



Data Protection Policy

Contents

Policy Statement	3
Data Protection Principles and How Fair Deal Follows Them	3
Fairly, Lawfully and In a Transparent Manner	3
Processed For Specified, Explicit and Legitimate Purpose	3
Adequate, Relevant and Not Excessive	3
Accurate and Up to Date	4
Not Kept Longer Than Necessary	4
Secure And Confidential	4
1. The Rights of Data Subjects	4
2. Keeping Data Subjects Informed	4
Data Subject Access	5
Rectification of Personal Data	5
Erasure of Personal Data	5
Restriction of Personal Data Processing	6
Data Portability	6
Automated Decision-Making & Profiling	6
Accountability And Record Keeping	6
Personal Data Collected, Held, and Processed	7
Data Security - Transferring Personal Data and Communications	8
Data Security - Storage	8
Data Security - Disposal	9
Data Security - Use of Personal Data	9
Data Security - IT Security	9
Organisational Measures	9
Transferring Personal Data to a Country Outside the EEA	10
Data Breaches	10
Training	11
Policy Monitoring and Review	11
Document Information	12
Amendment History	12

Policy Statement

Fair Deal, a company registered in Scotland under Company Number SC141688 whose registered office is at 355a Tormusk Road, Castlemilk, Glasgow, G45 0HF is committed to a policy of protecting the rights and privacy of its service users, their families, staff, volunteers and board members along with all other individuals with whom it conducts business. Fair Deal will do this in accordance with EU Regulation 2016/679 General Data Protection Regulation (GDPR).

The GDPR defines “personal data” as any information relating to an identified or identifiable natural person (a “data subject”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

This Policy sets out Fair Deal’s obligations regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles set out herein must be followed at all times by Fair Deal, its employees, agents, contractors, volunteers, board members or other parties working on behalf of Fair Deal.

Fair Deal is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

Data Protection Principles and How Fair Deal Follows Them

Fair Deal may variously act as “data controller” or “data processor” dependant on the nature of the personal data involved. This is recorded as part of Fair Deal’s data register.

Fair Deal must ensure that personal data is processed in accordance with the following principles:

Fairly, Lawfully and In a Transparent Manner

Fair Deal will tell individuals the reasons for processing their personal data, how it uses such personal data and the legal basis for processing in its privacy notices. Where Fair Deal relies on its legitimate interests as the basis for processing personal data, it will carry out an assessment to ensure that those interests are not overridden by the right and freedoms of individuals.

Processed For Specified, Explicit and Legitimate Purpose

Fair Deal will not use personal data for a purpose other than those advised to the data subjects. If personal data held is requested by external organisations for any reason, this will only be passed on if the data subjects concerned agree or if it is required by law. Also, external organisations must state the purpose of processing and agree not to copy the personal data for any purpose other than the agreed purpose.

Adequate, Relevant and Not Excessive

Fair Deal will monitor from time to time the personal data held for internal purposes, ensuring Fair Deal does not hold excessive personal data in respect of the individuals to whom the personal data relates. If personal data given or obtained is excessive for such purpose, it will be immediately deleted or destroyed. Where special category data is concerned, Fair Deal will only collect or retain the minimum amount of information required.

Accurate and Up to Date

Fair Deal will ensure that all personal data held is accurate and where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased, or rectified without delay.

Not Kept Longer Than Necessary

All personal data for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. It will be deleted or destroyed as soon as is reasonably practicable.

Secure And Confidential

Fair Deal takes the security of personal data seriously and therefore has appropriate technical and organisational measures in place to protect personal data against loss, accidental destruction, misuse or disclosure.

Where Fair Deal engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement technical and organisational measures to ensure the security of data.

1. The Rights of Data Subjects

The GDPR sets out the following rights applicable to data subjects:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure (also known as the 'right to be forgotten')
- The right to restrict processing
- The right to data portability
- The right to object; and
- Rights with respect to automated decision-making and profiling

2. Keeping Data Subjects Informed

Fair Deal shall provide the information set out below to every data subject:

- a) Where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and
- b) Where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose:
 - i. if the personal data is used to communicate with the data subject, when the first communication is made; or
 - ii. if the personal data is to be transferred to another party, before that transfer is made; or
 - iii. as soon as reasonably possible and in any event not more than one month after the personal data is obtained.

The following information shall be provided:

- i. Details of Fair Deal including, but not limited to, the identity of its Data Protection Lead
- ii. The purpose(s) for which the personal data is being collected and will be processed and the legal basis justifying that collection and processing
- iii. Where applicable, the legitimate interests upon which Fair Deal is justifying its collection and processing of the personal data

- iv. Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed
- v. Where the personal data is to be transferred to one or more third parties, details of those parties
- vi. Details of data retention
- vii. Details of the data subject's rights under the GDPR
- viii. Details of the data subject's right to withdraw their consent to Fair Deal's processing of their personal data at any time
- ix. Details of the data subject's right to complain to the Information Commissioner's Office (the "supervisory authority" under the GDPR)
- x. Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it; and
- xi. Details of any automated decision-making or profiling that will take place using the personal data, including information on how decisions will be made, the significance of those decisions, and any consequences

Data Subject Access

Data subjects may make subject access requests ("SARs") at any time to find out more about the personal data which Fair Deal holds about them, what it is doing with that personal data, and why.

Employees wishing to make a SAR should do using a Subject Access Request Form, sending the form to Fair Deal's Data Protection Lead at annmariedocherty@fair-deal.org

Responses to SARs shall normally be made within one month of receipt, however this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed

All SARs received shall be handled by Fair Deal's Data Protection Lead.

Fair Deal does not charge a fee for the handling of normal SARs. Fair Deal reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

Rectification of Personal Data

Data subjects have the right to require Fair Deal to rectify any of their personal data that is inaccurate or incomplete.

Fair Deal shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing Fair Deal of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

Erasure of Personal Data

Data subjects have the right to request that Fair Deal erases the personal data it holds about them in the following circumstances:

- i. It is no longer necessary for Fair Deal to hold that personal data with respect to the purpose(s) for which it was originally collected or processed
- ii. The data subject wishes to withdraw their consent to Fair Deal holding and processing their personal data

- iii. The data subject objects to Fair Deal holding and processing their personal data (and there is no overriding legitimate interest to allow Fair Deal to continue doing so)
- iv. The personal data has been processed unlawfully
- v. The personal data needs to be erased in order for Fair Deal to comply with a particular legal obligation; or
- vi. The personal data is being held and processed for the purpose of providing information society services to a child

Unless Fair Deal has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

In the event that any personal data that is to be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

Restriction of Personal Data Processing

Data subjects may request that Fair Deal ceases processing the personal data it holds about them. If a data subject makes such a request, Fair Deal shall retain only the amount of personal data concerning that data subject (if any) that is necessary to ensure that the personal data in question is not processed further.

In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

Data Portability

Fair Deal does not process personal data using automated means:

Objections to Personal Data Processing

Data subjects have the right to object to Fair Deal processing their personal data based on legitimate interests, direct marketing (including profiling).

Where a data subject objects to Fair Deal processing their personal data based on its legitimate interests, Fair Deal shall cease such processing immediately, unless it can be demonstrated that Fair Deal's legitimate grounds for such processing override the data subject's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.

Where a data subject objects to Fair Deal processing their personal data for direct marketing purposes, Fair Deal shall cease such processing immediately.

Automated Decision-Making & Profiling

Fair Deal does not use personal data in automated decision-making processes and does not use personal data for profiling purposes.

Accountability And Record Keeping

Fair Deal's Data Protection Lead is the Chief Executive contactable at fionadunwoodie@fair-deal.org

The Data Protection Lead shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, Fair Deal's other data protection-related policies, and with the GDPR and other applicable data protection legislation.

Fair Deal shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

- i. The name and details of Fair Deal, its Data Protection Lead, and any applicable third-party data processors
- ii. The purposes for which Fair Deal collects, holds, and processes personal data
- iii. Details of the categories of personal data collected, held, and processed by Fair Deal, and the categories of data subject to which that personal data relates
- iv. Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards
- v. Details of how long personal data will be retained by Fair Deal; and
- vi. Detailed descriptions of all technical and organisational measures taken by Fair Deal to ensure the security of personal data.

Personal Data Collected, Held, and Processed

The following personal data is collected, held, and processed by Fair Deal:

Type of Data	Purpose of Data	Retention Period
Name	Personal Data required to provide support in line with individual service user welcome packs to service users and their families	None specified
Personal details in completed new start form	The employment, training and development of Fair Deal staff	Current employment and 6 years after employment ends.
Emergency Contact information	The involvement, training and development of Fair Deal volunteers and board members	9 months
Application forms	Recruitment and related records	9 months after recruitment closes
Personal Details	Recruitment and involvement of agency staff within the service	destroy once contract ends
Conflict of Interest Form	Board/Sub Committee business, including the AGM and Election Process	Retained while member is current.
Personal details - name	Financial Accounts & Records	Held indefinitely
Photos	Advertising, Marketing & Public Relations	None specified

Type of Data	Purpose of Data	Retention Period
Board member names	Companies House and other regulatory authority requirements	Shred once online

Data Security - Transferring Personal Data and Communications

Fair Deal shall ensure that the following measures are taken with respect to all communications and other transfers involving personal data:

- a) All emails containing personal data must be encrypted
- b) All emails containing personal data must be marked “confidential”
- c) Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances
- d) Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable
- e) Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted
- f) Where personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data
- g) Where personal data is to be transferred in hardcopy form it should be passed directly to the recipient [or sent using courier or hand delivered]; and
- h) All personal data to be transferred physically, whether in hardcopy form or on removable electronic media shall be transferred in a suitable container marked “confidential”.

Data Security - Storage

Fair Deal shall ensure that the following measures are taken with respect to the storage of personal data:

- a) All electronic copies of personal data should be stored securely using passwords
- b) All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar
- c) All personal data stored electronically should be backed up on a daily basis with backups stored offsite. All backups should be encrypted using a 256bit 8TTPS certificate
- d) No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets, and smartphones), whether such device belongs to Fair Deal or otherwise without the formal written approval of the Data Protection Lead and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary; and
- e) No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of Fair Deal where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the GDPR (which may include demonstrating to Fair Deal that all suitable technical and organisational measures have been taken).

Data Security - Disposal

When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of.

Data Security - Use of Personal Data

Fair Deal shall ensure that the following measures are taken with respect to the use of personal data:

- a) No personal data may be shared informally and if an employee, agent, sub-contractor, volunteer or other party working on behalf of Fair Deal requires access to any personal data that they do not already have access to, such access should be formally requested from the Data Protection Lead
- b) No personal data may be transferred to any employees, agents, contractors, volunteers or other parties, whether such parties are working on behalf of Fair Deal or not, without the authorisation of the Data Protection Lead
- c) Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors, volunteers or other parties at any time
- d) If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it; and
- e) Where personal data held by Fair Deal is used for marketing purposes, it shall be the responsibility of the Data Protection Lead to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service

Data Security - IT Security

Fair Deal shall ensure that the following measures are taken with respect to IT and information security:

- a) All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols
- b) Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of Fair Deal, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords
- c) All software (including, but not limited to, applications and operating systems) shall be kept up-to-date. Fair Deal's IT staff shall be responsible for installing any and all security-related updates; and
- d) No software may be installed on any Fair Deal - owned computer or device without the prior approval of the Data Protection Lead

Organisational Measures

Fair Deal shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

- a) All employees, agents, contractors, volunteers or other parties working on behalf of Fair Deal shall be made fully aware of both their individual responsibilities and Fair

Deal's responsibilities under the GDPR and under this Policy, and shall be provided with a copy of this Policy

- b) Only employees, agents, sub-contractors, volunteers or other parties working on behalf of Fair Deal that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by Fair Deal
- c) All employees, agents, contractors, or other parties working on behalf of Fair Deal handling personal data will be appropriately trained to do so
- d) All employees, agents, contractors, or other parties working on behalf of Fair Deal handling personal data will be appropriately supervised
- e) All employees, agents, contractors, or other parties working on behalf of Fair Deal handling personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise
- f) Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed
- g) All personal data held by Fair Deal shall be reviewed periodically
- h) The performance of those employees, agents, contractors, volunteers or other parties working on behalf of Fair Deal handling personal data shall be regularly evaluated and reviewed
- i) All employees, agents, contractors, volunteers or other parties working on behalf of Fair Deal handling personal data will be bound to do so in accordance with the principles of the GDPR and this Policy by contract
- j) All agents, contractors, volunteers or other parties working on behalf of Fair Deal handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of Fair Deal arising out of this Policy and the GDPR; and
- k) Where any agent, contractor or other party working on behalf of Fair Deal handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless Fair Deal against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure

Transferring Personal Data to a Country Outside the EEA

Fair Deal does not transfer personal data to countries outside of the EEA.

Data Breaches

- a) All personal data breaches must be reported immediately to the Data Protection Lead
- b) If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Chief Executive must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it
- c) In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described in the clause above) to the rights and freedoms of data subjects, the Chief Executive must ensure that all affected data subjects are informed of the breach directly and without undue delay
- d) Data breach notifications shall include the following information:
 - i. The categories and approximate number of data subjects concerned
 - ii. The categories and approximate number of personal data records concerned
 - iii. The name and contact details of the Data Protection Lead who is responsible for data protection (or other contact point where more information can be obtained)

- iv. The likely consequences of the breach; and
- v. Details of the measures taken, or proposed to be taken, by Fair Deal to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

Training

Fair Deal will provide training to all staff and volunteers about their data protection responsibilities as part of the induction process and at regular intervals thereafter.

Policy Monitoring and Review

The Data Protection Lead will monitor and evaluate the policy regularly. The policy will be assessed with regard to the effectiveness within Fair Deal. This policy will be reviewed to keep up to date with any changes involved in dealing with all aspects of data protection.

Document Information

Document Ref:	Data Protection Policy
Version:	4
Date of Version:	02/05/2019
Created By:	Ann Marie Docherty
Approved By:	Anne Marie Borthwick
Confidentiality Level:	Controlled: Uncontrolled if printed

Amendment History

Date	Version	Created By	Description of Change
25/04/2019	1	Ann Marie Docherty	Initial Release
25/04/2019	2	Elaine Davidson	Added in a Front Cover sheet
02/05/2019	3	Elaine Davidson	Updated the Front Cover/version/date
29/03/2024	4	Liz Connor	Checked with current legislation. Footer amended and formatted.