Name of Policy & Procedure: Confidentiality Status: In place Discussed with Board (Governance & Quality): May 2018 Date: May 2018 Review date: May 2020	

CONFIDENTIALITY POLICY

1 PURPOSE

1.1 This policy outlines Richmond Borough Mind's (RB Mind) approach on access to information held by the organisation. It sets out the framework in which the organisation balances openness to information for all its stakeholders, whilst protecting confidentiality for staff, service users, and its own business interests.

1.2 The overriding aim of this Policy is to protect and promote the best interests of individuals and RB Mind, and any question concerning confidentiality should be answered by reference to this principle.

1.3 The Confidentiality Policy and associated procedures set the framework within which personal and any other potentially sensitive information is to be collected, stored, handled and disclosed.

2 SCOPE

2.1 During the course of everyday working, RB Mind staff and volunteers handle a great deal of information, in both paper and electronic formats. Some of this is the personal data of beneficiaries, suppliers, staff, volunteers, supporters/campaigners, donors and trustees and is covered by our Data Protection Policy. Information about RB Mind and its work may also be sensitive and confidential and could, if disclosed, have adverse implications for the Charity.

2.2 This Policy is designed to work with and support various codes of professional conduct that are applicable to some of the work undertaken by the Charity, as well as to support our approach to safeguarding children and vulnerable adults, data protection, and use of information technology. It should be read in conjunction with the Data Protection Policy.

2.3 The Policy applies to all staff and volunteers of the organisation and third party contractors. You should familiarise yourself with this Policy, and the Data Protection Policy, and comply with their terms when processing personal data on our behalf.

3 PRINCIPLES

3.1 All personal data and confidential information about RB Mind, our partners and other third party organisations must be kept and handled confidentially, whether the information has been received formally, informally or discovered by accident – anything seen or overheard accidentally is still personal data.

Broadly, this includes:

- Any information which relates to, or is about, an identified or identifiable individual i.e., their name linked with any other information about them (address, telephone number, etc.)
- Anything else provided to us in confidence by third parties and that is not a matter of public record
- Sensitive organisational information that could be used to damage RB Mind

3.2 When working with RB Mind you must:

- Treat all personal data and sensitive organisational information as confidential to RB Mind
- Comply with the law regarding the protection and disclosure of information (including the Data Protection Legislation) and our policies, including our Data Protection Policy.

3.3 In order to deliver services, confidential information provided by service users to one member of staff will be made available to others in the team. This information could also be shared to management in supervising the delivery of services.

3.4 **Responsibilities**

The CEO is responsible for ensuring that all confidential information processed by the Charity is handled in line with this Policy and associated procedures, and for providing assurance of such to the trustees.

All Line Managers will be responsible for ensuring that all RB Mind staff working in a service delivery role have read this Policy and the Data Protection Policy and are working to the required standards. They will ensure that a high standard of record keeping is maintained by conducting regular audits and ensure staff are trained.

All RB Mind staff and volunteers with access to confidential information have responsibilities to ensure that they comply with this Policy and with any guidance subsequently produced.

3.5 Any breach of this Policy could have very serious consequences for an individual or for RB Mind and will be treated as a serious disciplinary matter.

3.6 Occasionally services delivered by RB Mind are run in partnership with the NHS. Consequently staff may need to be aware of additional principles that apply to NHS services as a result of the Caldicott Report. The report sets out a number of general good practice principles as detailed below:

- **Justify the purpose(s)** - Every proposed use or transfer of patient identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed by the appropriate guardian.
- **Do not use patient identifiable information unless it is absolutely necessary** - Patient identifiable information items should not be used unless there is no alternative. The need for patients to be identified should be considered at each stage of satisfying the purpose.
- **Use the minimum necessary patient identifiable information** - Where the use of patient identifiable information is considered to be essential, each individual item of information should be justified with the aim of reducing identifiability.
- **Access to patient identifiable information should be on a strict need to know basis** - Only those individuals who need access to personally identifiable information should have access to it, and they should only have access to the items that they need to see.

- **Everyone with access to patient identifiable information should be aware of their responsibilities** - Action should be taken to ensure that those handling patient identifiable information are fully aware of their responsibilities and obligations to respect patient/client confidentiality.
- **Understand and comply with the law** - Every use of patient identifiable information must be lawful. Someone in each organisation (in the NHS and Local Authority this the Caldicott Guardian) should be responsible for ensuring that the organisation complies with legal requirements.
- **The duty to share information can be as important as the duty to protect patient confidentiality** - Professionals should, in the patient's interest, share information within this framework. Official policies should support them doing so.

4 HANDLING CONFIDENTIAL INFORMATION

4.1 All personal data should be treated in the strictest confidence and in accordance also with our Data Protection Policy. Personal data should only be disclosed outside the Charity in line with these policies, and appropriate permissions should be evidenced to allow RB Mind to store information.

4.2 When handling personal data and other confidential information of RB Mind, its partners and other third party organisations, always follow a few simple rules:

- Even in the most innocent of conversations, do not discuss any part of your work that could cause either an individual or RB Mind embarrassment or harm
- Be aware of who else may be listening, particularly in areas open to the public
- Get into the habit of checking and clearing your work area and locking your desk and filing cabinets before leaving at the end of each day.
- Always lock your computer screen if you leave your desk unattended and log out completely when you have finished for the day
- Never leave confidential information unattended, either put it in an envelope marked confidential or lock it away.
- If you need to take sensitive documents away from the office, seek permission first
- If person-identifiable information must be transported, this should be carried in a locked box, or in a sealed envelope marked confidential and addressed to Richmond Borough Mind, 32 Hampton Road, Twickenham, TW2 5QB.
- Do not read or process confidential documents on public transport
- Remember that information in the wrong hands can cause a lot of damage and unnecessary stress

In discussions or meetings:

- Only disclose information that is relevant
- Do not discuss personal information about another person, unless relevant to their care
- Do not disclose the name of a person making an allegation about someone else without the complainant's consent
- Refer to beneficiaries by reference codes (e.g. initials) in management meetings

When entering into correspondence with an individual that will contain personal data (including, for example, sensitive information such as health data), you should:

- Check with the person concerned that they can be written to at their home address or make arrangements for letters to be collected or sent elsewhere
- Check whether correspondence should be marked private and confidential

When collecting and/or recording information about a person:

- Offer a private interview

- If the conversation is over the telephone and someone else might hear, do not repeat aloud any personal information. If necessary, ask the person to say it again.
- Explain first why the information is needed and how it will be used and obtain their consent if required. If we need to collect it for legal or other purposes, we must tell them that.
- Each client will need to have the Privacy Notice for the service in question explained to them. All clients should also be referred to the Privacy Policy on RB Mind's website for more information http://www.rbmind.org/

4.3 When collecting sensitive personal data (for example, health information) in many cases we will need to have explicit consent – this can be an oral or written statement. We should also explain:

- Who will have access to it
- The implications of not giving the information
- Any special procedures for protecting particularly sensitive information

If the individual does not agree, do not record or pass on the information. Explain this and its implications to the person, including that this may mean that they will be unable to access the service.

4.4 Ensure that any personal data you record is:

- **Factual and relevant** - Keep expressions of opinion to a minimum and make sure they are fully justifiable on the basis of the factual information.
- **Accurate** - Wherever possible, take notes during interviews and conversations and use the person's own words. Check the record with them if possible. Where appropriate, ask for and examine supporting documents and record this on file.
- **Comprehensive and clear** - Another staff member might have to form a judgement from the information and the person concerned may wish to read it.

4.5 Your work is likely to bring you into contact with information that is personal to someone or organisational information that is not yet ready for distribution. Anyone worried or distressed by something they hear or read should seek guidance and support from their manager.

4.6 **Handling incoming information**

Internal post marked confidential should be passed to the addressee unopened. If anything of a confidential nature is not in an envelope, put it in a sealed and appropriately marked envelope before passing it to the addressee.

If you open confidential correspondence by mistake, reseal it or use a new envelope and write your name and 'opened in error' on the outside before forwarding it to the addressee.

4.7 **Typing and administration**

The administration, typing, printing, photocopying, faxing and filing of confidential information must only be carried out by employees or volunteers who are familiar with RB Mind confidentiality procedures.

The following precautions should always be taken:

- Take care to securely destroy all unused rough work and any spare copies
- When photocopying, do not let anyone else read the documents, make only the required number of copies and check that nothing is left in the machine afterwards
- When faxing, ensure the first page clearly shows the contents are confidential, the fax is sent by a designated person, and alert the recipient in advance to collect it from the machine immediately. Place any incoming confidential faxes arriving

when the recipient is not present in an envelope marked confidential before passing on the fax to the recipient.

4.8 **Working with computers**

RB Mind employees and volunteers have access to RB Mind computers, which can only be accessed by their individual username and password, which must be kept confidential to the individual.

A permission system is in place so that staff and volunteers only have access to the folders and files on the shared computer drives which are relevant to their work. Staff are required to report any instances where they are able to access data which they should not.

RB Mind employee's laptop computers and mobile phones will often contain personal data due to the nature of their work. Therefore, all RB Mind portable devices will also be encrypted and/or password protected and authorised by the Office Manager, to ensure that in the event of loss or theft, data security is not compromised.

No RB Mind data should be stored on a staff or volunteer's personal equipment, be it a computer, mobile phone, memory stick etc. RB Mind data can be accessed from a personal device using the internet, for example accessing webmail, but it must not be held on a personal device.

Computers should be locked or users should log out to prevent access if computers are left unattended i.e. if the user moves away from the screen, or if someone else who shouldn't see may be able to read the screen. (to lock: press windows button+L)

When using e-mail addresses, external recipients should not be grouped unless permission has been obtained. The Bcc facility on e-mail should not be used as a mechanism for sharing or distributing personal data.

4.9 **Storage of manual data**

Files with personal data must be kept in locked filing cabinets. This information is only accessible to project workers and their managers. Information held on service users must be relevant to the services they are accessing and any individual case work that is being conducted with them.

Staff and volunteers must minimise occasions when it is necessary to take papers containing personal details outside the office. On those occasions only the minimum necessary should be taken, and great care must be taken to keep them safe. If data is in a paper format, the staff member handling such data should ensure that any names of people and/or any information that could lead to identification of subject individuals is transported and stored securely. RB Mind will make available lockable storage boxes, or utilise self-addressed envelopes for information to be posted back to RB Mind, wherever necessary.

Archive paper files are held at our storage facility. Access to the room is controlled, with the key and access code held by the Office Manager.

4.10 **Financial data**

Financial data includes anything related to the management of the Charity's finances and income. Personal bank details, credit card and other payment information must be held securely and used only for the purposes given, e.g. to make payments for services or for setting up salary or expense payments. All data will be handled and maintained following RB Mind's Finance Procedures and the auditing requirements as determined by the Charity Commission and Companies House.

4.11 **Keys**
All keys to RB Mind properties, as well as filing cabinets and desk drawers storing confidential information, must be kept securely with spare keys kept in a key cabinet or drawer that is kept locked.

5 ACCESS TO SENSITIVE INFORMATION

5.1 Staff will generally have access to all information that they genuinely need to know to carry out their work, and are under a duty to respect the confidentiality of all personal data held by RB Mind.

5.2 Staff must make privacy information available to the individual to explain the purpose of recording the personal data, how that information will be used and whether it will be shared with any third parties when they collect the information. If this causes concern, special arrangements for recording and access will be made where possible. If concerns cannot be allayed it may be impossible for RB Mind to undertake a particular activity for a given individual.

6 INFORMATION OBTAINED BY BENEFICIARIES

6.1 Beneficiaries involved in group work/peer support activities are likely to be aware of personal data about other beneficiaries and should be made aware of the need to respect their right to privacy.

6.2 Beneficiaries involved in group work/peers support activities will be asked to sign or confirm their agreement to a participation agreement prior to their involvement outlining their responsibilities and disclosure risks from other members.

6.3 RB Mind staff and volunteers will make beneficiaries aware of their responsibilities under these circumstances and they are responsible for ensuring they comply.

7 ACCESS TO CONFIDENTIAL INFORMATION

7.1 All employed staff, sessional workers and volunteers must sign a confidentiality agreement before being given access to RB Mind's information assets. For paid staff this agreement forms part of their Contract of Employment. For volunteers it is covered by our Volunteer Agreement.

8 SHARING WITH THIRD PARTIES

8.1 External agents and contractors who process personal data and other confidential information on behalf of RB Mind must be made aware of RB Mind's information governance requirements: what they can and cannot do, and who they should contact if things go wrong, prior to them being given any access to RB Mind's information assets.

8.2 The responsibilities of RB Mind as a Data Controller and the expectations of working with Data Processors and other Data Controllers is outlined in the Data Protection Policy. Appropriate agreement templates are also detailed in this policy and should be used, where appropriate, before the sharing of personal data commences.

8.3 Where RB Mind is working in partnership with another agency, it must be made explicit to service users that information will be exchanged in relevant service areas before they start accessing our services.

8.4 In cases of suspected abuse, staff must always act on information where there is reasonable cause for concern. Concerns should be referred immediately to the CEO, who will advise on reporting to the relevant authorities where appropriate. Situations where it is appropriate to disclose confidential information without consent are detailed in our Privacy Policy and in the appropriate Privacy Notices.

8.5 If an individual (i.e. family member) contacts the organisation trying to reach a service user, no information will be passed on without a service user's explicit permission.

8.6 Requests from the police for information about individuals will be dealt with by the CEO. Information may be disclosed to the police where an individual is engaged in illegal activity which poses a risk to others.

8.7 Any information request by the media must be referred to the CEO.

9 MANAGING A BREACH OF CONFIDENTIALITY

9.1 If accidental disclosure occurs, the responsible RB Mind manager should take swift action to minimise the damage. They should find out who knows about the incident, talk to them and remind them of their duty to maintain confidentiality.

9.2 The breach must be reported in line with RB Mind's Data Protection Policy. If there is the potential for adverse publicity then the CEO must be alerted.

9.3 All staff should help to prevent accidental disclosures occurring by regularly pointing out that certain information is confidential and checking that people have understood.

10 DISCLOSURE

10.1 The process for Data Subject Access Requests (DSAR) (requests from individuals for information about themselves) is outlined in the Data Protection Policy. Disclosure of personal data and other confidential information should only be made in accordance with this policy.

10.2 RB Mind may withhold information when:

- Information involves or relates to a third party who has not given consent to its disclosure
- Information has been given in confidence by a third party
- The information requested is of a sensitive nature e.g. commercially sensitive information or to protect the security of individual members of staff
- The information is held for the purposes of the prevention or detection of crime or the prosecution of offenders.

10.3 Where sensitivities of disclosing information become apparent these should be referred to the CEO for guidance and oversight.

11 DISPOSAL

11.1 When no longer required, all personal data and other confidential information, including computer printouts, will be securely shredded or destroyed, in line with the Data Protection Policy.

12 EQUALITY AND DIVERSITY

12.1 This policy must be applied consistently and in line with RB Mind's Equality and Diversity Policy.

13 MONITORING AND REVIEW

13.1 RB Mind will monitor the policy to ensure consistency and ensure that it is meeting the needs of service users and the organisation.

13.2 The CEO will be responsible for producing procedures for monitoring and review.

RELEVANT POLICIES

- Complaints Policy
- Data Protection Policy
- DBS Information Handling Policy
- Disciplinary Policy
- Email & Internet Policy
- Finance Procedures
- IT Policy
- Managing Incidents & Serious Incidents Policy
- Privacy Policy
- Safeguarding Adults at Risk Policy
- Safeguarding Children (Child Protection) Policy
- Suicide Protocol
- Supervision Policy
- User & Carer Involvement Policy
- Volunteer Policy
- Whistleblowing Policy

RELATED DOCUMENTS

- Contract of Employment
- Volunteer Agreement