**Confidentiality Policy & Agreement**

All matters related to users are treated as confidential within DMD Pathfinders. Every new member of staff, and all volunteers at DMD Pathfinders are expected to sign a form promising to keep all information relating to users confidential. No information will be divulged to anyone without the user’s permission, or his or her next of kin if the client is unable to give this permission. Written permission has to be obtained from the client or next of kin before replying to any official enquiries about the client.

It is also important that staff, volunteers and trustees maintain confidentiality regarding activities of DMD Pathfinders not in the public domain, for example project development work, bids in progress, and information regarding other staff and trustees.

This confidentiality policy addresses how staff and volunteers are expected to behave when discussing and sharing confidential information. It should be read in conjunction with the data protection policy which sets out guidelines for how physical and electronic data is to be collected and stored.

**The following points should be noted:**

**User confidentiality**

* DMD Pathfinders recognises that personal information about users may be shared informally between its staff, trustees or volunteers, where this is necessary in order to provide our services. All staff, volunteers and trustees should ensure that no discussions (online or offline) relating to an individual user of DMD Pathfinders take place outside of meetings or discussions between DMD Pathfinders staff, volunteers and trustees.
* Many of the services provided by DMD Pathfinders are provided online and via social media. DMD Pathfinders staff and volunteers should use social media profiles dedicated to work when posting about DMD Pathfinders or supporting our users. However, we also recognise there may be significant crossover between work and personal lives on social media and this may not always be possible. Staff or volunteers delivering services to users should therefore always ensure that they use appropriate privacy & publishing settings when posting on personal profiles to limit what users of the charity can view.

* Many trustees may have personal connections to users. Staff and volunteers on user-oriented projects should not share information about users with trustees except where required with designated trustees by procedures relating to handling complaints and investigations.
* DMD Pathfinders recognises that users need to feel secure in using services in a confidential manner. DMD Pathfinders will aim to ensure all users are afforded confidential interview space if it is required, and will ensure telephone services are provided by staff or volunteers in a confidential space.
* Staff and volunteers must not divulge any personal information relating to members of staff without consulting a senior member of staff, in the first instance. This includes whether an individual is being supported by DMD Pathfinders.
* DMD Pathfinders will not share any data outside of DMD Pathfinders without first obtaining the user’s consent, unless this is deemed necessary in accordance with our procedure (as set out below in “Necessary Breaches of Confidentiality ”).
* DMD Pathfinders’ answerphone messages will not be played while there is anyone waiting in the nearby area.
* DMD Pathfinders staff, volunteers or trustees must take care to note if there are other people around when they are talking on the telephone to a user. Names should not be repeated aloud, nor personal details.
* Users must be asked if it is acceptable to leave an answerphone message if staff, volunteers or trustees need to call them back.
* DMD Pathfinders staff, volunteers or trustees should not give out their own personal contact details, or those of others, to clients.

**Organisational confidentiality**

* It is imperative that DMD Pathfinders has the ability to plan its future activities in strict confidence. This will prevent other organisations from using our ideas without our consent, or releasing information before we are ready.
* Where projects are currently in development it is likely that services will change by the time they are launched. Releasing detailed information too early may raise expectations of users beyond what we can provide.
* Staff, volunteers and trustees must not share any information regarding DMD Pathfinders not already in the public domain, for example project development work, bids in progress, and information regarding other staff and trustees.
* Information not currently in the public domain which is to be released to the public must first be approved by the CEO or project manager for a specific project.
* No member of staff shall (except in the proper course of duty), during or after the period of employment under this agreement divulge to any person whosoever or otherwise make use of (and shall use their best endeavours to prevent the publication or disclosure of) any information concerning the affairs of DMD Pathfinders
* Trustees may often use personal social media profiles and contact details to facilitate easier, more flexible communication with other trustees and external organisations. It is important that trustees maintain professional boundaries and do not discuss confidential DMD Pathfinders business or service users outside of the Trustees facebook group or email discussions with other trustees.

**Expressed Consent to give Information**

It is the responsibility of the advisors to ensure that where any action is agreed to be taken by DMD Pathfinders on behalf of a user, that the user must first sign an authorisation form either by hand or electronic means. This should be placed in the user’s file.

DMD Pathfinders staff and volunteers providing services are responsible for checking with users if it is acceptable to call them, or write to them, at home or work in relation to their case.

All details of expressed consent must be recorded on the case file.

**Necessary breaches of Confidentiality**

DMD Pathfinders recognises that occasions may arise where individual staff and volunteers providing services should breach confidentiality. This might be due to a safeguarding concern or where it could prevent a serious crime.

On these occasions, where a staff member or volunteer feels confidentiality might need to be breached, the following steps need to be taken:

* 1. The staff member or volunteer should raise the matter immediately with their Line Manager or Supervisor.
  2. The staff member or volunteer must discuss with them the issues involved in the case and explain why they feel confidentiality should be breached and what would be achieved. The manager will discuss with the staff member or volunteer what options are available in each set of circumstances and will take a written note of this discussion.
  3. If the manager decides that confidentiality may need to be breached then they should take the following steps:

1. The Manager or Supervisor should contact the Data Protection Officer (CEO).
2. The manager should brief the Data Protection Officer on the full facts of the case, ensuring they do not breach confidentiality in doing so.
3. The manager should seek authorisation to breach confidentiality from the Data Protection Officer.
   1. If the Data Protection Officer agrees to breaching confidentiality, a full written report on the case should be made and any actions agreed.
   2. In the event of a breach becoming necessary, the user should be informed of this policy and the resulting need for DMD Pathfinders to breach confidentiality before any action is taken.
   3. The manager is then responsible for ensuring all the agreed actions are taken.
   4. If the Data Protection Officer does not agree to breach confidentiality, then this is the final decision of the organisation.

**Unauthorised breaches of Confidentiality**

Where a member of staff or volunteer is believed to have breached this confidentiality policy this will be treated as a disciplinary offence and treated accordingly, allowing for a proper investigation of the facts to take place before any action is taken. Depending on the circumstances, a breach of confidentiality could be classed as gross misconduct and lead to dismissal without notice.

In extreme circumstances, e.g. the malicious and deliberate disclosure of sensitive information, DMD Pathfinders might consider whether to pursue legal or criminal charges against the individual responsible.

Data breaches will be dealt with in line with our Data Protection Policy.

**Legislative Framework**

DMD Pathfinders will monitor this policy to ensure it meets statutory and legal requirements, including the Data Protection Act, Children’s Act, Rehabilitation of Offenders Act and Prevention of Terrorism Act. Training on the policy will include these aspects.

**Ensuring the Effectiveness of the Procedure**

All Trustees, Staff and Volunteers will receive a copy of the Confidentiality Policy, Data Protection Policy and Data and Privacy Statement. Existing and new staff and volunteers will be introduced to these policies during induction and training. The policy will be reviewed annually and amendments should be proposed and agreed by the Board of Trustees.

**Statement of Confidentiality.**

I have read the confidentiality policy and understand its implications and agree to abide by the confidentiality policy

**Signed** ........................................................................

(Member of Staff/Volunteer)

**Signed** .........................................................................

(Witnessed by Line Manager or Supervisor)