**DMD Pathfinders Data Protection Policy**

**Key details**

* Policy prepared by: Jon Hastie
* Approved by board / management on: Click here to enter a date.
* Policy became operational on: Click here to enter a date.
* Next review date: Click here to enter a date.

**Introduction**

DMD Pathfinders needs to gather and use certain information about individuals.

These can include users, organisations, suppliers, employees and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the company’s data protection standards — and to comply with the law.

**Why this policy exists**

This data protection policy ensures DMD Pathfinders

* Complies with data protection law and follow good practice
* Protects the rights of staff, customers and partners
* Is open about how it stores and processes individuals’ data
* Protects itself from the risks of a data breach

**Data protection law**

The Data Protection Act 1998 describes how organisations — including DMD Pathfinders — must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection Act is underpinned by eight important principles. These say that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not be held for any longer than necessary
6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways
8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

**People, risks and responsibilities**

**Policy scope**

This policy applies to:

All staff and volunteers of DMD Pathfinders, including contractors, suppliers and other people working on behalf of the charity.

It applies to all data that the charity holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998. This can include:

* Names of individuals
* Postal addresses
* Email addresses
* Telephone numbers
* …plus any other information relating to individuals

**Data protection risks**

This policy helps to protect DMD Pathfinders from data security risks, including:

* **Breaches of confidentiality.** For instance, information being given out inappropriately.
* **Failing to offer choice.** For instance, all individuals should be free to choose how the company uses data relating to them.
* **Reputational damage.** For instance, the charity could suffer if hackers successfully gained access to sensitive data.

**Responsibilities**

Everyone who works for or with DMD Pathfinders has some responsibility for ensuring data is collected, stored and handled appropriately.

The **board of trustees** is ultimately responsible for ensuring that DMD Pathfinders meets its legal obligations.

* The CEO and data controller,  **Jon Hastie** is responsible for:
  + Keeping the board updated about data protection responsibilities, risks and issues.
  + Reviewing all data protection procedures and related policies, in line with an agreed schedule.
  + Arranging data protection training and advice for the people covered by this policy.
  + Handling data protection questions from staff and anyone else covered by this policy.
  + Dealing with requests from individuals to see the data DMD Pathfinders holds about them (also called ‘subject access requests’).
  + Checking and approving any contracts or agreements with third parties that may handle the company’s sensitive data.
  + 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 company is considering using to store or process data. For instance, cloud computing services.
  + Approving any data protection statements attached to communications such as emails and letters.

**General staff guidelines**

* The only people able to access data covered by this policy should be those who **need it for their role**. Individual role descriptions for staff and volunteers should specify the level of data access necessary for each role.
* Data **should not be shared informally**. When access to confidential information is required, staff or volunteers can request it from their supervisors.
* **DMD Pathfinders will provide training** to all volunteers and staff to help them understand their responsibilities when handling data.
* Staff and volunteers should keep all data secure, by taking sensible precautions and following the guidelines below.
* In particular, **strong passwords must be used** and they should never be shared.
* Personal data **should not be disclosed** to unauthorised people, either within the charity or externally.
* Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of.
* Staff and volunteers **should request help** from their line manager or the data protection officer if they are unsure about any aspect of data protection.
* For home-workers, regular assessment and review of data security arrangements will be carried out.

**Data collection**

* DMD Pathfinders will ensure when collecting data that:
* There are legitimate grounds for collecting and using the personal data;
* Individuals have been made aware that data will be collected and what it will be used for, and told where they can find more information.
* Individuals have been given the opportunity to opt out of direct marketing.
* Individuals have been made aware of the consequences of providing or not providing the information.

**Data storage**

These rules describe how and where data should be safely stored, and apply whether in an office or a home-working environment. Questions about storing data safely can be directed to the IT manager or data controller.

When data is **stored on paper,** it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

* When not required, the paper or files should be kept **in a locked drawer or filing cabinet**.
* Employees should make sure paper and printouts are **not left where unauthorised people could see them**, like on a printer. Printed data should never be taken out of the office or home working environment.
* **Data printouts should be shredded** and disposed of securely when no longer required.

When data is **stored electronically**, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

* Data should only be stored on **designated computers and servers**, and should only be uploaded to an **approved cloud computing services**.
* Data should be **protected by strong passwords registered to individual users** that are changed regularly and never shared between staff and volunteers.
* Data should be **backed up frequently**. Those backups should be tested regularly, in line with the company’s standard backup procedures.
* Data should not be **stored on removable media** (like a CD or DVD).
* Data should **never be saved directly** to laptops or other mobile devices like tablets or smart phones.
* All servers and computers containing data should be protected by **approved** **security software and a firewall**.
* Personal data processed for any purpose or purposes shall **not be kept for longer than is necessary** for that purpose or those purposes. Data will be permanently deleted when no longer needed (including from trash folders and backup copies as soon as reasonably practical).

**Data use**

Personal data is of no value to DMD Pathfinders unless the charity can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

* Staff and volunteers should ensure **the screens of their computers are always locked** when left unattended.
* Personal data **should not be shared informally**. In particular, it should never be sent by email, as this form of communication is not secure.
* Data must be **encrypted before being transferred electronically**. This is carried out automatically when using Google Drive.
* Personal data should **never be transferred outside of the European Economic Area** unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.
* Staff and volunteers **should not save copies of personal data to their own computers.** Always access and update the central copy of any data using Google Drive.

**Data accuracy**

The law requires DMD Pathfinders to take reasonable steps to ensure data is kept accurate and up to date.

It is the responsibility of all staff and volunteers who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

* Data will be held in **as few places as necessary**. Staff should not create any unnecessary additional data sets.
* Staff should **take every opportunity to ensure data is updated.** For instance, by confirming a customer’s details when they call.
* DMD Pathfinders will make it **easy for data subjects to update the information** the charity holds about them. For instance, via the company website.
* Data should be **updated as inaccuracies are discovered**. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

**Data breaches**

A data security breach can happen for a number of reasons:

* Loss or theft of data or equipment on which data is stored
* Inappropriate access controls allowing unauthorised use
* Equipment failure
* Human error
* Unforeseen circumstances such as a fire or flood
* Hacking attack
* ‘Blagging’ offences where information is obtained by deceiving the organisation who holds it

If a data breach has occurred, DMD Pathfinders will respond in the following way:

* The Data Protection Officer will identify what data has been compromised and how, and establish whether damage limitation can be carried out including retrieving and securing the data if possible. This might include temporarily restricting data from staff and volunteers.
* The Data Protection Officer will assess the nature of the data that may have been compromised and the level of risk to individuals, as well as any ongoing threat to data security.
* The Data Protection Officer will decide who needs to be notified of the breach. Notification should have a clear purpose, whether this is to enable individuals who may have been affected to take steps to protect themselves or to allow the appropriate regulatory bodies to perform their functions, provide advice and deal with complaints.
* DMD Pathfinders’ Board of Trustees and the Data Protection Officer will review policies, procedures and operational arrangements (including staff awareness) on data management to ensure these are fit for purpose and make any necessary changes to attempt to prevent further breaches.

**Rights of individuals**

All individuals who are the subject of personal data held by DMD Pathfinders are entitled to:

* Ask **what information** the company holds about them and why.
* Ask **how to gain access** to it.
* Be informed **how to keep it up to date.**
* Be informed how the charity is **meeting its data protection obligations**.

If an individual contacts the charity requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the data controller at [Jon.Hastie@DMDPathfinders.org.uk](mailto:Jon.Hastie@DMDPathfinders.org.uk). The data controller can supply a standard request form, although individuals do not have to use this.

Individuals will be charged £10 per subject access request. The data controller will aim to provide the relevant data within 14 days.

The data controller will always verify the identity of anyone making a subject access request before handing over any information.

**Disclosing data for other reasons**

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, DMD Pathfinders will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and taking legal advice where necessary.

**Providing information**

DMD Pathfinders aims to ensure that individuals are aware that their data is being processed, and that they understand:

* How the data is being used
* How to exercise their rights

To these ends, the charity has a Data & Privacy Statement, setting out how data relating to individuals is used by the charity.

[This is available on request. A version of this statement is also available on the charity’s website.]