

ABBNEYFIELD SCOTLAND LIMITED

DATA PROTECTION POLICY

This Policy sets out important information about:

- the data protection principles with which we, Abbeyfield Scotland, must comply;
- what is meant by personal information and sensitive personal information;
- how we gather, use and (ultimately) delete personal information and sensitive personal information in accordance with the data protection principles;
- where more detailed privacy information can be found;
- rights and our obligations in relation to data protection; and
- the consequences of failure to comply with this Policy.

1 Introduction

- 1.1 We obtain, keep and use personal information about our service users (and their next of kin), job and volunteer applicants, current and former employees and volunteers, contractors, suppliers, business contacts, consultants, Board members and donors for a number of specific lawful purposes relevant to our activities and functions as a registered social landlord and charity in Scotland.
- 1.2 This Policy sets out how we comply with our data protection obligations and seek to protect personal information that we handle and use as part of our activities and functions as a registered social landlord and charity in Scotland, regardless of the medium on which that personal information is stored. The purpose of the Policy is also to ensure that staff understand and comply with the rules governing the collection, use and deletion of personal information to which they may have access during their work with us.
- 1.3 We are committed to complying with our data protection obligations, and to being concise, clear and transparent about how we obtain and use personal information and how (and when) we delete that information once it is no longer required.
- 1.4 We recognise that the correct and lawful treatment of personal information will maintain confidence in our organisation and is conducive to successful business operations. Protecting the confidentiality and integrity of personal information is a critical responsibility that we always take seriously. We are exposed to potential fines of up to EUR 20 million or 4% of our total annual turnover, whichever is higher and depending on the breach, for failure to comply with the provisions of data protection legislation.

- 1.5 Our Data Protection Officer (DPO) is responsible for informing and advising us and our staff on our data protection obligations, and for monitoring compliance with those obligations and with our policies. If members of staff have any questions or comments about the content of this Policy or if they need further information, they should contact the DPO.

2 Scope

- 2.1 This Policy applies to the personal information of service users (and their next of kin), job and volunteer applicants, current and former employees and volunteers, contractors, suppliers, business contacts, consultants, Board members and donors.
- 2.2 Staff should refer to our transparency statements and our other relevant policies, including the Information Security Policy, the Data Security Breach Management Policy, and Response Procedures for Data Subject Requests, which contain further information regarding the protection of personal information.
- 2.3 We will review and update this Policy in accordance with our data protection obligations and we may amend, update or supplement it from time to time.

3 Definitions

For the purposes of this Policy:

criminal records information	means personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures;
data breach	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information;
data subject	means an individual to whom the personal information relates;
personal information	means information relating to an individual, who can be identified (directly or indirectly) from that information;
processing	means obtaining, recording, organising, storing, amending, retrieving, disclosing and/or destroying personal information, or using or doing anything with it; and

sensitive personal information

means personal information about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetics information, biometric information (where used to identify an individual) and information concerning an individual's health, sex life or sexual orientation.

4 Data protection principles

4.1 We will comply with the following data protection principles when processing personal information in carrying out our activities and functions:

4.1.1 we will process personal information lawfully, fairly and in a transparent manner;

4.1.2 we will collect personal information for specified, explicit and legitimate purposes only, and will not process it in a way that is incompatible with those legitimate purposes, unless the processing has been first notified to the data subject;

4.1.3 we will only process personal information that is adequate, relevant and necessary for the above specified, explicit and legitimate purposes;

4.1.4 we will keep accurate and up to date personal information, and take reasonable steps to ensure that inaccurate personal information is deleted or corrected without delay;

4.1.5 we will keep personal information for no longer than is necessary for the purposes for which the personal information is processed; and

4.1.6 we will take appropriate technical and organisational measures to ensure that personal information is kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

5 Basis for processing personal information and sensitive personal information

5.1 In relation to any processing activity, we will, before the processing starts for the first time, and then regularly while it continues:

5.1.1 review the purposes of the processing activity, and select the most appropriate lawful basis (or bases) for that processing i.e.

(a) that the data subject has consented to the processing;

(b) that the processing is necessary for the performance of a contract between us and the data subject;

- (c) that the processing is necessary for compliance with a legal obligation to which we are subject;
 - (d) that the processing is necessary for the protection of the vital interests of the data subject or another person; or
 - (e) that the processing is necessary for the purposes of our legitimate interests or a third party, except where those interests are overridden by the interests or fundamental rights and freedoms of the data subject;
- 5.1.2 except where the processing is based on consent, satisfy ourselves that the processing is necessary for the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose);
- 5.1.3 document our decision as to which lawful basis applies, to help demonstrate our compliance with the data protection principles;
- 5.1.4 include information about both the purposes of the processing and the lawful basis for it in our relevant transparency statement(s);
- 5.1.5 where sensitive personal information is processed, also identify a lawful special condition for processing that information (see paragraph 5.4.2 below), and document it; and
- 5.1.6 where criminal offence information is processed, also identify a lawful condition for processing that information, and document it.
- 5.2 When determining whether our legitimate interests are the most appropriate basis for lawful processing, we will:
 - 5.2.1 conduct a legitimate interests' assessment (LIA) and keep a record of it, to ensure that we can justify our decision;
 - 5.2.2 if the LIA identifies a significant privacy impact, consider whether we also need to conduct a data protection impact assessment (DPIA);
 - 5.2.3 keep the LIA under review, and repeat it if circumstances change; and
 - 5.2.4 include information about our legitimate interests in our transparency statement(s).
- 5.3 Sensitive personal information is sometimes referred to as "special categories of personal information".
- 5.4 We may from time to time need to process sensitive personal information as part of our activities and functions as a registered social landlord and charity in Scotland. We will only process sensitive personal information if:
 - 5.4.1 we have a lawful basis for doing so as set out in paragraph 5.1.1 above; and

5.4.2 one of the special conditions for processing sensitive personal information applies e.g.

- (a) the data subject has given explicit consent;
- (b) the processing is necessary for the purposes of exercising the employment law rights of the data subject or our employment law obligations;
- (c) the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent;
- (d) processing relates to personal information which is manifestly made public by the data subject;
- (e) the processing is necessary for the establishment, exercise or defence of legal claims; or
- (f) the processing is necessary for reasons of substantial public interest.

5.5 Before processing any sensitive personal information, staff must notify the DPO of the proposed processing, in order that the DPO may assess whether one of the above special conditions applies.

5.6 Sensitive personal information will not be processed until:

5.6.1 the assessment referred to in paragraph 5.5 above has taken place; and

5.6.2 the data subject has been properly informed (by way of transparency statement) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

5.7 We do not carry out automated or electronic decision-making (including profiling) based on a data subject's sensitive personal information.

5.8 Our transparency statements set out the types of sensitive personal information that we process, what it is used for and the lawful basis for the processing.

5.9 Consent is one of the lawful bases for processing personal information and sensitive personal information.

5.10 A data subject consents to processing of their personal information if they indicate agreement either by a statement or positive action to the processing. Consent requires affirmative action, so silence, pre-ticked boxes or inactivity are unlikely to be enough. If consent is given in a document which deals with other matters, then consent must be kept separate from those other matters.

- 5.11 Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if personal information is to be processed for a different and incompatible purpose which was not disclosed when the data subject first consented via the relevant transparency statements.

6 DPIAs

- 6.1 Where processing is likely to result in a high risk to a data subject's data protection rights (e.g. where we are planning to use a new form of technology which involves or could involve the processing of personal information, such as a new document management system), we will, before commencing the processing, carry out a DPIA to assess:
- 6.1.1 whether the processing is necessary and proportionate in relation to its purpose;
 - 6.1.2 the risks to data subjects; and
 - 6.1.3 what measures can be put in place to address those risks and protect personal information.
- 6.2 Before any new form of technology is introduced, staff must contact the DPO in order that a DPIA can be carried out.
- 6.3 If the technology involves the processing of employee personal information, the DPO will seek the views of a representative group of employees as part of undertaking the DPIA.

7 Documentation and records

- 7.1 We will keep written records of our processing activities, including:
- 7.1.1 our name and contact details, including the contact details of the DPO;
 - 7.1.2 the purposes of processing personal information;
 - 7.1.3 a description of the categories of data subjects and categories of personal information processed by us;
 - 7.1.4 categories of recipients of personal information processed by us;
 - 7.1.5 where relevant, details of transfers to countries outside the European Economic Area (EEA), including documentation associated with how we protect the personal information after transfer;
 - 7.1.6 how long we keep personal information; and
 - 7.1.7 a description of the technical and organisational security measures that we have in place to protect the security of personal information.
- 7.2 As part of our record of processing activities, we document:

- 7.2.1 information required for our transparency statements;
 - 7.2.2 records of consent;
 - 7.2.3 controller-processor (service provider) contracts;
 - 7.2.4 the location of personal information within our systems;
 - 7.2.5 DPIAs; and
 - 7.2.6 records of data breaches.
- 7.3 If we process sensitive personal information or criminal records information, we will keep written records of:
- 7.3.1 the relevant purpose(s) for which the processing takes place, including (where required) why it is necessary for that purpose;
 - 7.3.2 the legal basis for our processing; and
 - 7.3.3 whether we retain and erase the personal information in accordance with our Data Retention Policy and, if not, the reasons for not following the policy.
- 7.4 We will conduct regular audits of the personal information that we process and update our documentation accordingly, including by:
- 7.4.1 distributing questionnaires and interviewing staff to obtain to a complete picture of our processing activities; and
 - 7.4.2 reviewing our policies, procedures, contracts and agreements to address areas, such as retention, security and data sharing.
- 7.5 We document our processing activities in electronic form, so we can add, remove and amend information easily.

8 Transparency statements

- 8.1 We will issue transparency statements from time to time, informing data subjects about the personal information that we collect and hold about them, how they can expect their personal information to be used and for what purposes. This applies whether we collect personal information directly from the data subject or from third parties.
- 8.2 We will take appropriate measures to provide information in transparency statements in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

9 Data subjects' rights and requests

- 9.1 Data subjects have rights when it comes to how we handle their personal information. These include rights to:

- 9.1.1 withdraw consent to processing of their personal information at any time;
 - 9.1.2 receive certain information about our personal information processing activities;
 - 9.1.3 request access to their personal information that we hold about them;
 - 9.1.4 ask us to erase their personal information if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate personal information or to complete incomplete personal information;
 - 9.1.5 restrict processing of personal information in specific circumstances;
 - 9.1.6 challenge processing which has been justified based on our legitimate interests or in the public interest;
 - 9.1.7 request a copy of an agreement under which personal information is transferred by us to another organisation based outside of the EEA;
 - 9.1.8 prevent processing of personal information that is likely to cause damage or distress to the data subject or anyone else;
 - 9.1.9 be notified of a data breach which is likely to result in high risk to their rights and freedoms;
 - 9.1.10 make a complaint to the Information Commissioner's Office about our processing of their personal information; and
 - 9.1.11 in limited circumstances, receive or ask for their personal information to be transferred to a third party in a structured, commonly used and machine-readable format.
- 9.2 The identity of the data subject exercising any of the rights listed above must be verified.
- 9.3 Staff must immediately forward any such request received by them to the DPO.

10 Staff obligations

- 10.1 Staff are responsible for keeping their personal information up to date. Staff should let the Human Resources department know if the information they have provided to us changes, for example, if they move to a new house.
- 10.2 Staff may have access to a range of personal information during their employment and staff must help us to meet our data protection obligations.
- 10.3 If staff have access to personal information, they must:

- 10.3.1 only access the personal information that they have authority to access, and only for authorised purposes;
 - 10.3.2 only allow other staff to access personal information if they have appropriate authorisation;
 - 10.3.3 only allow third parties to access personal information if they have specific authority to do so from the DPO or their line manager;
 - 10.3.4 ensure that any sharing of personal information complies with the transparency statement provided to data subjects and the third party with whom it is shared agrees to put appropriate security measures in place to protect the personal information;
 - 10.3.5 keep personal information secure (e.g. by complying with rules on access to premises, computer access, password protection and secure file storage and destruction and other appropriate precautions);
 - 10.3.6 not remove personal information, or devices containing personal information (or which can be used to access it), from our premises, unless appropriate security measures are in place (such as encryption or password protection) to secure the information and the device; and
 - 10.3.7 not store personal information on local drives or on personal devices that are used for work purposes.
- 10.4 Staff should contact the DPO if they are concerned or suspect that one of the following has taken place (or is taking place or likely to take place):
- 10.4.1 processing of personal information without a lawful basis for its processing or, in the case of sensitive personal information, without one of the conditions in paragraph 5.4.2 being met;
 - 10.4.2 any data breach as set out in paragraph 13.1 below;
 - 10.4.3 access to personal information without the proper authorisation;
 - 10.4.4 personal information not kept or deleted securely;
 - 10.4.5 removal of personal information, or devices containing personal information (or which can be used to access it), from our premises without appropriate security measures being in place; or
 - 10.4.6 any other breach of this Policy or of any of the data protection principles set out in paragraph 4.1 above.

11 Information security

- 11.1 We will use appropriate technical and organisational measures (based on our size, available resources, volume of personal information processed and risks) to keep personal information secure, and to protect against

unauthorised or unlawful processing and against accidental loss, destruction or damage. These may include:

- 11.1.1 making sure that, where possible, personal information is encrypted;
 - 11.1.2 ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services. Confidentiality means only those who need to know and are authorised to use personal information can access it. Integrity means that the personal information is accurate and suitable for the purpose for which it is processed. Availability means that authorised users can access the personal information when they need it for authorised purposes;
 - 11.1.3 ensuring that, in the event of a physical or technical incident, availability and access to personal information can be restored in a timely manner; and
 - 11.1.4 a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
- 11.2 Where we use external organisations to process our personal information on our behalf, such as our contractors and service providers, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of our personal information. Contracts with external organisations must provide that:
- 11.2.1 the organisation may act only on our written instructions;
 - 11.2.2 employees of the organisation processing the personal information are subject to a duty of confidence;
 - 11.2.3 appropriate measures are taken to ensure the security of processing;
 - 11.2.4 sub-contractors are only engaged by the organisation with our prior consent and under a written contract;
 - 11.2.5 the organisation will assist us in providing subject access and allowing data subjects to exercise their data protection rights;
 - 11.2.6 the organisation will assist us in meeting our obligations in relation to the security of processing, the notification of data breaches and DPIAs;
 - 11.2.7 the organisation will delete or return all personal information to us as requested at the end of the contract; and
 - 11.2.8 the organisation will submit to audits and inspections, provide us with whatever information we need to ensure that they are meeting their data protection obligations, and tell us immediately if the organisation is asked to do something that could breach data protection law.

- 11.3 Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is amended, staff must seek approval of its terms by the DPO.

12 Storage and retention of personal information

- 12.1 Personal information will be kept securely.
- 12.2 Personal information should not be retained for longer than necessary. The length of time over which personal information should be retained will depend upon the circumstances, including the reasons why the personal information was obtained. Staff should follow our Data Retention Policy, which sets out the relevant retention period. Where there is any uncertainty, staff should consult the DPO.
- 12.3 Personal information that is no longer required will be deleted permanently from our systems and any hard copies will be destroyed securely.

13 Data breaches

- 13.1 A data breach may take many different forms, for example:

13.1.1 loss or theft of information or equipment on which personal information is stored;

13.1.2 unauthorised access to or use of personal information either by a member of staff or third party;

13.1.3 loss of personal information resulting from an equipment or systems (including hardware and software) failure;

13.1.4 human error, such as accidental deletion or alteration of personal information;

13.1.5 unforeseen circumstances, such as a fire or flood;

13.1.6 deliberate attacks on our IT systems, such as hacking, viruses or phishing scams; and

13.1.7 “blagging” offences, where personal information is obtained by deceiving our organisation.

- 13.2 We will:

13.2.1 make the required report of a data breach to the Information Commissioner’s Office without undue delay and, where possible, within 72 hours of becoming aware of it, if it is likely to result in a risk to the rights and freedoms of data subjects; and

13.2.2 notify the affected data subjects if a data breach is likely to result in a high risk to their rights and freedoms and where notification is required by law.

13.2.3 The DPO must be notified immediately as soon as staff become aware of a data breach. Staff should not attempt to investigate the matter themselves.

14 International transfers

We may only transfer personal information outside the EEA on the basis that that recipient country, territory or organisation is designated as having an adequate level of protection or that the organisation receiving the information has provided adequate safeguards so far as data protection is concerned. Further advice must be obtained from the DPO.

15 Training

We will ensure that staff are adequately trained regarding their data protection responsibilities. Staff whose roles require regular access to personal information will receive additional training to help them understand their duties and how to comply with them.

16 Consequences of failure to comply

16.1 We take compliance with this Policy very seriously. Failure to comply with the Policy:

16.1.1 puts at risk the data subjects whose personal information is being processed;

16.1.2 carries the risk of significant civil and criminal sanctions for us; and

16.1.3 may, in some circumstances, amount to a criminal offence by a member of our staff.

16.2 Due to the importance of this Policy, failure to comply with any requirement of it may lead to disciplinary action for a member of staff under our procedures, and this action may result in dismissal for gross misconduct. If an external organisation breaches this Policy, they may have their contract terminated by us with immediate effect.

16.3 Any questions or concerns about this Policy should be directed to the DPO.

Last updated: August 2018