Name of Local Mind	Carrick Mind
Policy	Information Sharing Policy
Version	1
Date when last reviewed	
Date when next review due	Nov 2019
Author	Jon Gladstone
This policy is for:	Staff, Trustees, Volunteers

1. Introduction

1.1 Sharing information between partner organisations is vital to the provision of co-ordinated and seamless services where Carrick Mind's work is delivered in partnership with other organisations. In addition, the sharing of information can help to meet the requirements of statutory and local initiatives. However, any decisions to share information, particularly personal data, must be based on an appropriate risk assessment and the basis for lawful sharing agreed.

1.2 This Information Sharing Policy (referred to as this **Policy**) and the attached agreement in Appendix 1 set out the basis for the sharing of personal data. In each case, it is important to:

- Identify the lawful basis for sharing the information
- Set out what information will be shared
- Define the common purposes for holding and sharing the information
- Set out how the information will be kept secure

1.3 Personal data will only be shared for a specific lawful purpose or where appropriate consent has been obtained.

1.4 No personal data can be shared until the attached agreement under Schedule 1 has been signed by both partners.

1.5 This policy covers data in respect of

- beneficiaries

- supporter/campaigners
- donors
- volunteers
- staff

It does not cover staff names and work emails used in routine transactions, e.g. working with an event or conference organiser.

2. The partner organisations agree:

2.1 To share personal data with each other where it is lawful and when they are required to do so.

2.2 To comply with the requirements of Data Protection Legislation and in particular with the Data Protection Principles.

2.3 To inform individuals when and how information is recorded about them and how their information may be used.

2.4 To ensure that adequate technical and non-technical security measures are applied to the personal data they hold and transfer.

2.5 To promote internal awareness of the protocol.

3. Purposes for which information will be shared

3.1. The purposes for sharing the personal data will be set out in the attached agreement.

3.2. Where the provision of anonymised or pseudonymised data is adequate Carrick Mind must use these as a preferred method.

3.3. The partner organisation must ensure that personal data will only be made available on a justifiable 'need to know basis'. This means that staff will only have access to the information if the function they are required to fulfil in relation to a particular activity cannot be achieved without access to the information in question.

3.4. It may not be necessary to disclose all personal data held. Only such personal data as is relevant for the purpose for which it is disclosed should be passed under the sharing arrangement to the recipient(s).

4. Organisational responsibilities

4.1. A number of safeguards are necessary in order to ensure a balance between maintaining confidentiality and sharing personal data appropriately. Organisations which share information under this protocol will adhere to the following:

4.1.1. Ensure staff and others handling personal data on their behalf are aware of and comply with:

- their responsibilities and obligations with regard to the confidentiality of personal data of people who are in contact with them
- the commitment of the organisation to share information legally and within the terms of an agreed specific information sharing agreement
- the commitment that personal data will only be shared on a need-to-know basis
- the understanding that disclosure of personal data which cannot be justified, whether intentionally or unintentionally will be subject to disciplinary action, and may be subject to legal sanctions on the organisation or individual.

4.1.2. Ensure information disclosed is recorded appropriately by:

- Ensuring that all personal data that has been disclosed to them under an agreement is recorded accurately on that individual's manual or electronic record.
- Putting in place procedures to record the details of the information shared, the provider and who received the information.

5. Information security and confidentiality

5.1. The organisations will set out in the attached agreement how security for the shared information will be achieved.

5.2. In addition to the above the organisations party to this protocol will put in place documented policies and procedures governing:

- the secure storage of all personal data retained within their manual and/or electronic systems
- the secure transfer of personal data both internally and externally.

5.3. Such procedures must cover:

- Internal and external postal arrangements
- Verbal communications (phone, meetings etc)
- Facsimiles
- Electronic mail
- the access by their employees and others to personal data held in manual or electronic systems, and to ensure that access to such information is controlled and restricted to those who have a legitimate need to have access.
- the retention and disposal of records containing personal data.

6. Data quality

6.1. Information shared should be of a good quality and it is recommended that the information shared follows either the Audit Commission's six principles of data quality, or other appropriate guidance used by the organisations sharing the information. The six data quality principles are:

- Accuracy
- Validity
- Reliability
- Timeliness
- Relevance and
- Completeness.

Further information about these principles can be found in the Audit Commission document entitled "Improving information to support decision making: standards for better quality of data".

7. Access to information

7.1. Partner organisations will maintain accurate, up-to-date and relevant records and will fully inform individuals about the information that is recorded about them, who may see their information, for what purposes and their right to access or object to having their personal data disclosed.

7.2. Under Data Protection Legislation, individuals also have the right to access, subject to exemptions, information held about them and to correct any factual errors that may have been made. Where records are rectified, whether at the request of the individual or otherwise, any changes made as a result will be recorded and communicated to all organisations with whom the data had previously been shared.

7.3. Requests for access to information, objection or amendment should be sent to the relevant organisation's Data Protection Officer.

8. Sharing with organisations who are not signatories to this protocol

8.1. No information provided by partners to these procedures will be released to any other third party without the permission of the partner that disclosed the data (the **Owning Partner**) unless required to do by law or as permitted by the Data Protection Legislation in the public interest. Permission will always be sought in advance where possible from the Owning Partner and the Owning Partner will always be notified of any such disclosure in writing as soon as possible.

9. Monitoring and review

9.1. The organisations signed up to this protocol will review this protocol annually unless new or revised legislation necessitates an earlier review.

9.2. Each partner organisation will be individually responsible for monitoring and reviewing the implementation of this protocol.

10. Breach of Confidentiality

10.1. Each partner to this protocol will have in place appropriate measures to investigate and deal with the inappropriate or unauthorised access to, or use of, personal data whether intentional or unintentional.

10.2. In the event that personal data shared under this protocol is or may have been compromised, whether accidental or intentional, the organisation making the discovery will, without delay:

- Inform the Owning Partner of the details
- Take steps to investigate the cause
- Take disciplinary action against the person(s) responsible, if appropriate
- Take appropriate steps to avoid a repetition
- Take appropriate steps, where possible, to mitigate any impacts.

10.3. On being notified of a breach, the Owning Partner along with the organisation responsible for the breach, and others as appropriate, will assess the potential implications for the individual whose information has been compromised, and agree whether/ how to:

- Notify the individual(s) concerned;
- Advise the individual(s) of their rights; and
- Provide the individual(s) with appropriate support.

10.4. Where a breach is identified as serious, it may have to be reported to the commissioner/funder (where relevant), the Information Commissioner's Office and where possible the individuals who have been affected. The Owning Partner, along with the breaching organisation and others as appropriate, will assess the potential implications, identify and agree the appropriate action.

11. Complaints

11.1. The partner organisations must have in place procedures to address complaints relating to the disclosure of information. The partner organisations agree to cooperate in any complaint investigation where they

have information that is relevant to the investigation. Partners must also ensure that their complaints procedures are well publicised.

11.2. If the complaint affects more than one partner organisation it should be brought to the attention of the appropriate complaints officers who should liaise to investigate the complaint.

12. Organisational and individual responsibilities

12.1. Disclosure of personal data between partners without consent must meet the criterion for claiming an exemption under the Data Protection Legislation. Without such justification, both the organisation and the member of staff expose themselves to the risk of prosecution and liability to fines or claims under the Data Protection Legislation or damages for a breach of the Human Rights Act 1998.

12.2. Each partner will keep the other partner fully indemnified against any and all costs, expenses and claims arising out of any breach of this agreement and in particular, but without limitation, the unauthorised or unlawful access, loss, theft, use, destruction or disclosure by the offending partner or its subcontractors, employees, agents or any other person within the control of the offending partner of any data obtained in connection with this agreement.

Appendix One:

Personal Information Sharing Agreement

This Information Sharing Agreement ("**Protocol**") sets out the terms of the sharing of Personal Information as defined under Data Protection Legislation.

"Data Protection Legislation" means the General Data Protection Regulation (GDPR), the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) and, to the extent that it deals with Data Protection, the E-Commerce Directive 2000/31/EC together with any legislation, regulations or codes of practice made there under.

1. Managing the protocol

1.1. The organisations involved in this information sharing agreement are:

1.1.1 Carrick Mind, Unit 7, Jubilee Wharf, Commercial Road, Penryn, TR10 8FG

1.1.2 [Enter Text]

In relation to the following activities:

[insert contract/SLA/project name data sharing relates to]

For the duration of:

[Enter text]

1.2 This Protocol is owned equally by all/both partner organisations and is co-ordinated and administered on their behalf by:

_____ (role)

Of _____ (organisation).

1.3 This agreement will be reviewed annually and routinely reviewed following changes in legislation or statutory notices.

1.4 Where relevant, organisations should seek the agreement of their Caldicott Guardian, nominated deputy or Information Governance Officer before signing this protocol.

2. Legality

Sharing personal information in accordance with this protocol is lawful under Data Protection Legislation

[Add Text]

Where special categories of information (sensitive information) are processed the Legal condition under article 9 of the General Data Protection Regulation is required and documented below:

[Add Text]

and other legislation or statute is described below:

[Add Text]

3. Sharing information

3.1 The purpose of this information sharing agreement is:

[Add Text]

3.2 The information to be shared between signatory organisations is:

	Information	Data Controller Organisation	Owner
3.2.1			
3.2.2			
3.2.3			
3.2.4			

4. Data Controller(s)

The Data Controller for the information to be shared is listed above along with the role (owner) which has operational responsibility for the data.

4.1 The registration number and named contacts for each Data Controller organisation are:

Organisation	Registration No	Named Person	Contact Details

4.2 The information must only be used for the purposes stated in paragraph 3.1. The agreement of the Data Controller must be sought before using shared information for any other purpose.

4.3 The partner organisations receiving shared information must review the need to continue to hold it after _____ (period or date) and must destroy it after _____ (period or date). The outcome of review or destruction must be notified to the relevant Data Controller.

5. Caldicott Guardian (s)

5.1 The named Caldicott Guardians (where applicable) for each organisation are:

Organisation	Named Person	Role	Contact Details

6. Information quality

6.1 The quality assurance checks generally applied within _____ (originating organisation) are:

[Add Text]

6.2 Partner organisations receiving shared information are responsible for applying relevant quality assurance before using the information.

6.3 If information is found to be inaccurate, it is the responsibility of the partner organisation discovering the inaccuracy to notify the Data Controller. The Data Controller will ensure that the source data is corrected and will notify all recipients, who will be responsible for updating the information they hold.

6.4 Partner organisations will not be liable for any financial or other costs incurred by other parties to this protocol as a result of any information being wrongly disclosed by another party to this agreement or as a result of any negligent act or omission by another party to this agreement.

7. Information format and frequency

7.1 The format in which the information will be shared is _____

7.2 The frequency with which the information will be shared is _____
until _____

8. Information security and confidentiality

8.1 Security for the exchange of information will be achieved through:

[Add Text]

8.2 Security for the storage of exchanged information will be achieved through:

[Add Text]

8.3 Release to third parties
No information provided by partners to these procedures will be released to any third party without the permission of the owning partner.

8.4 Partner organisations receiving shared information will:

8.4.1 ensure that their employees are able to access only the shared information necessary for their role;

8.4.2 ensure that their employees are appropriately trained so that they understand their responsibilities for confidentiality and privacy;

8.4.3 protect the physical security of the shared information.

9. Consent to share personal information

9.1 It is generally good practice to seek the consent of service users. However, partner organisations agree that disclosure without consent is lawful if certain conditions are met. For example, personal information may be shared when anonymised or to ensure the performance of public functions or legal obligations.

9.2 Occasionally, an individual may refuse to give consent to share their information. Where it is lawful to share such information in spite of the refusal, the Data Controller must record the refusal of consent and the reasons for overriding that refusal.

9.3 The Data Controller is responsible for ensuring that data subjects are advised that their information is being or may be shared.

10. Complaints

10.1 The partners will use their standard organisational procedures to deal with complaints from the public arising from information sharing under this agreement.

10.2 If the complaint affects more than one partner organisation it should be brought to the attention of the appropriate complaints officers would should liaise to investigate the complaint.

11. Agreement

We undertake to implement and adhere to this information sharing protocol and agreement.
We undertake to ensure that our organisational procedures are consistent with this information sharing protocol and agreement.

The Data Controller and Caldicott Guardian of each partner organisation (where applicable) should sign this agreement.

Organisation 1:	
Signed:	
Date:	
Name:	
Position:	

Organisation 1:	
Signed:	
Date:	

Name:	
Position:	

Organisation 2:	
Signed:	
Date:	
Name:	
Position:	

Organisation 2:	
Signed:	
Date:	
Name:	
Position:	