Data Protection Policy

Policy

MALVERN HOUSE is committed to meeting its legal and moral obligations under the 1998 Data Protection Act. We will strive to observe the law in all collection and processing of personal data and will meet any subject access requests in compliance with the law. MALVERN HOUSE will take due care in the collection and storage of any sensitive data. Our staff will do their utmost to keep all data accurate, timely and secure.

Procedure

MALVERN HOUSE needs to keep certain information about students, staff, volunteers, clients, agencies and other organisations in order to operate effectively. The company recognises that all staff, clients, students and other contacts are entitled to know what personal information MALVERN HOUSE holds and processes about them and all purposes that the information will be used for. The procedure section of this document outlines how they can exercise their rights to obtain access or restrict use of their info.

To comply with the 1998 Act all information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this MALVERN HOUSE complies with the 8 Data Protection Principles which are set out in the 1998 Act. In summary these state that personal Data shall be:

- Processed fairly and lawfully
- Obtained for specified and lawful purposes and only processed for those purposes
- Adequate , relevant and not excessive
- Accurate and up to date.
- Kept for no longer than necessary
- Processed in accordance with data subject's rights
- Protected by appropriate security
- Not transferred without adequate provision

Data

These procedures relate to the use of personal data, i.e. information about individuals. This includes client or student records, membership/mailing lists, records of staff or volunteers/interns and contact databases that have named individuals. Information that is intended to become part of these systems and any set of files where you can easily go to information about a specific individual (e.g. files that are numbered and there is a list matching client names to numbers) is also covered by these procedures.

Consent

Consent must be given before MALVERN HOUSE can use people's personal data:

- All clients/students should give MALVERN HOUSE consent to hold and use their data for specified purposes
- All application forms for positions within MALVERN HOUSE must have a data protection statement
- In particular MALVERN HOUSE must get explicit consent to process sensitive personal data, i.e. information as to the data subject's racial or ethnic origin, physical or mental health or condition, sexuality, previous offences or any details relating to criminal convictions etc. Forms asking for this data must explain why it is needed and what will be done with it.

Note- Consent does not have to be in writing e.g. when someone fills in an application form their consent is implied by the act of filling in the form. However if you think a dispute is possible it is a good idea to have evidence of consent, e.g. staff should ask clients if they give consent for their details to be held on file for specified purposes and then make a note that consent was given in the relevant client's file.

In order to give consent all clients, staff, students etc must be issued with information about how their data is used. A standard statement on leaflets and forms, a standard paragraph in letters for new users or a notice in a contract is sufficient. The data protection statement needs to:

- Identify the company MALVERN HOUSE and the purpose(s) for which the data is required
- Identify possible disclosures to other organisations and offer an opt out from disclosure to other organisations if this is appropriate
- Indicate any data items on forms that are voluntary
- Explain explicitly why any sensitive data is needed

Example statement:

MALVERN HOUSE will use the information you have provided for the purposes of *(details of usage)*. Your information will not be disclosed to any other person or organisation except in connection with the above purposes. Any sensitive data collected, e.g. information about age, gender, health etc, will only be used to help us compile information for funders and other bodies. If you have any queries about the use of your data, please contact *(manager of service area)*.

Disclosing personal information

- Managers can only disclose personal data with consent or where there is a legal requirement
- Managers must comply with any assurances given at the time information was collected, i.e. stick to the purposes specified when consent was given. This means data collected for one purpose cannot be used for another without getting consent.
- Managers must review the data protection implications whenever using information for any new or slightly different purpose is considered. The only exceptions to this are where a law other than the 1998 Data Protection Act requires a disclosure and where you decide it is necessary to disclose information in connection with a crime.

Individual's access to information

All staff members, volunteers and students of MALVERN HOUSE services have the right to view all information held about them and to have a copy of the information.

- All requests to gain access to information held must be made in writing to the Data Protection Compliance Officer (see appendix A) and accompanied by proof of identity.
- The right to view is free (a copy may be charged for at the standard copying rate up to a maximum of £10).
- MALVERN HOUSE will provide a viewing time/a copy of the information within 40 calendar days.

Please note: *requests to see all personal data have a legal status and must be handled correctly.*

Restrictions on access

There is some information that MALVERN HOUSE does not have to provide. This is mainly true when there is information that identifies others.

Individuals do not have the right to see confidential references sent by MALVERN HOUSE. They may however, make an application to the recipient of the reference. To avoid confusion all staff requesting references should specify whether the reference is expected to be provided in confidence and kept confidential or to be accessible to the data subject.

Security and confidentiality

All managers are responsible for ensuring that:

- staff and volunteers/interns are aware of this policy and the requirements of the Data Protection Act outlined within it when they collect or handle data about an individual
- staff and volunteers/interns within their teams work within the guidelines of the MALVERN HOUSE policy
- access to files by staff and volunteers/interns is restricted
- all manual files within their project containing personal data are kept locked in cabinets.

All staff are responsible for ensuring that:

- information about data processing and data protection rights is covered during inductions or during initial meetings with new students and/or clients
- confidentiality is maintained and that personal data is not disclosed unnecessarily.
- all personal data which they hold (e.g. client and student files and case notes) is kept securely
- unauthorised personnel do not have access to other's personal data. For example files containing personal data must not be left on desks unattended and must be locked away in storage at the end of each day.
- data is not lost or damaged while in their care.
- access to personal information held on computers is restricted by passwords.

- personal information which they provide to MALVERN HOUSE in connection with their employment is accurate and up-to-date.

In addition staff must not share personal data with other organisations unless consent has been given or it is necessary for service provision.

Disposing of data

In general data must not be kept for longer than necessary and cannot be kept without good reason. In particular Criminal Records Bureau (CRB) disclosures must not be kept for longer than 6 months.

All personal data must be destroyed via shredding. While awaiting destruction, Personal data will be kept securely. Managers are responsible for ensuring that data is not kept longer than necessary and that it is disposed of via shredding.

Email and the Web

- Staff and volunteers/interns must take care when sending someone's personal data in an email
- They must know who will be receiving the information and confirm that no-one else has access to the email account
- Staff must make sure email addresses are not disclosed unnecessarily or inadvertently, e.g. use the bcc field when sending to multiple addresses.

Photographs

- Staff must get written consent before publishing photographs of individuals on a website or in a publication.
- The use of any photographs and the length of time they will be used should be made clear to the individual (the annual report one year is different from a photo that appears in every advert for a service over a decade).