

**Data Protection and Personal Information Policy**

# Scope

The Advonet Group is the lead partner in a consortium of advocacy provider agencies. The Advonet Group 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 this work and subcontracted and consortium organisations will be required to adopt this policy.

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

# Policy Statement

* The Advonet Group complies fully with the Data Protection Act 1998 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.
* GDPR provisions are in effect from 25 May 2018. Where not specified previously in this policy, Appendix 1 sets out the provisions that will be in effect on or before 25 May 2018.
* The Board of Trustees ensures that The Advonet Group is suitably registered with the Information Commissioner and that The Advonet Group’s Data Controller Registry information is maintained and updated when appropriate.
* The Board of Trustees confirms that The Advonet Group 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:
	+ 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 The Advonet Group, 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.
	+ 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 The Advonet Group’s registration.
	+ The Finance Director of The Advonet Group is the designated Data Protection Officer with responsibility for ensuring that data is used in accordance with the designated policies, procedures and practices of The Advonet Group and that a Privacy Impact Assessment is undertaken whenever required.
	+ 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 The Advonet Group.

# 1 Definitions

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

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

**1.3 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.

**Procedure**

# 1 Handling of personal/sensitive information

The Advonet Group 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 a month of making. the request.
	+ The right to prevent processing in certain circumstances.
	+ The right to correct, rectify, block or erase information regarded as wrong information.

# 2 Responding to a request for Personal Information

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

* The Advonet Group does not charge an administration fee for a request for personal information.
* The Advonet Group reserves the right to refuse requests that are manifestly unfounded or excessive. In this situation, The Advonet Group will provide a full explanation to the requestor detailing why, including notifying the requestor of their right to complain. Such response will be provided within a month of the request being made to The Advonet Group.
* 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.
* The Advonet Group will respond as soon as possible to the request and in all cases within one month of receiving the request.

# 3 Responsibilities of The Advonet Group

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

# 4 General responsibilities

* Everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice and are 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 personnel or a member of the public can be made aware of what to do.
* Queries about handling personal information are promptly and courteously dealt with.
* Methods of handling personal information are regularly assessed and evaluated.
* Performance with handling personal information is regularly assessed and evaluated.
* 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.

# 5 Specific responsibilities

All personnel within The Advonet Group 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 The Advonet Group must:
	+ - * + Ensure that they and all of their personnel who have access to personal data held or processed for or on behalf of The Advonet Group 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 The Advonet Group and that individual, company, partner or firm.
				+ Allow data protection audits by The Advonet Group of data held on its behalf (if requested).
				+ As far as possible, protect The Advonet Group against any prosecutions, claims, proceedings, actions or payments of compensation or damages.
				+ All representatives of The Advonet Group who are users of personal information will be required to confirm that they will abide by the requirements of the Act.

# 6 Responsibility of Data Protection Officer

* Ensure that The Advonet Group’s registration with the Information Commissioner is maintained.
* Review the Data Protection Register annually and notify the Information Commissioner of any changes.
* Ensure the policy is implemented.
* Ensure all workers and Board members are trained in data protection, at least by ensuring they have read and understand this policy.
* Develop best practice guidelines on the gathering, use, storage, retention and sharing of personal information.
* Carry out compliance checks to ensure adherence with the Data Protection Act and General Data Protection Regulations throughout the organisation.
* Deals with all requests from current and former service users, applicants and personnel to access information of files held about them by The Advonet Group.

# 7 Sharing Personal Information

* 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).
* 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.

# 8 Personal information and marketing

* Marketing refers to promotional activities. Where personal information held by The Advonet Group 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 28 days.
* The Advonet Group 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.
* The Advonet Group must give individuals the chance to opt out of receiving marketing on each occasion the organisation contacts them.

# 9 Privacy and Electronic Communications

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

# 10 Identity and contact information

* Identify The Advonet Group in any marketing message
* Provide appropriate contact details so that the individual or organisation receiving the message can contact The Advonet Group. This should be a postal address, email address or telephone number.
* For telephone marketing, identify The Advonet Group. Give address or telephone number if asked for it.

# 11 Change

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

# 12 Professional Opinion

* 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.
* 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.
* 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.
* 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.
* 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.

# 13 Security

The Advonet Group will review the security of the personal information it controls by asking: Is processing carried out by The Advonet Group, 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 The Advonet Group – in cost to reputation and to the trust of clients.
* The Data Protection Officer must have day-to-day responsibility for security measures.

# 14 Security measures – the Data Protection Officer

The Data Protection 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.
* Unless this is done, security will quickly become flawed and out of date.

# 15 Security measures – the organisation

The Advonet Group will:

* 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.
* Use the risk assessment to inform the changes to be made.
* Ensure the officer responsible has the standing and resources to make sure the job gets done.
* Ensure the organisation has security procedures in place for personnel to follow.
* Ensure there is co-ordination on security matters between key people in The Advonet Group.
* Check that personnel are taking their security responsibilities seriously.
* Ensure that a procedure is in place to make sure that security incidents are investigated and lessons learned.
* If access is given to anyone outside The Advonet Group, 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 The Advonet Group.
			* Have a written contract that sets out what The Advonet Group 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 The Advonet Group.
			* 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.

# 16 Security issues – personnel

* A high proportion of security incidents are shown to be personnel-related. The Advonet Group will take all reasonable steps to ensure the reliability of personnel who have access to personal information.
* 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.
* Include in the employment contract or in a confidentiality agreement what personnel can and cannot do with the personal information they handle.
* 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.
* 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.
* Ensure personnel understand that it is a criminal offence to deliberately give out personal information without the consent of The Advonet Group. Ensure personnel know that they can commit a criminal offence if they try to access or obtain personal information without the authority of The Advonet Group.
* Physical security: emphasis is put on technical security measures to protect computerised information, but physical security is just as important.
* Ensure that premises are secure with good quality doors and locks, and a well-lit exterior. The last person leaving The Advonet Group’s offices should activate the alarm system.
* Lock up paper-based information at night in a secure filing cabinet or cupboard.
* Prevent people being able to see the computers and screens from outside.
* Ensure control of access to the premises is appropriate. Supervise visitors and consider keeping these to public areas.
* Lock up laptops and other portable equipment and computer media like discs and memory sticks at night.
* Dispose of paper waste containing personal information securely by shredding.

# 17 Computer security

* 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.
* A networked system needs more controls than a stand-alone computer.
* A stand-alone that is connected to the internet and email will need more protection than one that is not.

# 18 Managing security on the computer system

* The Advonet Group will manage the operation of the computer system with procedures and document change.
* The Advonet Group will ensure that there are checks and balances in job roles to prevent unauthorised change or fraud.
* 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.
* The Advonet Group will ensure equipment is maintained to prevent against loss of or interruption to work.
* 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.
* The Advonet Group will control access to information that only certain people should see – for example, by setting privileges to certain parts of the network.
* There will be strategies to control access to computers when they are unattended e.g. by ensuring auto locking of inactive computers.
* The Advonet Group will obtain security updates for software to fix any vulnerability which has been discovered.
* 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.
* 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.
* If using internet or email, workers must ensure that firewall and virus protection is up to date. The Advonet Group will ensure there are systems in place to use if the computers become infected or hacked into.
* The Advonet Group will warn personnel about the insecurity of email and ensure that any sensitive personal information sent electronically is encrypted or sent by other means.

# 19 Data Protection and the use of Interpreters

* Interpreters are placed in a privileged position and as such are bound by The Advonet Group’s rules of confidentiality and data protection at all times. As with all Advonet Group staff and volunteers, any breach of confidentiality or misinformation would be dealt with through The Advonet Group’s 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 The Advonet Group. Any agencies used to provide interpreting services for The Advonet Group are responsible for training their staff in Data Protection and Confidentiality.

# 20 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 Group’s Complaints Policy and Procedure. If the outcome of this is not satisfactory then they should approach the Information Commissioners Office.

**Appendix 1: GDPR Provisions**

# Privacy Notice - transparency of data protection

Being transparent and providing accessible information to individuals about how we will use their personal data is important for our organisation. For all types of personal data collected, the following information will be documented:

* Who is collecting the data.
* How it is collected.
* Why it is being collected.
* How it will be used.
* Who it will be shared with.
* Details of transfers to outside of the UK and safeguards.
* Retention period.

# Conditions for processing

We will ensure any use of personal data is justified using at least one of the conditions for processing and this will be specifically documented. All staff who are responsible for processing personal data will be aware of the conditions for processing. The conditions for processing will be available to data subjects in the form of a privacy notice.

# 1. Justification for personal data

We will process personal data in compliance with all six data protection principles.

We will document the additional justification for the processing of sensitive data, and will ensure any biometric and genetic data is considered sensitive.

# 2. Consent

For data that we collect which is subject to active consent by the data subject, this consent can be revoked at any time.

# 3. Criminal record checks

Any criminal record checks are justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject.

# 4. Data portability

Upon request, a data subject should have the right to receive a copy of their data in a structured format. These requests should be processed within one month, provided there is no undue burden and it does not compromise the privacy of other individuals. A data subject may also request that their data is transferred directly to another system. This must be done for free.

# 5. Right to be forgotten

A data subject may request that any information held on them is deleted or removed, and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies.

**Privacy by design and default**

Privacy by design is an approach to projects that promote privacy and data protection compliance from the start. The DPO will be responsible for conducting Privacy Impact Assessments and ensuring that all IT projects commence with a privacy plan.

When relevant, and when it does not have a negative impact on the data subject, privacy settings will be set to the most private by default.

# 6. International data transfers

No data may be transferred outside of the EEA without first discussing it with the data protection officer. Specific consent from the data subject must be obtained prior to transferring their data outside the EEA.

# 7. Data audit and register

Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

# Reporting breaches

All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:

* Investigate the failure and take remedial steps if necessary.
* Maintain a register of compliance failures.
* Notify the Supervisory Authority (SA) of any compliance failures that are material either in their own right or as part of a pattern of failures.

# Monitoring

Everyone must observe this policy. The DPO has overall responsibility for this policy. They will monitor it regularly to make sure it is being adhered to.

# Appendix 2



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 The Advonet Group 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 Group office according to processes agreed with your line manager.

# The Advonet Group 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 The Advonet Group. Specifically:

* I agree to store confidential documents in a secure location when away from The Advonet Group 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 Group 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 The Advonet Group and must be returned when your employment with The Advonet Group ceases.

**Appendix 3**

# DATA RETENTION GUIDELINES

## 1. Introduction

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

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

## 2. Aims

The guidelines are intended to ensure that Advonet processes personal data in the form of employment and other records in accordance with the personal data protection principles, in particular that:

* Personal data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.
* Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. When personal data is no longer needed for specified purposes, it is deleted or anonymised as provided by these guidelines.
* Personal data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.
* Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.
* Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

The Data Protection Officer (DPO) is responsible for overseeing these guidelines.

Any questions about the operation of the guidelines should be submitted to the DPO.

# GENERAL PRINCIPLES ON RETENTION AND ERASURE

The Advonet Group'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 to facilitate you working for The Advonet Group.
* Records are kept secure and are protected against unauthorised or unlawful processing and against accidental loss, destruction or damage. Where appropriate The Advonet Group uses anonymisation to prevent identification of individuals.
* When records are destroyed, whether held as paper records or in electronic format, The Advonet Group will ensure that they are safely and permanently erased.

# EMPLOYEE & VOLUNTEER RECORDS: RETENTION AND ERASURE OF RECRUITMENT DOCUMENTS

The Advonet Group retains personal information following recruitment exercises to demonstrate, if required, that candidates have not been discriminated against on prohibited grounds and that recruitment exercises are conducted in a fair and transparent way.

The Advonet Group’s candidate privacy notice advises candidates how long The Advonet Group expects to keep their personal information for, once a recruitment decision has been communicated to them. This is likely to be for six months from the communication of the outcome of the recruitment exercise which takes account of both the time limit to bring claims and for claims to be received by The Advonet Group.

Information relating to successful candidates will be transferred to their employment record with The Advonet Group. This will be limited to that information necessary for the working relationship and, where applicable, that required by law.

Following a recruitment exercise information, in both paper and electronic form, will be held by the HR function Destruction of that information will take place in accordance with these guidelines.

# RETENTION AND ERASURE OF EMPLOYMENT RECORDS

The Advonet Group 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.

|  |  |
| --- | --- |
| **Type of employment record** | **Retention period** |
| Recruitment records - these may include: * Completed online application forms.
* Equal opportunities monitoring forms.
* Assessment exercises or tests.
* Notes from interviews and shortlisting 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 seven 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 seven 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 seven 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**  |   |
| 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.  |
| **Volunteer records**  |   |
| These will comprise recruitment, supervision, review records etc.  | Volunteer records will be kept in line with staff records (i.e. maximum of 7 years).  |
| **Client Record**  |   |
| These will compromise records of our contacts with clients.  | Client Records should be retained for a 12-year period to protect the organisation and to facilitate access to records or personnel information from appropriate persons.  |
| **Funding Records**   |   |
| These are funding agreements, contracts and reports and related documents detailing the work carried out to meet them.  | Original records required by funders will be retained in line with specific contract requirements.  |

**Storage of Information**.

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.
* All personnel information on staff employed by The Advonet Group 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, his/her 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.
* Any transfer of data must be monitored and systems put in place to ensure safe receipt.

## Identification of roles and responsibilities

* The SLT 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/SLT 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.
* The Advonet Group 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 Group 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 Group 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.

## 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 4



**Potential Data Protection Breach**

**Name of staff member completing the form:**

**Date of incident:**

|  |  |  |
| --- | --- | --- |
| **Phases of Response**  | **ICO advice**  |  |
| **Containment and recovery**  | ***Develop a plan including damage limitation measures***  | **What happened (describe)? What action has taken place to resolve it?**  |
| **Risk assessment**  | ***Assessment of risks: What are the risks associated with the breach? These are likely to affect what you do once the breach has been contained. In particular, you should assess the potential adverse consequences for individuals; how serious or substantial these are; and how likely they are to happen.***  | **What are the risks?** |
| **Notification of breaches**   | **Informing people about an information security breach can be an important part of managing the incident, but it is not an end in itself.**  | **How serious is the data breach?** To determine the seriousness – we should consider 1. **volume** (e.g. one off human error = low or database failure = high)
2. **detriment to the affected individual**
 |
|  | **You should be clear about who needs to be notified and why. You should, for example, consider notifying the individuals concerned; the ICO; other regulatory bodies; other third parties such as the police and the banks; or the media.**  | **c. Sensitivity** (e.g. sharing of highly sensitive personal data) ‘  |
| **Evaluation and response**  | **It is important that you investigate the causes of the breach and also evaluate the effectiveness of your response to it. If necessary, you should then update your policies and procedures accordingly**  | **Learning from incident and planned** **action**    |

**Date agreed with manager:**

**Date for review** (i.e. to check planned action has taken):

**Date submitted to Advonet’s Data Protection Officer:**