Old Mill Foundation
HOLISTIC CANCER SUPPORT CENTRE
Registered charity No. 1125120 Tel: 01792 851553

# Data Protection Policy

**Contents**



## 1. Introduction

1.1 In the course of its function, Old Mill Foundation gathers and holds personal data about individuals. This includes information about its employees, volunteers and clients. In dealing with this data, Old Mill Foundation is bound by the General Data Protection Regulations 2018 which requires us, the Old Mill Foundation to:

a) Properly process personal data in a lawful, fair and transparent manner
b) Collect personal data only for specified, explicit and legitimate purposes
c) Only store and collect personal data that is adequate, relevant and limited to what is necessary in relation to its purpose
d) To erase and update in a reasonable manner any inaccurate data

e) To store and retain data for only as long as is necessary in order to safeguard rights and freedoms of individuals
f) To process data in a manner that ensures appropriate security of the personal data

## 2. Definitions

2.1 The below definitions apply to this policy:

- ***Data Controller*** : a person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the GDPR. We are the Data Controller of all Personal Data relating to our organisation and Personal Data used in our business for our own commercial purposes.
- ***Data Protection Officer (DPO):*** the person appointed by us with responsibility for data protection compliance. That person is Debbie Barrow.
- ***Data Subject:*** a living, identified or identifiable individual about whom we hold Personal Data.
- ***General Data Protection Regulation (GDPR)***: the General Data Protection Regulation ((EU) 2016/679).
- ***Personal Data*:** any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Sensitive Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.
- ***Personal Data Breach***: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.
- ***Processing or Process***: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.
- ***Sensitive Personal Data***: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal Data relating to criminal offences and convictions.

## 3. General Provisions and Scope of the Policy

3.1 This policy applies to all Personal Data we process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users or any other Data subject.

3.2 This policy applies to all our staff. You must read, understand and comply with this policy when processing personal data on our behalf. This policy sets out what we expect from you. Any breach of this policy may result in disciplinary action.

3.3 Staff will be provided with training on GDPR periodically.

## 4. Lawfulness and Fairness

4.1 Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.

4.2 The GDPR allows processing for specific purposes, some of which are set out below:

a) The data subject has given his or her consent
b) The processing is necessary for the performance of a contract with the data subject
c) To meet out legal compliance obligations
d) To pursue our legitimate interests for purposes where they are not overriding because the processing prejudices the interest or fundamental rights and freedoms of data subjects

4.3 You must identify and document the legal ground being relied on for each processing activity.

## 5. Consent

5.1 We as data controllers only process personal data on the basis of one or more of the lawful bases set out in the GDPR, which include consent. A data subject must consent to the processing of their personal data. This may be done either by indicating agreement via a statement or a positive action.

5.2 Consent can be withdrawn at any time and will be promptly honoured. Consent may need to be refreshed if we intend to process personal data for a different and incompatible purpose which was not initially disclosed.

5.3 We keep records of all consents so that we can demonstrate compliance.

## 6. Transparency

6.1 The GDPR requires us to provide detailed, specific information to data subjects depending on whether the information was collected directly or from elsewhere. This information will be provided through appropriate notices which will be concise, transparent, intelligible, easily accessible and in clear and plain language.

6.2 When we collect data from data subjects directly, we provide the data subject with all the information required by the GDPR including the identity of data controller (us) and our DPO, how and why we will use, process, disclose, protect and retain that personal data through a notice.

6.3 If any personal data is collected indirectly we will provide the data subject with all the information required by the GDPR as soon as possible after collecting/ receiving the data.

## 7. Purpose Limitation

7.1 We only collect personal data for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.

## 8. Data Minimisation

8.1 Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

8.2 You may only process personal data when required in the performance of your job. You cannot process personal data for any reason unrelated to your job.

8.3 You may only collect personal data that you require for the performance of your job. Ensure that any personal data collected is adequate and relevant for the intended purposes.

8.4 If the data is no longer needed for specified purposes, it is to be deleted or anonymised.

## 9. Accuracy

9.1 Personal data must be accurate and, when necessary, kept up to date. It must be corrected or deleted without delay when inaccurate. You will ensure that the Personal Data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

## 10. Storage Limitation

10.1 Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

10.2 You will take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with all the Organisation's applicable records retention schedules and policies. This includes requiring third parties to delete such data where applicable.

10.3 You will ensure Data Subjects are informed of the period for which data is stored and how that period is determined in any applicable notice.

## 11. Protecting Personal Data

11.1 Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

11.2 You are responsible for protecting the Personal Data we hold. You must implement reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data. You must exercise particular care in protecting Sensitive Personal Data from loss and unauthorised access, use or disclosure.

11.3 You must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. You may only transfer Personal Data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

**12. Reporting a Personal Data Breach**

12.1 The GDPR requires us to notify Personal Data Breaches to the regulator and, in certain instances, the Data Subject.

12.2 We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.

12.3 If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the DPO and follow their instructions. You should preserve all evidence relating to the potential Personal Data Breach.

**13. Data Subject's Rights and Requests**

13.1 Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

(a) withdraw consent to Processing at any time;
(b) receive certain information about Processing activities;
(c) request access to their Personal Data that we hold;
(d) prevent our use of their Personal Data for direct marketing purposes;
(e) prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else; and
(f) be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms.

13.2 You must verify the identity of an individual requesting data under any of the rights listed above.

13.3 You must immediately forward any Data Subject request you receive to the DPO.

**14. Accountability**

14.1 As a Data Controller we must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. We are responsible for, and must be able to demonstrate, compliance with the data protection principles.

**15. Record Keeping**

15.1 The GDPR requires us to keep full and accurate records of all our data Processing activities.

15.2 These records should include, at a minimum, the name and contact details of the Data Controller and the DPO, clear descriptions of the Personal Data types, Data Subject types, Processing activities, Processing purposes, third-party recipients

of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place.

**16. Sharing Personal Data**

16.1 Generally we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

16.2 You may only share the Personal Data we hold with another employee or agent if the recipient has a job-related need to know the information and the transfer complies with GDPR.

**17. Policy Changes and Policy Dates**

| Reason for change | Section changed | Date changed | New version number |
|---|---|---|---|
| | | | |
| | | | |

| | |
|---|---|
| Trustee approval | 5th December 2018 |
| Review date | 4th December 2021 |

**Signed by ……Date……**

**Name printed Colin Tarry Position in Organisation Trustee Chair**