Date Issued and approved by the Executive Committee:	September 2014

HULL AND EAST YORKSHIRE MIND

DATA PROTECTION AND INFORMATION SECURITY POLICY

1. Introduction

1.1 Hull and East Yorkshire Mind ("the Organisation") needs to process certain personal information, for example about its employees, workers, volunteers, placement students, trustees and members, for a number of purposes such as to satisfy operational needs and to meet its legal obligations to funding bodies and government. The Organisation also processes personal information in order to recruit, employ/engage and pay employees, recruit volunteers, students and trustees, and to provide details of meetings and newsletters to members.

1.2 The types of personal information that the Organisation processes includes information about current, past and prospective:

- employees (which, for the purposes of this Policy, includes casual workers and self-employed contractors except where otherwise stated);
- volunteers and placement students (referred to as "students" in the remainder of this Policy);
- trustees;
- members of the Organisation (e.g. individuals who have made a donation to the Organisation or are subscribed to one of its mailing lists);
- suppliers which the Organisation communicates and transacts business with (where those suppliers are sole traders or partnerships); and
- service users (of all ages).

1.3 This Policy applies to all personal information, whether it is held on paper, on computer or other media.

1.4 The Organisation fully endorses and adheres to the Data Protection Act 1998 ("the Act"), including the eight data protection principles listed in Schedule 1 to the Act. These principles specify the legal conditions that must be satisfied in relation to obtaining, handling, processing, transporting and storing personal information.

1.5 This Policy applies to anybody who handles personal information or other confidential information held by the Organisation, including but not limited to employees, volunteers, trustees and students (each of which is a **"Data User"** for the purposes of this Policy). The confidentiality and non-disclosure obligations contained within this Policy shall continue to apply to all Data Users after their involvement with the Organisation (e.g. their employment/engagement) has ended.

1.6 The Organisation takes a proportionate approach to the handling of personal information in that not all Data Users have access to, or the right to access, all personal information held by the Organisation. The Organisation's general policy is that personal information should only be accessed by specific Data Users for specific purposes.

2. Statement of Intent

- Information security is about handling information properly in order to comply with the Act and build trust between Data Users and service users to create a confident and effective working relationship which safeguards the Organisation's reputation.
- This Policy supports the Organisation's obligations to respect the information rights of individuals and protect their privacy and dignity.
- Responsibility for keeping personal information secure does not rest solely with the Data User who receives the information. This Policy encourages appropriate line management and team discussions around information security issues such as confidentiality.
- Any disclosure of personal information held by the Organisation (whether it be related to a service user, employee or anybody else) must be legally justified having regards to the risks of disclosing that information to a third party.
- The Organisation has also prepared this Policy in order to inform you of the way in which your personal information will be handled.

3. Principles

3.1 To comply with the Act, the Organisation is required to ensure that all personal information that it processes is done so fairly, stored securely and not disclosed to any third party unlawfully. The Organisation must specifically comply with the data protection principles, which are set out in Schedule 1 to the Act. In summary these state that personal information shall:

- Be processed fairly and lawfully and shall not be processed unless certain specified conditions are met;
- Be obtained only for one or more specified and lawful purposes and shall not be processed in any manner incompatible with the relevant purpose(s);
- Be adequate, relevant and not excessive in relation to the relevant purpose(s);
- Be accurate and (where necessary) kept up to date;
- Not be kept for longer than is necessary for the relevant purpose(s);
- Be processed in accordance with the rights of data subjects;
- Be subject to appropriate technical and organisational measures so that it is kept secure from unauthorised or unlawful processing, accidental loss, destruction, and damage; and
- Not be transferred to a country outside the European Economic Area, unless that country ensures an adequate level of protection in relation to personal information.

3.2 The Organisation and all Data Users must ensure that they follow the above principles at all times, including in relation to any personal information which is in the public domain. In order to ensure that this happens, the Organisation has developed this Policy.

4. Satisfaction of Principles

4.1 In order to meet the requirements of the above eight principles, the Organisation will:

- Observe fully the conditions regarding the fair collection and use of personal information;
- Meet its obligations to specify the purposes for which personal information is used;

- Collect and process personal information only to the extent that it is needed to fulfil those specified purposes;
- Ensure the quality of personal information used;
- Apply strict checks to determine the length of time personal information is held (and delete personal information where it is no longer required);
- Ensure that the rights of individuals about whom the personal information is held, can be fully exercised under the Act;
- Take appropriate technical and organisational security measures to safeguard personal information; and
- Ensure that personal information is not transferred outside the European Economic Area without suitable safeguards.

4.2 The Organisation will only process personal information for such purposes, and disclose personal information to such third parties, in each case as have been notified to the Information Commissioner's Office ("ICO"). The Organisation's registration number with the ICO is ZA033688.

4.3 The Organisation has (in general terms) registered with the ICO that it processes personal information for the following purposes:

- Providing a voluntary service for the benefit of the public as specified in the Organisation's constitution;
- Maintaining personal records of the people who use our services to enable us to provide effective support
- Administering membership records;
- Fundraising and promoting the interests of the Organisation;
- Managing its employees and volunteers; and
- Maintaining its own accounts and records.

5. Hull and East Yorkshire Mind's Designated Information Compliance Manager

5.1 The Organisation's Information Compliance Manager is responsible for ensuring the Organisation's compliance with the Act and implementation of this Policy on behalf of the Executive Committee. The Information Compliance Manager is the Chief Executive Officer.

5.2 Any questions or concerns about the interpretation or operation of this Policy, or the handling of personal information, should be taken up in the first instance with the Information Compliance Manager.

6. Status of the Policy

6.1 The Executive Committee has approved this Policy. This Policy does not form part of an employee's formal contract of employment/engagement, but it is a requirement of each employee's employment/engagement with the Organisation that the employee will abide by all rules and policies implemented by the Organisation (including this Policy). It is also a requirement of all volunteers', students' and trustees' involvement with the Organisation that each such individual abides by the Organisation's rules and policies (including this Policy).

Any failure by a Data User to follow this Policy may lead to action being taken under the Organisation's disciplinary procedures (in the case of employees other than casual workers and self-employed contractors) or to the Data User being removed from their post (in the case of volunteers, students, trustees, casual workers and self-employed contractors). Any failure by a Data User to follow this Policy

(whether during or after their employment or other involvement with the Organisation has ended) may also lead to the Organisation taking legal action.

6.2 If you consider that this Policy has not been followed in respect of personal information about yourself or others you should raise the matter with your Line Manager or the Organisation's Information Compliance Manager.

7. Rights of Data Subjects

All individuals who are the subject of personal information held by the Organisation are known as data subjects, and are entitled to:

- Know what information the Organisation holds and processes about them and why;
- Ask how to gain access to it;
- Be given a description of the recipients or classes of recipients to whom their personal information may be disclosed;
- Receive a copy of any information constituting their personal data (as defined in the Act) held by the Organisation (including information relating to the source of that data);
- Prevent the processing of their personal information for direct marketing purposes;
- Ask to have inaccurate personal data amended; and
- Prevent processing that is likely to cause damage or distress to themselves or anybody else.

8. Data User Responsibilities

8.1 In addition to the obligations set out elsewhere in this Policy, all Data Users are responsible for:

- Checking that any information that they provide to the Organisation is accurate and up to date;
- Informing the Organisation of any changes to information which they have previously provided (e.g. change of address);
- Verifying the accuracy of any information previously provided to the Organisation where required by the Organisation from time to time; and
- Informing the Organisation of any errors in the information held by the Organisation about them. The Organisation cannot be responsible for any errors in the Data User's information unless the relevant Data User has informed the Organisation of the error.

8.2 If and when, as part of their responsibilities, Data Users collect information about other people (e.g. about colleagues, service users, students, members and volunteers (including information about personal circumstances)), all Data Users must comply with the provisions of this Policy (including but not limited to the provisions of Appendix 1). In particular, information given to Data Users by service users and external agencies is confidential information of the Organisation.

8.3 Data Users should be aware that there is no specific exemption in the Act which applies to information in the public domain, and that the Act and the eight data protection principles (such as the obligation to process personal data fairly and lawfully) also apply to information in the public domain.

8.4 Data Users' use of the Organisation's computer network, internet and email system (whether on the Organisation's premises or by remote access) may be monitored by the Organisation to ensure that its policies and procedures are being complied

with and for legitimate operational purposes, and you consent to such monitoring by your use of the Organisation's IT facilities.

9. Information Security

9.1 The need to ensure that information is kept securely means that precautions must be taken against physical loss or damage, and that both access and disclosure must be restricted. All Data Users are responsible for ensuring that:

- Any personal information which they come into contact with is kept securely;
- Personal information is not disclosed to any unauthorised third party, whether orally or in writing or accidentally or otherwise; and
- Any personal information which is sent to another individual (whether internal or external) must be clearly marked as 'Private and Confidential' and sent to a named person.

9.2 Data Users who are employees should note that unauthorised disclosure of personal information by an employee will potentially lead to disciplinary action, and may be considered gross misconduct in sufficiently serious or repeated cases.

9.3 The following steps should be taken at all times with regards personal information:

9.3.1 Manually Held Personal Information

- Manual personal information should be kept in lockable storage when not in use (including but not limited to storing information about service users in a locked cabinet);
- Personal information should not be left unattended, such as on desks or tables (including but not limited to within a project);
- Paper records containing personal information must be shredded and securely disposed of where no longer required (including but not limited to handwritten notes/letters which are subsequently typed up); and
- Personal information must not be left in the photocopier, printer or fax machine.

9.3.2 Electronically Held Personal Information

- Hard copies of personal information should not be taken from the Organisation's computer network unless absolutely necessary;
- Unattended ICT equipment should not be accessible to other users (e.g. via computer screens);
- Where personal information is stored on ICT equipment which is physically installed at the Organisation's premises, that equipment must be password protected (as must any files containing personal information held on that equipment);
- Personal information should never be copied onto any portable equipment or device without specific authorisation from the Information Compliance Manager;
- Where personal information is stored on any portable equipment or device (including but not limited to USB drives, CD-ROMs, DVD-ROMs and laptop computers), such equipment/device must be encrypted (password protection is not sufficient);

- Electronically stored personal information must be deleted when no longer required (including where stored on CD-ROM or DVD-ROM); and
- Personal information must not sent by email without specific authorisation from the Information Compliance Manager (as security cannot be guaranteed), and any personal information sent by email must be password-protected and encrypted.

9.4 Data Users must not take any personal information with them away from the premises without specific authorisation from their Line Manager. If any personal information is taken off the premises (whether held on paper or on an electronic device), it should be kept with you or in a secure location at all times (e.g. should be kept in a locked car boot during transit and must never be left unattended in a vehicle, even when parked at home) and should not be accessible by friends or family. In the event that any such information is lost or stolen, or you believe it may have been accessed by an unauthorised person or otherwise compromised, you must report it to the Information Compliance Manager immediately.

9.5 Data Users must not store or transfer personal information using any cloud storage or other file sharing system (such as Dropbox, Google Drive, Sky Drive or iCloud) without specific authorisation from the Information Compliance Manager. Such systems may involve the transfer of personal information outside the European Economic Area and potentially breach the eighth data protection principle contained within the Act.

9.6 Personal information may only be transferred to a third party data processor if the data processor agrees in writing to comply with the Organisation's procedures and policies, or puts in place adequate measures itself.

10. Subject Consent

10.1 In many cases, the Organisation can only process personal information with the consent of the relevant individual. The purposes for which personal information will be processed must therefore be communicated to all data subjects.

10.2 In some cases, it is necessary for the Organisation to process a person's sensitive personal information, including but not limited to information about health, criminal convictions, race, gender and family details. This may be for health and safety reasons or where required by the Organisation's other policies, such as health and safety and equal opportunities. Because of the sensitive nature of the information, and the potential concern and/or distress that disclosure of such information may cause to individuals, all employees, students, volunteers, trustees, service users and members must be asked to give explicit consent for the Organisation to do this.

10.3 It is a requirement of engagement for employees, volunteers, students and trustees, and of the provision of services to service users, that the Organisation is given consent to process specified classes of personal information about those individuals. This includes information about previous criminal convictions.

10.4 Employees/Volunteers/Students/Trustees

10.4.1 The Organisation has a duty of care to all employees and other individuals and must make sure that prospective employees, volunteers, students and trustees are suitable for their roles and do not pose a threat or danger to others.

10.4.2 In addition, some jobs or courses will bring employees, volunteers, students and trustees into contact with children, including young people between the ages of 16 and 18. The Organisation has a specific duty under the Children Act and other enactments to ensure that employees are suitable for any job offered.

10.4.3 Therefore, all prospective employees, volunteers, students and trustees will be required to give their consent to the processing of their personal information (including certain types of sensitive personal information) by completing the relevant form or document when an offer of employment, engagement, placement or trusteeship is made. A refusal to provide consent can result in rejection of the application.

10.4.4 The Organisation will also ask for information about particular health needs, such as medication used or any conditions such as asthma or diabetes. The Organisation will only use the information in the protection of health and safety of the individual.

10.5 Service Users (of all ages)

10.5.1 Service users must be told that their information will be shared within the Organisation and, if there is a risk element identified, with other agencies. All service users are required to sign an authorisation form which gives the Organisation permission to contact external agencies to discuss their concerns or obtain or pass on relevant information (see Appendix 2). The form should be discussed with the service user during an early contact session, signed by the service user and attached to the service user's notes.

10.5.2 If a service user states that they do not wish for their personal information to be shared with third parties then this should be respected other than in the following circumstances:

- Where the non-disclosure of the information would put the service user or another individual's health and safety at risk (such as child protection or vulnerable adult protection issues);
- Where there is reason to believe that unlawful or potentially harmful activities are taking place;
- Where there is a legal obligation to disclose the information; or
- Where there is a risk of suicide or self-harm to the individual,

provided that there are specific restrictions on sharing sensitive personal data without consent (which are set out in paragraph 1.5 of Appendix 1 of this Policy). In any event, all requests by third parties for personal information must be dealt with in accordance with section 14 of this Policy.

10.5.3 The above circumstances may arise as part of a case conference or if a service user is being sectioned. Further guidance on the exceptions to processing personal information with consent can be found in Appendix 1.

10.5.4 All service users must be informed of the above exceptions at the time of completing the authorisation form at Appendix 2. If any information about a service user is disclosed without the relevant service user's consent, the service user should be informed and given written reasons for the disclosure.

10.5.5 A leaflet which gives a brief summary Confidentiality, aimed at service users, can be found at Appendix 6 and sould be handed to service users at an early contact session.

10.6 Members

The Organisation also holds personal data about its members, which will typically constitute their contact details and bank account details (e.g. for receiving donations). Such information must only be used with the relevant member's prior consent and must only be used for the specific purpose(s) for which the information was given by the relevant member.

11. Retention of Information

The Organisation will keep some types of information for longer than others. By law, personal information (whether about employees, service users or any other individual) must only be retained for as long as there is a genuine need for it and cannot be stored indefinitely. All Data Users are required to follow the Organisation's retention protocols as set out in Appendix 4.

12. Disposal of Information

12.1 When personal information is no longer required (e.g. has passed its retention date), it must be securely deleted and/or destroyed (as the case may be). In the case of manual records (e.g. paper files), all such records must be securely shredded. If there is a significant amount of material which cannot be dealt with by normal shredding machines, you should contact the Information Compliance Manager who will arrange for it to be disposed of using a reputable disposal contractor.

12.2 Personal information which is held electronically must be permanently deleted once no longer required, with particular care taken that any 'hidden' data cannot be recovered. The Information Compliance Manager can advise on permanent deletion of computerised records.

13. Subject Access Requests

13.1 Anybody whose personal information is processed by the Organisation (including but not limited to the Organisation's employees, volunteers, students, members and service users) has the right (subject to certain statutory exemptions and restrictions) to access any personal information that is held by the Organisation about them (whether held on computer or manually).

13.2 Any person who wishes to exercise this right should do so in writing.

13.3 The Organisation will make a charge of £10 on each occasion that access is requested, although the Organisation has discretion to waive this. This charge will be automatically waived for employees.

13.4 The Organisation aims to comply with requests for access to personal information as quickly as possible, and in any event must provide a response within 40 calendar days.

13.5 If a Data User receives a subject access request they should refer it to the Information Compliance Manager immediately to ensure it is dealt with appropriately, and not respond directly to the request.

14. Third Party Requests for Personal Information

14.1 The Organisation will protect the privacy of its service users (and other individuals about whom it holds personal data) as far as possible. This Policy requires Data Users to be vigilant when dealing with information requests relating to such individuals.

14.2 The Organisation believes that Data Users handling information should be supported so that any personal information about service users which is passed to another agency is done so in a sound, sensitive and legally correct manner within a culture of partnership working and effective risk management.

14.3 Information about the Organisation's employees, volunteers, trustees, students, members, service users and other individuals must not be disclosed to any third party except in accordance with this Policy and the Organisation's authorised procedures. For example, you must never assume that it is acceptable for a husband to be given information about his wife; they may be estranged or simply wish to keep their details separate. You must also not discuss individual cases with the press.

14.4 It is important to establish with each service user what level of information they are happy to be disclosed to their family, carers and friends (as those close to the service user often have an expectation that the information will be available to them). If a service user states that they do not wish for their information to be shared with family and/or friends, this should be rechecked with them periodically and as requests for information arise.

14.5 Unless you have been specifically authorised to the contrary by the Organisation's Management Team, in the event that you receive a request from a third party for disclosure of, or to inspect, information relating to any individual (including but not limited to service users) you should refer the request to the relevant supervisor (who will liaise with the Management Team before responding). You should make such a referral in all cases and should not respond to the request regardless of the identity of the requestor (including where the requestor is the police or any other government agency or public authority) as the Organisation has a set procedure for responding to such requests that must be followed.

14.6 Any Data User who is authorised by the Management Team to respond to a verbal request for information (whether regarding a service user or other individual) must make a contemporaneous written record at the time of disclosure which sets out what information was disclosed and why, and can demonstrate that the Data User has considered the risks of disclosure and sought to mitigate them where possible.

14.7 Subject to the authorisation requirements in sections 14.5 and 14.6 above, if you are in doubt as to the identity of an individual, you must verify their identity before disclosing personal information to them. If you receive a request for personal information by telephone, are not sure about the caller's identity and it cannot be checked, you should require that the caller puts their request in writing.

14.8 Subject to the authorisation requirements in sections 14.5 and 14.6 above, any disclosure of personal information relating to a service user should be discussed with the service user wherever possible, and their consent obtained (including

requests made by family or close friends of a service user, or another agency which is supporting that service user). In the event that the service user does not provide consent or it is not considered appropriate to ask them for consent, you should refer the issue to your Line Manager and a written record of the discussion and its outcome shall be made.

14.9 Subject to the authorisation requirements in sections 14.5 and 14.6 above any disclosure of personal information relating to service users must be identified as either:

- 'Hard' information based on facts/evidence; or
- 'Soft' information based on opinion/hearsay.

14.10 Data Users should not withhold concerns based on intuition due to a lack of factual evidence, but should make it clear at the time of disclosure that the disclosure is based on a personal opinion.

15. Use of CCTV

15.1 The Organisation has installed CCTV systems at its premises in order to protect the integrity of the Organisation's property and the security and health and safety of its employees, volunteers, trustees, students, members, service users and other visitors.

15.2 In order to maintain a secure and safe environment for its employees, volunteers, trustees, students, members, service users and other visitors the Organisation also needs to monitor its property and the working environment generally to ensure that those individuals are carrying out safe working practices. Using CCTV acts as a deterrent to potential trespassers, thieves and vandals and those who choose to breach the Organisation's health and safety rules and other procedures.

15.3 The Organisation has considered alternatives to using CCTV, such as additional regular inspections of its property, but has concluded that such alternatives would be less effective and more costly. In particular, there are situations which will require a rapid response if the risk to an individual's safety is to be minimised. CCTV is the best way for the Organisation to achieve this.

15.4 The Organisation shall display prominent signs at main entrances to sites where CCTV cameras are present unless in exceptional circumstances it is deemed necessary not to do so. Only senior members of staff have routine access to live and recorded images generated by the CCTV systems, although images will be provided to law enforcement authorities where appropriate. The Organisation may use recorded images as evidence in misconduct and performance related investigations as well as in disciplinary and court proceedings.

16. Summary

16.1 This Policy should be read in conjunction with the policies, agreements and legislative requirements listed in Appendix 3. Any breach of this Policy by a Data User may lead to disciplinary action being taken and/or criminal prosecution. Any questions or concerns about the interpretation or operation of this Policy should be referred to the Information Compliance Manager.

16.2 This Policy may be amended by the Organisation at any time. Any changes will be notified to you in writing.

Appendix 1: Guidelines for Processing Personal Information

All Data Users must comply with the guidelines set out in this Appendix.

1. Information about Employees/Volunteers/Students/Members/Service Users (of all ages)

1.1 Most Data Users will be required to process information about individuals (including sensitive personal information) as part of their day-to-day duties, including when:

- They receive a referral from another agency;
- The service user makes a self referral;
- Service users make information enquiries;
- Managing the application process;
- Conducting needs assessments and support planning;
- Writing service user case notes; and
- Liaising with external agencies on behalf of the service user.

1.2 The information that Data Users deal with on a day-to-day basis will cover categories such as:

- General personal details such as name and address;
- Date of birth;
- National Insurance Number;
- Next of kin and emergency contacts;
- Named workers and organisations; and
- Project-specific relevant history e.g. employment, debt, housing.

1.3 Data Users must not access such information unless the Organisation has given them permission to do so. In any event, personal information should only be collected to the extent that it is required for the specific purpose notified to the individual. Any information which is not necessary for that purpose should not be collected in the first place.

1.4 An individual's sensitive personal information (e.g. information about an individual's physical or mental health, sexual orientation, political or religious views, ethnicity or race) should generally only be collected and processed with the relevant individual's explicit consent. All clients should therefore sign a consent form (see Appendix 5).

1.5 The only exception to this is where the processing of sensitive personal information is necessary in order to protect the vital interests of the individual or another person in circumstances where consent cannot be given or it cannot reasonably be expected to be obtained, or where it is necessary in order to protect the vital interests of another person in a case where consent by or on behalf of the individual has been unreasonably withheld. For example:

- where there is a safeguarding concern which presents a risk to the individual or another person;
- when an individual is injured and unconscious and in need of medical attention;
- when an emergency contact needs to be informed if an individual is unwell; or
- where the individual is injured and unconscious, but in need of medical attention, and a Data User informs the hospital that the individual is pregnant or a Jehovah's Witness.

1.6 All Data Users have a duty to make sure that they comply with the data protection principles contained within the Act, which are summarised in section 3 of this Policy. In particular, Data Users must ensure that records are and remain:

- Accurate;
- Up to date;
- Processed fairly and lawfully; and
- Kept and disposed of safely and in accordance with this Policy.

1.7 Inaccurate or out-of-date information should be destroyed.

1.8 Personal information must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the information is processed, the individual must be informed of the new purpose before any processing occurs.

1.9 Data Users must not disclose personal information to any other employee, volunteer, student, service user or other individual except where done so in accordance with the Organisation's authorised policies and procedures (including this Policy).

1.10 Whenever Data Users are discussing service users (such as at a team meeting, handover meeting, external telephone call or a conversation with the service user themselves) the following steps should be taken:

- The office door should be closed at all times;
- If somebody not authorised to discuss the case enters the office, the conversation should cease and the person should be attended to or arranged to come back later;
- If a telephone call is received or is required to be made during a meeting with a service user, the service user should be asked to leave the room for the duration of the call;
- Information about any service user should not be shared with other service users; and
- In any event, personal information should only be shared between Data Users where strictly necessary to enable those Data Users to discharge their duties to the Organisation and the individuals about whom the information relates.

1.11 If any personal information is received by fax, you should specify to the sender which fax machine the information should be sent to and stand by the machine at the time it is transmitted so that the information can be retrieved from the fax machine at the earliest possible opportunity. If the information is not received, you must contact the sender immediately to let them know.

1.12 Personal information should not be sent by fax except as a last resort when no other method of communication is available. If sending such information by fax, you must ensure that the recipient is standing by their fax machine at the time of transmission so that they can retrieve it at the earliest possible opportunity.

1.13 Data Users attending case conferences should only take the relevant documents with them and not the whole file. Any such documents must be kept with the Data Users at all times.

1.14 Data Users shall not view or otherwise handle in the workplace personal information relating to their family, friends and acquaintances. Any such activity shall be deemed a serious breach of this Policy.

1.15 Personal information (whether relating to an employee, service user or other individual) must not be discussed outside the workplace or disclosed to any third party other than in accordance with this Policy.

1.16 Any requests for references that you receive must be referred to the HR Administrator (for employment references) or the Volunteer Co-ordinator (for volunteer references). In particular, Data Users should never provide references for any other individual on social or professional networking sites, as such references (whether positive or negative) can be attributed to the Organisation and create legal liability for both the Organisation and the author of the reference. References should not be given about an individual to a third party unless that individual has provided consent.

1.17 Personal comments and opinions in correspondence and other documents (whether derogatory or otherwise, and whether in relation to service users or other individuals) should be avoided wherever possible as individuals have the right to receive copies of all information that the Organisation holds about them, including such written comments and opinions. If you do write an opinion, you must be as objective as possible, state whose opinion it is and the fact that it is an opinion.

1.18 All email messages may be disclosed in legal proceedings in the same way as paper documents, and should be treated as potentially retrievable even after they have been deleted.

1.19 Before processing any personal information, all Data Users should consider the following checklist:

- Do you really need to record the information?
- Is the information sensitive?
- If it is sensitive, do you have the data subject's explicit consent?
- Has the individual been told that this type of information will be processed?
- Are you authorised to collect/store/process the information?
- If yes, have you checked with the data subject that the information is accurate?
- Are you sure that the information is secure?
- If you do not have the data subject's consent to process, are you satisfied that it is in the legitimate interests of the Organisation or a third party to process the information (having regards to the legitimate interests of the data subject)?

2. Client Management Information System ("CMIS")

2.1 In the event that you are given authorised access to the Organisation's CMIS, you must observe the following rules:

- You must keep your log-in details for the CMIS secure and not share them with any other person (whether or not a Data User). If you suspect that any of your log-in details may no longer be secure, you must immediately change any such log-in details and notify the administrators of the CMIS and the Information Compliance Manager in order that the previous log-in details can be disabled;

- Unless you have been specifically authorised to the contrary by the Organisation's Management Team, you must not print any material from the CMIS (including but not limited to via the 'Print Screen' function);

- You must not export any material from the CMIS into an electronic file (including but not limited to spreadsheets) except where strictly necessary for the performance of your duties and where done so on an anonymous basis (i.e. all information which may be capable of identifying a service user should be deleted. This includes names, but also applies to information that a third party could use in conjunction with other information to ascertain the individual's identity, such as date of birth and address);

- You must not use the CMIS to access information about any individual to whom you are not formally assigned; and

- You must not access the CMIS from a location outside the Organisation's premises except with the specific approval of the Information Compliance Manager. In the event that you are given such approval, you must:

    - Only access the CMIS using equipment which is in a secure physical location that cannot be viewed by third parties; and

    - Only access the CMIS via a secure computer network.

2.2 The Organisation reserves the right to monitor your usage of the CMIS to ensure your continued compliance with this Policy, which shall include checking usage history with regards to modification of service user files.

2.3 You must not access the CMIS if you have not been given specific log-in details by the Organisation.

Appendix 2: Authorisation Form

To consent to contact with other agencies/individuals (involved in your care and support) to seek or share information when necessary

Hull & East Yorkshire Mind is committed to working with people and providing a confidential service. We may share information within the organisation if necessary. However, there may be times when we would need to discuss your care and support needs with other carers and services. We would be grateful if you could give us permission to contact other agencies and individuals involved in your care and support.

I,…… give my permission for staff at Hull & East Yorkshire Mind to discuss any aspect of my care and support needs with the following agencies and individuals:

☐	GP	☐	Benefits Agency
☐	CPN	☐	CAB
☐	Other health workers	☐	Housing providers
☐	Social worker	☐	Substance misuse service
☐	Family/carer/next of kin	☐	Solicitor
☐	Psychiatrist/psychologist	☐	Others _____
☐	School	☐	Others _____

Is there an agency or anyone you do not wish us to contact? **No** ☐ **Yes** ☐

If yes, who? _____

_____

_____

I acknowledge that in exceptional circumstances Hull & East Yorkshire Mind may contact agencies/individuals without my consent:

- where we consider that an individual's health and safety is at risk or there appears to be child protection or vulnerable adult protection issues;
- where we have reason to believe unlawful or potentially harmful activities are taking place;
- where we are permitted or required by law to disclose such information; or
- where we consider there to be a risk of suicide or self-harm if the information is not disclosed

Signed…… Date……..……

Print Name……

Workers Name…… Date ……

Signature……

Appendix 3: Key policies, agreements and legislative requirements

- Article 8 Human Rights Act 1998
- Data Protection Act 1998
- BMA Ethical guidance: confidentiality and disclosure of health information (1999)
- Common law duty of confidence
- General protocol for sharing information between agencies in Kingston upon Hull and the East Riding of Yorkshire. Aug 2004
- Child protection guidelines and procedures. Area Child Protection Committee for Hull & East Yorkshire
- Multi-agency Policy, Procedures and Practice Guidelines for the protection of Vulnerable Adults in Hull and East Riding of Yorkshire
- Operational procedures for the sharing of information to meet the housing needs of mental health service users
- Hull & East Yorkshire Mind Risk Management Policy
- Hull & East Yorkshire Mind Code of Conduct for Staff and Volunteers
- Hull & East Yorkshire Mind Safeguarding Adults Policy
- Hull & East Yorkshire Mind Safeguarding Children Policy
- Hull & East Yorkshire Mind Whistleblowing Policy
- Hull & East Yorkshire Mind Information Technology, Email and Internet Use Policy

Appendix 4: Retention Protocols

The following is a list of the Organisation's retention protocols, all of which can be accessed via the Organisation's 'F' drive under the Proformas/Retention of Records folder:

- Buildings, plant and engineering;
- Employee – personnel records;
- Income – monies received;
- Insurance documents;
- Other documents;
- Payroll documentation;
- Pension records;
- Purchase invoices and supplier documentation; and
- Resident – care records.

Appendix 5: Use of personal information – client consent form

Hull & East Yorkshire Mind's Data Protection Policy requires us to obtain consent from clients for their information to be used for certain purposes, and in particular express consent regarding use of their sensitive personal data.

Hull & East Yorkshire Mind may process your personal information in the following circumstances:

- When we receive a referral from another agency;
- If you make a self-referral;
- If you make any enquiries for information;
- When managing the application process;
- When conducting needs assessments and support planning;
- When writing client case notes; and
- When liaising with external agencies on your behalf.

We may process the following types of personal information about you:

- Name and address;
- Date of birth;
- National Insurance number;
- Next of kin and emergency contacts;
- Named workers and organisations; and
- Project-specific relevant history (e.g. employment, debt, housing, GP details).

We may also process your sensitive personal information regarding your:

- Physical or mental health;
- Political or religious views;
- Sexual orientation;
- Ethnicity or race; and
- Medication and case history (e.g. in support plans and case notes).

All of the above personal data will be stored securely at Hull & East Yorkshire Mind's premises and on its secure electronic systems. We will not disclose your personal information to any third parties to which you have not previously consented except in the following limited circumstances:

- where we consider that an individual's health and safety is at risk or there appears to be child protection or vulnerable adult protection issues;
- where we have reason to believe unlawful or potentially harmful activities are taking place;
- where we are permitted or required by law to disclose such information; or
- where we consider there to be a risk of suicide or self-harm if the information is not disclosed.

I agree to Hull & East Yorkshire Mind processing my personal data as set out above.

Signed…… Date……..……

Print Name……

Workers Name…… Date ……

Signature……

What is Confidentiality?

Confidentiality is keeping information that has been spoken or written privately. Confidential information will be kept within the team but if necessary may be shared within the wider organisation. Notes and personal details will be kept in a secure office and electronically on our secure computer system.

It will usually be agreed during your early contact or assessment by a project at Hull & East Yorkshire Mind that you are willing for us to contact other appropriate agencies to seek further information.

Exceptions to Confidentiality

We may be required to disclose your confidentiality in the following limited circumstances:

- Where an individual's health and safety is at risk
- Where there are (or may be) Child Protection or Vulnerable Adult Protection issues.
- Where there is reason to believe unlawful or potentially harmful activities are taking place.
- Where we are permitted or required by law to disclose such information
- Where we consider there to be a risk of suicide or self harm if the information is not disclosed

We will inform you when there is a need to disclose confidential information in this way and explain why this is necessary.

Any information given will be on a need to know basis and at all times your dignity and respect will be maintained.

When confidential information is no longer needed information will be shredded or deleted.

All of our dealings with confidential information shall be made in the best interests of yourself and/or others.

Should you have any concerns or worries about confidentiality then please speak to your key worker or service manager or ask for a complaints procedure form and follow its procedure.

For more information about confidentiality please ask to view our Data Protection & Information Security Policy.

Hull & East Yorkshire Mind
Wellington House
108 Beverley Road
Hull
HU3 1XA

Tel: 01482 240200
Email: info@mindhey.co.uk
Web: http://www.mindhey.co.uk/

Registered Charity Number 1101976
Company Number 4936165
Charity registered in England

Confidentiality

The Facts