## The Dunhill Medical Trust

**Title:** **Data Protection Policy**
**Version:** **2.2**
**Date:** **May 2020**
**To be reviewed:** **May 2021**
**Classification:** **Public**

### 1. Introduction

The Dunhill Medical Trust (DMT) holds personal data about its employees, Trustees and Committee members, grant holders, suppliers and other individuals for a variety of purposes relating to delivery of its charitable objectives. It seeks to adhere to the principles of data protection legislation, in particular to meet the requirements of the General Data Protection Regulation (GDPR) effective May 2018.

### 2. Compliance

The Trust seeks to ensure that all data is collected and used fairly, stored safely and not disclosed to any other person unlawfully as outlined in six data protection principles found in the GDPR. These state that personal data shall be:

- Processed fairly, lawfully and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary
- Accurate and rectifiable
- Retained for no longer than necessary
- Processed in a manner that ensures integrity and confidentiality

This policy sets out how the Trust seeks to protect personal data and ensure that its staff, Trustees and external advisors understand the rules governing their use of personal data to which they have access in the course of their work. In particular, this policy requires staff to ensure that the Executive Director are consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

Any breach, whether deliberate or through negligence, may lead to disciplinary action being taken.

### 3. Definitions

| | |
|---|---|
| **Business purposes** | The purposes for which personal data may be used by the Trust: Personnel, administrative, financial, grant administration, regulatory, and payroll<br><br>Business purposes include the following:<br>• Compliance with our legal, regulatory and corporate governance obligations and good practice<br>• Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests<br>• Ensuring that policies are adhered to (such as policies covering email and internet use)<br>• Operational reasons, such as recording transactions and grants, processing grant applications, training, statistical analysis<br>• Investigating complaints |

| | |
|---|---|
| | • Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments<br>• Monitoring staff conduct, disciplinary matters<br>• Distribution of information about the charity's grants, events, etc. |
| **Processing** | Any operation performed on personal data.<br><br>This includes creating, obtaining, holding, sorting, retrieving, amending, sharing, destroying of data, etc. |
| **Personal data** | Information relating to identifiable individuals, such as job applicants, current and former employees, Trustee and Committee members, grant applicants and grant holders past and present, and supplier contacts.<br><br>Personal data we gather may include: individuals' name and contact details, educational background, financial and pay details, education and skills, marital status, nationality, job title, CV. |
| **Sensitive personal data** | This is defined as personal data about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings. Any use of sensitive personal data should be strictly controlled in accordance with this policy. |
| **Data Subject** | A living individual to whom the data relates and who can be identified by the data stored. |
| **Data Controller** | A legal individual, public authority, agency or other body which, alone or jointly with others, determines the purposes and methods of processing personal data. |
| **Data Processor** | A legal individual, public authority, agency or body which processes personal data on behalf of the controller. |

**4. Scope**

This data protection policy applies to:

- DMT employees
- DMT Trustees and external advisors

It applies to all data (whether paper, electronic, encrypted) that the Trust holds relating to identifiable individuals. This can include:

- names of individuals
- postal addresses
- email addresses
- telephone numbers
- any other information relating to an individual.

This policy supplements the Trust's other policies relating to information security. DMT may supplement or amend this policy with additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.

## 5. Responsibilities

Everyone who works for or with the Dunhill Medical Trust has some responsibility for ensuring data is collected, stored and handled appropriately and in line with this policy. However, some people have specific areas of responsibility:

- The **Board of Trustees** is ultimately responsible for ensuring that the Trust meets its legal obligations
- **Trustees and External Advisors** are responsible for:
    - Ensuring that any personal data they receive on behalf of the Trust is held securely and only for the purpose stated
    - Ensuring that personal data is held for no longer than necessary, and is then removed from personal devices, or paper copies securely destroyed either by shredding or handing over to DMT's staff for confidential waste disposal
- The **Executive Director** is responsible for:
    - Keeping the Board updated about data protection responsibilities, risks and issues
    - Approving any contracts or agreements with third parties that process personal data on behalf of the Trust
    - Approving any data protection notices attached to communications such as emailed mailings
    - Addressing any data protection queries from the media
- The **Executive Director's delegate (role to be determined from time to time)** is responsible for:
    - The day-to-day implementation of this policy
    - Reviewing data protection procedures and related policies in line with an agreed schedule
    - Arranging data protection training and advice for those covered by this policy
    - Responding to data protection questions from staff, Trustees and external advisors in relation to data protection and the GDPR
    - Dealing with Subject Access Requests from individuals wishing to know what personal data is held about them by the Trust.
    - Checking any contracts or agreements with third parties that process personal data on behalf of the Trust
    - Documenting the type of personal data held by the Trust, including how it is collected, under what legal basis, how long it will be retained.
- Via the **Trust's IT Consultant**, the **Executive Director and Executive Director's delegate** are responsible for:
    - Ensuring all systems, services and equipment used for storing data meet acceptable security standards
    - Performing regular checks and scans to ensure security hardware and software is functioning properly
    - Evaluating any third-party services the Trust is considering using to store or process data, e.g. cloud services.
- **All employees** are responsible for:
    - Understanding their data protection obligations
    - Checking with the Executive Director that any new or proposed data processing is handled in accordance with data protection regulations
    - Ensuring that any new mailings use the latest contact information in accordance with up-to-date preferences from individuals
    - Ensuring data is not shared, processed or stored incorrectly or in a careless way that would cause a breach of data protection laws
    - Regularly reviewing personal data held; if it is found to be out of date or no longer required, it should be deleted and disposed of

- Raising any concerns and reporting any breaches or errors to the Executive Director without delay
- Referring any Subject Access requests to the Executive Director without delay.
-

**6. Processing of personal data**

Under the GDPR there are six conditions/legal bases for processing data. Use of any personal data must be justified using one of these conditions:

i) Consent, where the person gives active consent
ii) Contract, to fulfil or prepare for a potential contract
iii) Legal obligation
iv) Vital interests, eg to save someone's life
v) Lawful authority, in the public interest
vi) Legitimate interest

Personal data must be processed fairly and lawfully in accordance with individuals' rights. Generally, for DMT, this means that personal data will not be processed unless the individual whose details are being processed would expect this to happen or has consented to this happening.

The processing of all data must be:

- Necessary to deliver DMT's objectives
- In the Trust's legitimate interests whilst not unduly prejudicing the individual's privacy

*Sensitive personal data*
As a rule, the Trust does not process any sensitive data, except in the case of recruitment/ employment. Where it is necessary to process sensitive personal data DMT will require the data subject's *explicit* consent to do this unless exceptional circumstances apply or we are required to do this by law (e.g. to comply with health and safety at work obligations). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

*Third Parties*
If the Trust enters into agreements with third parties which includes the sharing of personal data, DMT will ensure that adequate protection is offered ensuring that clauses are written in the agreements stating that data will only be used in accordance with the defined purposes.

**7. Privacy Notice**

Being transparent and providing accessible information to individuals about how we will use their personal data is important. A Privacy Notice must be available to all those about whom the Trust processes data, via the website, any software we use to support the grants application process or in emails.

The notice:

- Sets out the purposes which DMT holds personal data on individuals, how it will be used and how long it will be held
- Highlights that DMT's work may require it to give information to third parties such as peer reviewers and other professional advisers; if information is likely to be going outside of the EU this needs to be highlighted
- Explains that individuals have a right of access to the personal data that the Trust holds about them and informs individuals who they should contact

**8. Accuracy and relevance**

The Trust will ensure that any personal data processed is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. DMT will not process personal data for any purpose unconnected with that for which is was originally obtained unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that the Trust corrects inaccurate personal data relating to them.

Staff members must take reasonable steps to ensure that personal data held about them is accurate and updated as required.

Data subjects have an obligation to ensure that information they provide is accurate and up-to-date and to inform the Trust of any changes or errors.

**9. Data storage, security and destruction**

All users of personal data must ensure that all such data they hold is kept secure against loss or misuse, in accordance with the Trust's Information Security Policy. Where other organisations process personal data as a service on the Trust's behalf, this will be carried out in accordance with the Trust's Outsourcing and Third Party Compliance Policy.

In cases when personal data is stored on printed paper, it should be kept in a secure place, ie locked cabinet, where unauthorised personnel cannot access it. Printed papers with personal data should be shredded or put in the confidential waste sacks when they are no longer needed.

Personal data stored on computers, CDs, memory sticks or other mobile devices must be secured in accordance with the Trust's Information Security Policy and sub-policies.

Data should be regularly backed up.

All servers containing sensitive data must be approved and protected by security software and strong firewall.

**10. Data retention**

Personal data must not be retained for any longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with the Trust's Document/Data Retention Policy.

**11. Transferring data internationally**

There are restrictions on international transfers of personal data.

There are only a few ways in which DMT currently transfers data outside of the European Economic Area (EEA):

- Mail-outs via Mailerlite, which is covered by the Trust's agreement with Mailerlite as a data processor on behalf on the DMT; recipients of emails via Mailerlite will have given consent to receive information from the Trust, which they can withdraw at any time. Mailerlite is covered by the EU-US Privacy Shield certification.
- Financial records and processing via Xero. When personal data is hosted or processed outside of the EEA by Xero, Xero ensures that it remains protected by safeguards in line with EU law. For example, some data is processed in New

Zealand which is recognised by the EU as an 'adequate' country to receive and process EU personal data, and are therefore in accordance with the requirements of the GDPR. If information is processed in the US or Australia, other safeguards are in place, e.g. the EU-US Privacy Shield certification, to ensure compliance with the GDPR.

- Peer review of research grants. Research grant applicants will be aware of the need for peer review and will be asked to confirm their acceptance that this may require data transfer outside of the EU when they initiate a new application via the Trust's Grants Management System. The personal data being transferred is minimal, i.e. name only.

Any further transfers of personal data anywhere outside of the EEA cannot take place without first consulting the Executive Director and an assessment of the risk and impact being documented.

**12. Individual Rights**

Individuals are entitled to ask:

- what information is held about them and why
- how to gain access to it
- how to keep it up-to-date

If an individual contacts the Trust requesting this information, this is called a subject access request. Subject access requests should be made to the Executive Director. These requests must be processed within one month, provided there is no undue burden and it does not compromise the privacy of other individuals. The Executive Director will always verify the identity of anyone making a subject access request before handing over any information. Information must be provided in a structured and commonly used format. No charge is to be made for responding to a subject access request.

A data subject may also request that their data is transferred directly to another system. This must be carried out free of charge.

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. However, the Trust will need to keep basic data to identify that individual and retain it solely for suppression purposes to prevent further unwanted processing. This activity is in the mutual interests of the individual who wishes their privacy rights to be upheld and the Trust which is required to fulfil this right.

**13. Processing data in accordance with the individual's rights**

Individuals have the opportunity to indicate their preferences for receiving (or not receiving) information from the Trust via the website contact page and via the online Grants Management System. When planning any direct mailing employees must ensure that these preferences are adhered to. Staff are required to check the latest available information prior to carrying out such a mailing.

## 14. Training

All staff will receive training on data protection and the GDPR. New joiners will receive training as part of their induction process. Further training will be provided at least every two years or whenever there is a substantial change in the law or the Trust's policy and procedures.

## 15. Reporting breaches

All members of staff have an obligation to report actual or potential data protection compliance failures to the Executive Director as soon as these are identified. This allows the Trust to investigate the failure, take remedial steps and report to the Information Commissioner's Office (ICO) if necessary. A register of compliance failures will be maintained to log any material failures reported to the ICO.

## 16. Data audit and documentation

Annual data audits to manage and mitigate risks will be undertaken. This will be carried out by the Executive Director and Director of Grants & Research together with the Trust's IT consultant. They will meet annually to review DMT's GDPR Controller documentation to ensure it is adequate and up-to-date.