Confidentiality Policy

Introduction

We are entrusted with people's personal information and undertake to hold it confidentially and securely.

This policy sets out procedures for storing and accessing confidential information and applies to trustees, staff, volunteers and service users.

Receiving and storing information

Personal information on users, staff, trustees and volunteers will be received and held in confidence. This means that information given to us for one purpose should not be shared with a third party or used for a different purpose without explicit consent of the individual to whom the information relates. Only the addressee should open any incoming mail (including email) marked 'Private' and/or 'Confidential'.

We will ensure that personal information is held in marked files in locked drawers or cabinets. Only authorised staff will hold keys. Security of personal data held on computers is also paramount. We will allow individuals access to information held about them and, where appropriate, correct it or erase it. We will take security measures to prevent unauthorised or accidental access to, alteration, disclosure or loss and destruction of information. Files must be password protected and access restricted to relevant staff.

Under the Section 7 of Data Protection Act 1998, any Subject Access Requests to access an individual's personal information will be responded to in line with Move Momentum's Data Protection policy and procedure. We will keep personal information for as long as is required in line with Move Momentum's Data Protection Policy.

We must prevent loss through fire, flood or other disaster. Backup files should be held. Files, 'hard' or 'soft', will be cleared of personal or sensitive information, e.g. disciplinary, that is no longer required.

Passing on personal information

Information given to us will not be shared with a third party without permission, preferably in writing. In the case of users, such written permission should be obtained using a standard form.

However, information may be shared with a third party without consent where:

- There is a perceived risk to life; or
- There is perceived likelihood of harm.
- There is a statutory requirement.

In this case, a line manager must be consulted and approve that information can be passed on. A written record should also be kept, including dates, times, methods of contacts and persons spoken to.

We have a duty to inform Social Services and/or the Police if we believe someone is being neglected or abused, or at immediate risk of harm resulting from neglect or abused. As stated in our Safeguarding Policy.

Monitoring

When information has been passed on under the circumstances stated above, i.e. disclosure without consent, copies of written records should be passed to the manager. The manager may report this to The Board.

Breaches of this policy may constitute an offence and will likely cause reputational damage as a result of the harm caused by any breach of trust placed in us by others. Any breach will likely result in disciplinary action.

We are committed to reviewing our Confidentiality policy annually.

This policy was last reviewed and approved by the Board of Trustees on 28/10/20