear why we are collecting their personal data and what we will do with it.
- Adequate and limited to what is necessary to enable Advonet to provides services.
- Accurate, and updated as necessary.
- Held by Advonet will be able to be accessed by individuals
- Kept for no longer than is necessary
- Held securely and processed in a manner that ensures appropriate security of the personal data.

- 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 Data Protection Impact Assessment ('DPIA') will be undertaken before personal data is shared other than in compliance with Advonet's registration.

- The Finance Director of Advonet is the designated Data Protection Officer with responsibility for ensuring that data is used in accordance with the designated policies, procedures and practices of Advonet and that a DPIA is undertaken whenever required.

- The Board of Trustees recognises the rights that GDPR provides to individuals in respect of their personal data, including but not limited to, their right to be informed about their data is collected and processed, the right to access, rectify or request erasure of their data.

- This policy applies to all personal data processed by Advonet.

1 Definitions

The Act provides conditions for the processing of any personal data. It also makes a distinction between personal data and special categories of personal data (which are more sensitive in nature). Special categories of data require a higher level of protection.

1.1 Personal data is defined as data relating to a living individual who can be identified:

- Directly from that data;
- Indirectly from 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.

1.2 Special categories of 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
- Health data
- Biometric data
- Sexual life or sexual orientation
- Criminal proceedings or convictions.

1.3 Processing: includes collecting, disclosing, recording, holding, using, altering, storing, erasing or destroying personal information. The definition is very wide and covers virtually any action carried out on a computer.

1.4 Data controller: someone who decides what data to process and why.

1.5 Data processor: someone who does not have a purpose of your own for processing the data and they only process and act on a client's instructions.

2 Processing of personal and special categories of personal information

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

- Observe fully the conditions regarding the fair, lawful and transparent collection and use of personal information.
- Specify the purpose for which information is used.
- Collect and process appropriate information and only to the extent that it is needed to provide our services or to comply with any legal or contractual requirements.
- Ensure that appropriate privacy notices are in place advising staff, and others, how and why their data is being processed, and in particular, advising data subjects of their rights.
- Ensure the quality of information used.
- Apply Advonet's data retention policy so that personal data is only held for as long as necessary.
- Ensure personal information is processed securely and ensure that personal data can only be accessed by those who need to
- 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 a month of making the request
    - The right to object to their personal data being processed in certain circumstances
    - The right to correct, rectify or erase information regarded as wrong information.
    - The right to have personal data erased

- The right to data portability (to obtain and reuse their personal data for their own purposes across different services).
- Rights related to automated decision-making including profiling.

2.1 General data protection responsibilities for all staff, volunteers and partners

- Everyone must take responsibility for following good data protection practice.
- Managers must supervise their teams.
- Everyone should ensure they know the process to follow if they receive an enquiry about accessing personal information.

- Queries about personal information must be promptly and courteously dealt with.
- 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.
- Everyone has responsibility for reporting any data protection breaches or concerns to the Data Protection Officer or to their Line Manager, who will inform the Data Protection Officer.

2.2 Specific responsibilities: all personnel

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 e.g. locked filing cabinets or lockable security wallets.
- Personal data and special categories of personal data held on computers and computer systems is protected by the use of secure passwords
- Individual passwords to all systems and pieces of IT equipment should be such that they are not easily compromised e.g. 'password' and '1234' are not appropriate.
- All paper records containing personal information, once they are no longer required, must be shredded (either onsite or via a third-party confidential shredding service).
- 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 data protect ion laws. Any breach of any provisions of data protection laws 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.

2.3 Specific responsibilities: Data Protection Officer

- Ensure that Advonet's registration with the Information Commissioner is maintained.
- Review the Data Protection Register annually and notify the Information Commissioner of any changes.

- Ensure the data protection policy is implemented and forms part of the trustee, staff and volunteer induction.
- Ensure that access to personal information held on databases and servers is restricted so that users can only access information necessary for the role.
- Carry out compliance checks to ensure adherence with the Data Protection Act and General Data Protection Regulations throughout the organisation.
- Ensure that contracts are in place with any processor used to handle data on Advonet's behalf.
- Deals with all requests from current and former service users, applicants and personnel to access information of files held about them by Advonet.
- Maintain a central register of any potential or actual data breaches of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. The Data Protection Officer shall promptly assess the risk to people's rights and freedoms and if appropriate, report breaches to the Information Commissioner.
- Ensure appropriate back-up and disaster recovery solutions in place.

2.5 Processing personal data (outside normal service use)

- There may be rare occasions when it is appropriate to share an individual's personal data.
- If you consider this to be necessary then you must inform the DPO, or in their absence a member of the Senior Management Team, who will perform a DPIA.
- 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.

3 Responding to a request for Personal Information/ Subject Access Request

This is a request by current and former service users, applicants, staff and volunteers to access any personal information held about them by Advonet. The request can be made verbally or in writing (which could be a letter, an email or via social media):

- Advonet does not charge an administration fee for a request for personal information.
- A request can be made to any one in the organisation. If you think that you have received a request for personal information then staff must ensure that the Standard Access Request ('SAR') form is completed. If the request is verbal then the staff member taking the request is responsible for taking all the information required to complete the form. A copy of SAR form can be found as an Appendix to this policy.
- Advonet reserves the right to refuse requests that are manifestly unfounded or excessive. In this situation, Advonet will provide a full explanation to the requestor detailing why, including notifying the requestor of their right to complain to the ICo and their ability to enforce their right through a judicial remedy. Such response will be provided within a month of the request being made to Advonet.
- Information provided will include both the information held and details of the processing carried out on that information.
- 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. This means some requests will contain documents with information redacted which is not personal to the person making the request.
- Advonet will respond to all cases within one month of receiving the request. In the event, that a request is particularly complex or involves a significant amount of data then Advonet may seek to extend the deadline for a response by up to a further two months. If this is required the requestor will be notified within one month of the original request, in writing of the reason why.
- Advonet may require an individual to provide proof of identity to confirm who they are.
- Requests made on behalf of others will only be processed where Advonet is satisfied that the third party making the request is entitled to act on behalf of the individual. It is the responsibility of the third party to provide evidence of this entitlement.

4 Marketing

- Marketing refers to promotional activities. Where personal information held by Advonet is used for the purpose of marketing or distribution lists, the list of targets will be contacted for consent to ensure that active consent is in place. This exercise will be performed annually.
- All individuals can stop their personal information being used for direct marketing at any time. Requests must be complied with and within a reasonable period of time – no longer than one calendar month.
- Advonet will tell individuals what their personal information will be used for, and in particular:
    - is the name of the organisation
    - Why we want their data
    - What we will do with it
    - Anything else necessary to make sure the information is being used fairly and transparently – 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
    - That an individual can withdraw their consent at any time.
- Advonet must give individuals the chance to opt out of receiving marketing on each occasion the organisation contacts them by providing appropriate contact details for Advonet.

5 Electronic Communications

- Telephone marketing: Advonet will 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.
- Automated calls: Advonet will not make automated calls without getting the individual's permission first.
- Electronic mail – do not send electronic mail marketing without obtaining the individual's permission first. (Applies only to messages sent to individuals).
- 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.
- All calls made should identify that Advonet and the address and telephone number of the organisation should be given if requested.
- An individual can withdraw permission at anytime and their request must be complied with as soon as possible and within one calendar month of receiving the request.

6 Data Standards (Accuracy, Minimising and Storage Limitation)

Accuracy

- All personal information should be accurate, and where necessary kept up to date. This is particularly the case if having incorrect information could have implications for the individual.
- At the recruitment stage, Advonet will take reasonable steps to check the identity and reliability of personnel including obtaining references and checking that these and an applicant's qualifications are valid.
-
- Where records include a record of opinion this is not necessarily inaccurate personal data, if the individual disagrees with it, or if it is later proved to be incorrect.
- Opinions should be clearly identified as such in records and where appropriate, whose opinion it is.
- An opinion which contains factual information which is incorrect can be challenged.
- 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.
- 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

Minimisation

- 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.
- 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.

Storage Limitation

- Personal information should not be kept for longer than is necessary to do the job it is intended for, unless there is a different and valid need to keep a comprehensive record (see Data Retention policy in Appendix).

7 Data Protection

Advonet will process personal data securely to prevent such data being accidentally or deliberately compromised.

7.1 Organisation security measures

Advonet:

- Carries out an information 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.
- Include a confidentiality and data protection clause in all employees' contracts.
- Ensure that there is an up to date business continuity plan
- Ensure that the security policy is kept up to date.
- Ensure that Advonet premises are kept secure
- Keep staff informed and trained as to what their responsibilities are.
- Perform periodic checks to ensure that security measures remain appropriate and are being followed.
- If access is given to anyone outside Advonet, e.g. for computer maintenance, ensure that security is in place to oversee what they do.
- Using a third-party organisation to process personal information increases security risk. The following measures are in place to mitigate this risk:
    - Third party organisations are requested to confirm their policies and procedures comply with GDPR in relation to 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.
    - Carry out a periodic check of security arrangements to ensure that these are still appropriate and up to date.

7.2 Technical security measures

- A high proportion of security incidents are shown to be personnel-related.
- Train all staff and volunteers in their responsibilities about personal information.
- Ensure staff and volunteers 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 and that staff and volunteers understand the proper procedure to identify a caller.

- Ensure staff and volunteers understand that it is a criminal offence to deliberately give out personal information without the consent of Advonet and that they can commit a criminal offence if they try to access or obtain personal information without the authority of Advonet.
- All visitors to Advonet offices must be supervised at all times when on the premises. This is the responsibility of the individual that they are visiting.
    - Physical security is also important. Physical security in place includes: Premises are secure with good quality locks and doors. They can only be accessed with an entry code
    - Alarm is activated by last person leaving the office
    - All paper based personal data should be locked in a secure filing cabinet or drawer.
    - All computers should be logged out of and switched off before leaving the premises.
    - Laptops, tablets and phones should be locked up if in the office or kept in a secure location if off-site.
    - All personal data which is no longer required should be shredded.
    - When transporting client data outside the office, paper copies should be transported securely using lockable wallets.

7.3 Computer security

- Advonet will ensure that there are checks and balances in job roles to prevent unauthorised change or fraud.
- Advonet will appoint an IT firm to support all hardware and software and ensure that IT systems protection is kept up to date.
- Advonet will ensure equipment is maintained to prevent against loss of or interruption to work.
-
- All staff should use their individual log-on details to access Advonet computer network and databases.
- All passwords should be unique and not be easily guessed.
- Advonet will control access to information that only certain people should see – for example by setting privileges to certain parts of the network.
- 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)
- Deletion procedures will be effective, especially on equipment which is being discarded.
- Regular backups of information held on computer are taken.

- 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.
- All staff must immediately notify the DPO (or in their absence a member of the Senior Management Team) if they lose or misplace any item of equipment (e.g. phone, laptop or tablet) that holds personal data. This is to ensure that the equipment can be blocked from accessing Advonet's systems as soon as possible.

8 Data Protection and the use of Interpreters/ Signers

- Interpreters and signers are placed in a privileged position and as such are bound by Advonet's confidentiality and data protection policies 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.

9 Escalating Concerns

If there are any concerns over any matter relating to Data Protection then the Data Protection Officer should be informed. Complaints and concerns can be escalated through the Advonet Complaints Policy and Procedure. If the outcome of the complaints procedure is not satisfactory then an individual can raise their concerns directly with the Information Commissioners Office.

The Data Protection Officer can be contacted at Advonet by:

Writing to: Advonet, Unity Business Centre, 26 Roundhay Road, Leeds LS7 1AB
Emailing: clare.dearostegui@advonet.org.uk

Appendix 1
DATA RETENTION GUIDELINES

1. Introduction

This statement sets out the responsibilities and activities in regard to the management of Advonet's records. This policy takes account of the following legislation:

- GDPR 2018
- Data Protection Act 2018
- Human Rights Act 1998
- Freedom of Information Act 2000
- The Police Act 1997
- Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975

2. GENERAL PRINCIPLES ON RETENTION AND ERASURE

Advonet's approach to retaining records is to ensure that it complies with the data protection principles referred to in these guidelines and, in particular, to ensure that:

Records are regularly reviewed to ensure that they remain adequate, relevant and limited to what is necessary. Records are kept secure and are protected against unauthorised or unlawful processing and against accidental loss, destruction or damage. Where appropriate Advonet uses anonymisation to prevent identification of individuals.

- When records are destroyed, whether held as paper records or in electronic format, Advonet will ensure that they are safely and permanently erased.

2.1 RETENTION AND ERASURE OF RECRUITMENT AND EMPLOYMENT RECORDS

Advonet has regard to recommended retention periods for particular employment records set out in legislation, referred to in the table below.

However, it also has regard to legal risk and may keep records for up to seven years (and in some instances longer) after your employment or work with us has ended.

All personnel information on staff employed by Advonet should be filed centrally (in Finance Director's office). These files should be stored in a locked cabinet, and be accessible only to the individual concerned, the HR administrator, their line manager and any relevant senior managers. Files should contain all information relating to employment issues and terms and conditions of service, including the individual's application form, references and sickness records. Information relating to DBS disclosures is found in a separate policy.
Any electronically held personnel records must be password protected and stored so that only authorized personnel may access them.
Any electronically held information that is subject to this policy must be encrypted if it is being transferred electronically.

Type of employment record	**Retention period**
Recruitment records These may include: Completed online application forms or CVs. Equal opportunities monitoring forms. Assessment exercises or tests. Notes from interviews and short-listing exercises. Pre-employment verification of details provided by the successful candidate. For example, checking qualifications and taking up references. (These may be transferred to a successful candidate's employment file.) Criminal records checks. (These may be transferred to a successful candidate's employment file if they are relevant to the ongoing relationship.)	Six months after notifying candidates of the outcome of the recruitment exercise.
Immigration checks	Three years after the termination of employment.

Contracts	
These may include: Written particulars of employment. Contracts of employment or other contracts. Documented changes to terms and conditions.	While employment continues and for ten years after the contract ends.
Collective agreements	
Collective workforce agreements and past agreements that could affect present employees.	Any copy of a relevant collective agreement retained on an employee's record will remain while employment continues and for ten years after employment ends.
Payroll and wage records	
Payroll and wage records Details on overtime. Bonuses. Expenses. Benefits in kind.	These must be kept for at least three years after the end of the tax year to which they relate. However, given their potential relevance to pay disputes they will be retained for seven years after employment ends.
Current bank details	Bank details will be deleted as soon after the end of employment as possible once final payments have been made
PAYE records	These must be kept for at least three years after the end of the tax year to which they relate. However, given their potential relevance to pay disputes they will be retained for seven years after employment ends.
Payroll and wage records	These must be kept for six years from the financial year-end in which payments were made. However, given their

	potential relevance to pay disputes they will be retained for seven years after employment ends.
Records in relation to hours worked and payments made to workers	These must be kept for three years beginning with the day on which the pay reference period immediately following that to which they relate ends. However, given their potential relevance to pay disputes they will be retained for seven years after the working relationship ends.
Travel and subsistence.	While employment continues and for seven years after employment ends.
Record of advances for season tickets and loans to employees	While employment continues and for seven years after employment ends.
Personnel records	
These include: Qualifications/references. Consents for the processing of special categories of personal data. Annual leave records. Annual assessment reports. Disciplinary procedures. Grievance procedures. Death benefit nomination and revocation forms. Resignation, termination and retirement.	While employment continues and for ten years after employment ends.
Records in connection with working time	

Working time opt-out	Three years from the date on which they were entered into.
Records to show compliance, including: Time sheets for opted-out workers. Health assessment records for night workers.	Three years after the relevant period.
Maternity records	
These include: Maternity payments. Dates of maternity leave. Period without maternity payment. Maternity certificates showing the expected week of confinement.	Four years after the end of the tax year in which the maternity pay period ends.
Accident records	
These are created regarding any reportable accident, death or injury in connection with work.	For at least four years from the date the report was made.

Client Record Retention Periods

- Records will be retained for a minimum 10- or 12-year period to protect the organisation and to facilitate access to records or personnel information from appropriate persons. Original records required by funders will be retained in line with specific contract requirements.
- The record keeping system must be maintained so that the records are properly stored and protected, can easily be located and retrieved.
- A record keeping system should;
    - Monitor the movement and location of records so that they can be easily retrieved and updated
    - Promote control of access to confidential information
    - Identify vital records

Identification of roles and responsibilities

- The SMT is responsible for approving a framework for managing and overseeing its duties in relation to records management a set out in this policy.
- The CEO/SMT is responsible for the management of these records and in accordance with this policy all staff will be made aware of their record keeping responsibilities.
- Advonet will advise all service areas and individuals on the retention and management of their records, and where appropriate will take custody of those records.
- Advonet employees will be responsible for creating and maintaining records in relation to their work that are authentic, objective and reliable in line with:
    - Quality Performance Mark
    - Contracts and other funding requirements
    - Code of Conduct
    - Confidentiality policy

Training and Awareness

- Advonet employees are involved in creating; maintaining and using records, it is vital that everyone understands record management responsibilities as set out in this policy. Staff responsible for managing records will be appropriately trained so that they understand the need for records management.

A training programme will be established to ensure that all relevant staff are aware of their obligations around GDPR, Freedom of Information and Records Management.

3. Disposal of Records

- With increasing public access to records and the Freedom of Information Act, disposal of records will only happen as part of a managed process.
- The system will ensure that:
    - Appropriate records are reviewed and disposed of / transferred each year following procedures for destroying confidential material and magnetic media. Personnel files will be destroyed 10 years after an employee has left. Client files will normally be destroyed 12 years after contact ceases.
    - Documentation of the disposal/transfer of records is completed and retained.
    - Records subject to a Freedom of Information request are not destroyed.

Appendix 2
Standard Access Request Form
You do not have to use this form but it will help us to give an accurate response to your subject access request.

Please complete the table below and return the form by post or email to the Data Protection Officer at Advonet, Unity Business Centre, 26 Roundhay Road, Leeds LS7 1AB or clare.dearostegui@advonet.org.uk

Date request is made	
Name of Person making request	
Address	
Email address	
Preferred response format (post or email)	
Other name(s) by which you have been known (if applicable)	
Relationship to Advonet (e.g. service user, employee)	
Is the request for the person's own personal information?	Yes/ No (circle one) If No, we will need evidence showing the person making the request is allowed to access another person's personal information. Please speak to the Data Protection Officer if you are unsure.
Description of your request, including information to help us locate the personal data you seek. Please give as much information as possible such as dates and which service you used.	

Please note you may be asked to provide proof of your identity.