Name of Local Mind	Carrick Mind
Policy	Confidentiality Policy
Version	3
Date when last reviewed	Nov 18
Date when next review due	Nov 20
Author	Jon Gladstone
This policy is for:	Staff, volunteers and clients

1. Introduction & Background

1.1 During the course of everyday working, Carrick 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 Carrick Mind and its work is also sensitive and confidential and could, if disclosed, have adverse implications for the Charity.

1.2 Carrick Mind aims to strike a balance between encouraging openness, avoiding unnecessary secrecy and bureaucracy, and ensuring individual privacy is respected. 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.

1.3 Most breaches of confidentiality happen through lack of thought or consideration of the possible consequences, or a lack of private or secure facilities. The best protection against breaches of confidentiality is to keep to a minimum the number of people who have access to sensitive information. Anyone worried or distressed by something they hear or read should seek guidance and support from their manager.

2. Scope

2.1 The policy and procedures in this policy (referred to as this **Policy**) are applicable to staff, volunteers, trustees, contracted third parties and members of consultative fora. If you are in any doubt about the application of this Policy, please seek guidance from the Chief Executive.

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 guidance used by the Charity on safeguarding children and vulnerable adults, data protection, and use of information technology. It should be read in conjunction with the Data Protection Policy, Access to Information Policy, Information Sharing Policy.

2.3 If a situation arises where there is a potential conflict between the codes and this Policy, please seek guidance from a manager. If necessary, managers should seek guidance from the Chief Executive.

3. Policy Statement

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

3.2 When working with Carrick Mind you must:

- Treat all personal data and sensitive organisational information as confidential to Carrick 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 Any breach of this Policy could have very serious consequences for an individual or for Carrick Mind and will be treated as a serious disciplinary matter.

4. Information to be kept confidential

4.1 All personal data and confidential information about Carrick 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.

4.2 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 Carrick Mind.

5. Handling Confidential Information

5.1 All personal data should be treated in the strictest confidence and in accordance also with our Data Protection Policy.

5.2 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.

5.3 When handling personal data and other confidential information of Carrick 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 Carrick 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. It is acceptable to leave some work out, but lock away anything confidential or even for limited circulation
- 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 someone comes near you while you are working, discreetly cover the material or ask the person to go away
- If you need to take sensitive documents away from the office, seek permission first
- Do not read or process confidential documents on public transport
- Do not leave confidential documents unattended in cars or public places
- Store them securely at home and do not show them to other household members
- Remember that information in the wrong hands can cause a lot of damage and unnecessary stress

5.4 In discussions or meetings

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

5.5 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
- Check whether branded franking is acceptable to the person or use stamps as an alternative

5.6 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.
- We should give them a copy of our privacy notice or refer them to the privacy notice on Carrick Mind's website for more information.

5.7 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 in writing, do not record or pass on the information. Explain this and its implications to the person
- Do not ask questions that are not relevant

5.8 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 the 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

5.9 Handling incoming information

- All external post should be opened and checked by the appropriate person before being passed on to the addressee, however it is labelled. Special arrangements may need to be made in exceptional circumstances after discussion with a manager.
- 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

5.10 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 Carrick Mind confidentiality procedures.
- The following precautions should always be taken:
  - .1 Take care to securely destroy all unused rough work and any spare copies
  - .2 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

5.11 Working with computers

- No disks, CDs or other portable storage media should be used to store personal data unless encrypted and unless authorised by Carrick Mind.
- All/any personal data stored on laptops to undertake outreach or remote clinical services should be encrypted.
- Computers should be locked or users should log out to prevent access if computers are left unattended for any length of time.

- 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.

5.12 Keys

- All keys to Carrick Mind properties must be kept securely with spare keys kept in a key cabinet or drawer that is kept locked. Do not keep keys in unlocked drawers.
- Filing cabinets and desk drawers with confidential information should be kept locked and keys kept securely with spare keys kept in a locked key cabinet. Do not keep keys in unlocked drawers.

6. Access to sensitive information

6.1 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 Carrick Mind.

6.2 Staff should have explained or made 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 Carrick Mind to undertake a particular activity for a given individual.

7. Information obtained by beneficiaries

7.1 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.

7.2 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.

7.3 Carrick Mind will make beneficiaries aware of their responsibilities under these circumstances and they are responsible for ensuring they comply.

8. Access to confidential information

8.1 All employed staff, sessional workers and volunteers must sign a confidentiality agreement before being given access to Carrick Mind information assets. For paid staff this agreement forms part of their

contract of employment. For volunteers it is covered by Carrick Mind's volunteer confidentiality pledge.

9. Sharing with third parties

9.1 External agents and contractors who process personal data and other confidential information on behalf of Carrick Mind must be made aware of Carrick 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 Carrick Mind's information assets.

9.2 All agents and contractors in receipt of Mind confidentiality information should complete and sign a confidentiality agreement at the outset of the contract being established. Where those third parties are specifically processing personal data (as a data processor) for Carrick Mind, the contract should also set out that Carrick Mind is the data controller and the third party is a data processor and the respective obligations of both parties under the Data Protection Legislation.

9.3 Carrick Mind managers who responsible for contracting with third party organisations where access to Carrick Mind's information assets is required should undertake a due diligence check and risk assessment to establish the adequacy of the third party's confidentiality, security and information governance arrangements.

10. Managing a breach of confidentiality

10.1 If accidental disclosure occurs, the responsible Carrick 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.

10.2 The breach must be reported to the Chief Executive If there is the potential for adverse publicity then the Chair must be alerted.

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

11. Disclosure

11.1 Disclosure of personal data and other confidential information should only be made in accordance with Carrick Mind's Information Sharing Policy and Information Access Policy.

12. Disposal

12.1 When no longer required, all personal data and other confidential information, including computer printouts, will be securely shredded or destroyed.

13. Roles and responsibilities

13.1 The Board of Trustees is responsible for gaining assurance that confidentiality is managed appropriately within the Charity and that adequate resources are made available to implement this Policy.

13.2 The Chief Executive 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.

13.3 The Chief Executive is responsible for ensuring that access to confidential information is audited in line with the Carrick Mind's audit policies and procedures.

13.4 The Chief Executive is responsible for providing advice in relation to this Policy.

13.5 The Chief Executive is responsible for ensuring that confidentiality clauses are contained within all contracts in accordance with the Confidentiality Agreements Procedure and that confidentiality training is included in inductions.

13.6 Managers will be responsible for ensuring that all Carrick Mind staff working in a service delivery role have read this Policy, the Information Sharing Policy and Access to Information Policy and are working to the required standard. They will ensure that a high standard of record keeping is maintained by conducting regular audits and will provide training for staff.

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