

1. Who this policy applies to

This policy applies to all data within Mid Kent Mind (MKM) from all sources including our employees, volunteers and clients. It also includes sensitive data about our organisation, for example unpublished financial information and intellectual property.

2. Aims of this policy

The policy aims to protect our clients, employees, volunteers and our organisation as whole from the possibility of personal and organisational data being passed on to individuals or organisations who have no right to that information.

3. Policy content

3.1 General confidentiality statement

All our employees and volunteers are required to respect the right of clients and of other employees and volunteers to confidentiality as far as possible within the constraints of legal requirements and the safety of other people. This policy also takes on board current legislation including:

- Data Protection Act 2018;
- UK GDPR;
- Public Disclosure Act 1996;
- Employment Rights Act 1996;
- Children's Act 2004;
- Rehabilitation of Offenders Act 1974;
- Prevention of Terrorism Act 2005.

Absolute confidentiality cannot be guaranteed and this will be made clear to clients at the earliest possible opportunity. Where it is thought necessary to pass on information to another individual or organisation this will be assessed on the basis of their application and full consideration of whether there is a legal duty to disclose information. The client will be advised in writing that information has been requested, and by whom. Where possible, the consent of the person about whom the request has been made will be sought, if at all possible. The client will be advised that they should seek legal advice if they strongly object to information being passed to a third party. This policy covers not only information

given deliberately by the person concerned or by other people about the person, but also information acquired accidentally or through observation.

3.2 Circumstances in which confidentiality may be breached

The general law does not give an absolute right to confidentiality except where there is a contractual provision to this effect.

Legal and statutory requirements affecting us include, but are not limited to:

- reporting notifiable diseases to the Director of Public Health where appropriate;
- reporting accidents at work, in certain circumstances, to the Health and Safety Executive;
- replying to certain specific enquiries from Government Departments e.g. Department of Employment or Department of Social Security, or the Inland Revenue. Not all such enquiries are covered by statutory requirements so a check on the legal status of the request should be made before supplying information;
- passing on information on terrorist activities and information requested on road accidents involving personal injury, to the police;
- reporting on trafficking in illegal substances that comes to the notice of our staff or volunteers;
- giving evidence in court if a subpoena is issued.

3.3 Duty of care

We exercise a duty of care to the users of our services, our staff and our volunteers. It may therefore be necessary to breach confidentiality where a client is acting, or likely to act, in a way that could cause serious harm to him or herself, or put other service users or staff at risk.

We also owe a more general duty of care towards members of the public. It may be necessary to pass on information to the police or statutory authorities where there is considered to be a serious risk to a particular person or persons, or to the public in general.

Our employees and volunteers share with all citizens a duty of care towards children and vulnerable adults.

If our employees know or suspect that a child is at risk the Social Services Child Protection Unit must be informed. If our employees know or suspect that a vulnerable adult has been abused Social Services Care Management must be

informed in accordance with safeguarding policies. (Please see our Safeguarding Adults at Risk Policy and Safeguarding Children and Young People Policy).

3.4 Giving information to the police

There is no duty to provide the police with information except in the case of suspected or actual terrorism. However, our policy is that our employees and volunteers have a duty in the public interest not to withhold from the police any information concerning criminal activity of a serious nature. Some examples of criminal activity of a serious nature are:

- An offence that is capable of attracting a prison sentence of 12 months or more (age 18+ years for England age 21+ years for Scotland and Northern Ireland).
- An offence falling within the definition of serious crime in section 263(1) of the Act (i.e. where the conduct involves the use of violence, results in substantial financial gain or is by a large number of persons in pursuit of a common purpose)
- An offence which involves, as an integral part of it, the sending of a communication
- An offence which involves, as an integral part of it, a breach of a person's privacy

This should preferably be done with the knowledge of the person concerned and whenever possible with their cooperation but there may be circumstances where the risk to others is too great for this to be advisable or possible.

3.5 Passing on information to others

Where there is a legal duty to pass information to others, such information will only be passed after discussion and approval by the CEO. Other staff are not permitted to pass on such information. Where there is no legal obligation but there may be a duty of care to pass on information the decision whether or not to do so will in the end remain one of individual judgement. Points for consideration are:

- is the risk a real one;
- how great is the danger to self or to another person;
- will the breach of confidentiality avoid the harm;
- is there no other way of avoiding the harm;

- the advice of the appropriate line manager or project leader should be sought and, except where there is a legal requirement to breach confidentiality, a senior staff member must be informed and they will inform the chair.

Where it is decided that information must be passed on to another individual or organisation the basis on which disclosure is to be made must be clear and unambiguous. Those disclosing the information must first have an understanding as to the intended use of the information requested and by whom.

Requests from statutory bodies must be submitted in writing, even when there is a legal obligation on our organisation to comply with the request.

We will not pass on personal details (e.g. addresses, phone numbers) without consent. However, an offer can be made to pass on or forward messages.

The process of informing the person and seeking consent need not be followed where the consent of the person concerned can be implied, for example where a reference is requested, where the Department of Employment asks for information about a former employee in order to pay benefit or when a service user has signed a disclaimer on a referral form.

3.6 Care of information

- Our volunteers and employees will take care:
- not to be overheard when discussing confidential information on the phone, or with the client or appropriate staff;
- not to leave information lying around and to keep confidential information in locked filing cabinets when not in use.
- to keep records which include no more than the minimum information required.
- to destroy information when it is no longer required.
- Lock computer when leaving it unattended

3.7 Complaints

People who wish to make a complaint to us either about another agency or individual or about our employees, our volunteers or an aspect of our services may be concerned about the confidentiality of information they are giving. The preservation of confidentiality will be given high priority, subject to the exceptions listed above in section 3.5 and/or if it is necessary to breach confidentiality in order to properly investigate the complaint. The permission of the complainant will always be sought for this but in cases where the welfare of

the complainant or other people is seriously at risk it may be necessary to breach confidentiality even if that permission is withheld.

3.8 Access to information

Clients have a right to see their personal files. Access must be granted under supervision in order to protect the confidentiality of other people's files and/or third party information. It may be necessary for the client to request access in writing and for an appointment to be made. An appropriate staff member should be present in order to answer any questions that may arise. The file may not be removed from our premises but documents may be photocopied, on request. A charge may be made for this at the discretion of our staff. A record will be kept of requests and access given.

When a letter about an individual is written to us by a professional or carer the writer should be informed that the client is permitted access to his/her file and their advice sought on what action they wish us to take. This could include returning the letter to the sender or, in exceptional cases, keeping the letter in a separate confidential place.

4. Policy review

This policy should be reviewed every three years by Board of Trustees. Upon review, this policy should be submitted to the relevant approving committee for approval