Confidentiality Policy

1. CONFIDENTIALITY STATEMENT

Macc is committed to providing a confidential service to all users of its services and believes that principles of confidentiality must be integrated across all aspects of the organisation. Macc believes that users of its services deserve the right to confidentiality to protect their interests and to safeguard the organisation.

The purpose of this policy document is to establish a clear and agreed understanding of what confidentiality means within Macc, to encourage uniformity and to ensure that users of Macc services know what they can expect from the organisation. Users of Macc services refers not only to individuals who use the services but also groups and organisations. The policy document applies to all staff, volunteers, trustees and consultants of Macc and continues to apply after their service or involvement with Macc has ended. Any breach of confidentiality will be treated as a serious matter and may result in disciplinary action being taken.

2. GENERAL PRINCIPLES

2.1 Macc recognises that colleagues (employees, volunteers trustees consultants) gain information about individuals and organisations during the course of their work or activities. In most cases, such information will not be stated as confidential and colleagues may have to exercise common sense and discretion in identifying whether information is expected to be confidential. This policy aims to give guidance but if in doubt, seek advice from your line manager and or ask the person who supplied the information.

2.2 It is essential that all documentation, information and computer systems used within Macc, are protected to an adequate level from events which may jeopardise confidentiality. These events will include accidents as well as behaviour deliberately designed to breach confidentiality.

- Laptops or other electronic media taken out of the office should be password protected / encrypted and never left unattended. Macc colleagues should not leave Macc laptops, tablets, phones etc. in their cars. (see Macc Acceptable Use Policy)

- Confidential files taken out of the office should be kept under lock and key at all times.

- Colleagues are able to share information with their line manager in order to discuss issues and seek advice.

- Colleagues should avoid exchanging personal information or comments (gossip) about individuals with whom they have a professional relationship.

- Colleagues should avoid talking about organisations or individuals in social settings.

- All information gathered by colleagues will only be shared within Macc except where permission to share more widely has been expressly given.

- Colleagues will not disclose to anyone, other than their line manager, any information considered sensitive, personal, financial or private without the knowledge or consent of the individual, or an officer, in the case of an organisation.

- There may be circumstances where colleagues would want to discuss difficult situations with each other to gain a wider perspective on how to approach a problem. Names or identifying information must remain confidential within Macc.

- Where information is of a sensitive nature and/or may cause a conflict of interest for Macc staff, the information may be restricted to certain staff only on a need to know basis. For example Macc have a clear separation between the duties of our internal grants management team workers and our capacity building workers.

- Where there is a legal duty on Macc to disclose information, the person to whom the confidentiality is owed will be informed that disclosure has or will be made, unless there are safeguarding or legal reasons that would prevent this.

- Where an individual we hold confidential information about is deceased Macc will still treat this data as protected data for the purposes of this policy.

3. WHY INFORMATION IS HELD

3.1 Most information held by Macc relates to the employees, trustees, users of our services, funders, consultants etc.

Information is kept to enable Macc colleagues to understand the history and activities of individuals and organisations in order to deliver the most appropriate services.

Anonymised information about our users relating to the nine protected characteristics under the Equality Act 2010 is kept for the purposes of monitoring Macc's equal opportunities policy and for reporting to funders.

4. ACCESS TO INFORMATION

4.1 Information is confidential to Macc as an organisation and may be passed to colleagues, line managers or trustees to ensure the best quality service for users of its services.

Where information is sensitive, i.e. it involves disputes or legal issues; it will be confidential to the employee dealing with the case and their line manager. Such information should be clearly labelled 'Confidential' and should state the names of the colleagues entitled to access the information and the name of the individual or group who may request access to the information.

Colleagues will not withhold information from their line manager unless it is purely personal.

4.2 Users of Macc services may have sight of records held in their name or that of their organisation. For requests to see individual records please see our data protection policy and subject access request form. In the case of an organisations records, the request must be in writing and signed by the organisations Chair or Chief Executive. Macc will respond within 30 days. Sensitive information as outlined in paragraph 4.1 will only be made available to the person or organisation named on the file.

4.3 Employees of Macc may have sight of their personnel records, see our Data Protection policy and complete a subject access request form, where the request is for full access to all records, or a substantial portion of them. Requests may take up to 30 days to process, depending on complexity.

4.4 When photocopying or working on confidential documents, colleagues must ensure they are not seen by people in passing. This also applies to information on computer screens.

5. STORING INFORMATION

5.1 General non-confidential information about organisations is kept in unlocked filing cabinets/shelves.

5.2 Confidential information about organisations is kept in locked filing cabinets and drawers and on password protected computer drives. Macc operates a clear desk policy for confidential documents.

5.3 Employees' personnel information will be kept in lockable filing cabinets by line managers and the Finance Manager and will be accessible to the Chief Executive.

5.4 Filing cabinet drawers holding confidential information should be lockable. All files containing confidential information should be labelled 'confidential'.

5.5 In an emergency situation, the Finance Manager may authorise access to files by other people as necessity and business continuity dictates.

5.6 Confidential information stored on computer will be protected by use of passwords.

5.7 See also Macc's Record Retention & Data Cleansing Policy, Data Protection Policy.

6. DUTY TO DISCLOSE INFORMATION

6.1 There is a legal duty to disclose some information including:

- Child abuse which will be reported to the Social Services Department
- Drug trafficking, money laundering, acts of terrorism or treason will be disclosed to the police. (See separate Macc procedures to prevent potential money laundering).
- In addition, colleagues believing an illegal act has taken place, or that a user of Macc's services is at risk of harming themselves or others, must report this to their line manager or the Chief Executive who will report it to the appropriate authorities.
- Macc has a duty of care towards vulnerable adults with whom staff and volunteers have contact. All volunteers and staff have a duty of public interest to report concerns relating to adult abuse, this overrides the duty of confidentiality. (See separate policy on Safeguarding).
- Macc has a duty of care towards children and young people under the age of eighteen. It is a requirement that any member of Macc staff or any volunteer working on behalf of Macc has a responsibility to pass on information and concerns regarding a child or young person who may have been or are likely to be harmed or abused; this overrides the duty of confidentiality. (See separate Policy on Safeguarding).

Users of Macc's services should be informed of any disclosure relating to them, where it is safe to do so and where legislation does not prevent this.

7. DISCLOSURES

7.1 Macc complies fully with the Disclosure and Barring Service Code of practice and regarding the correct handling, use, storage, retention and disposal of Disclosures and Disclosure information. (See separate Policy on the Recruitment).

7.2 Disclosure information is always kept separately from an applicant's personal file in secure storage with access limited to those who are entitled to see it as part of their duties. It is a **criminal offence** to pass this information to anyone who is not entitled to receive it.

7.3 DBS Documents will be kept up to 6 months and then destroyed by secure means. Photocopies will not be kept. However, Macc may keep a record of the date of issue of a Disclosure, the name of the subject, the type of Disclosure requested, the position for which the Disclosure was requested, the unique reference number of the Disclosure, as allowed by the Disclosure and Barring Service.

8. DATA PROTECTION ACT 2018 AND GDPR

8.1 Information about individuals, whether on computer or on paper, falls within the scope of the Data Protection Act 2018 and GDPR and must comply with the data protection principles. These are that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected only for legitimate purposes that have been clearly explained and not further processed in a way that is incompatible with these purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- Accurate and, where necessary kept up-to-date
- Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
- Processed in a way that ensures appropriate security of the personal data

Macc has a separate Data Protection Policy.

9. BREACH OF CONFIDENTIALITY

Employees who are dissatisfied with the conduct or actions of other colleagues should raise this with their line manager as outlined in the grievance procedure.

Colleagues accessing unauthorised files or breaching confidentiality may face disciplinary action. Ex-employees breaching confidentiality may face legal action.

10. WHISTLE-BLOWING POLICY

Macc has a Whistle-blowing Policy which is intended to encourage and enable staff and volunteers to raise serious concerns connected with any area within the organisation or any organisation that they come into contact with while carrying out activities on behalf of Macc. The Whistle-blowing Policy applies to all employees and volunteers and is in addition to the Grievance and Complaints Policies.

11. DISPOSING OF CONFIDENTIAL MATERIAL

Colleagues are reminded that Macc provides confidential waste facilities which should be used for all confidential material which is no longer required. All documentation (including printed e-mails, notes, scrap paper, reports, files) that are not in the public domain should be destroyed using the confidential waste facilities provided.

Colleagues should ensure that confidential electronic information is double deleted. Refer to record retention and data cleansing policy for guidance.

12. MONITORING

The effectiveness of this policy and of confidentiality at Macc will be monitored. This is done by:-

- Recording all complaints about breaches of confidentiality, and regularly reviewing these in management team.

- Addressing issues of breaches or possible breaches of confidentiality directly with the person.

13. DATA PROTECTION

In the implementation of this policy, Macc may process personal data and/or special category personal data collected in accordance with its GDPR and data protection policy, (in order to conduct any investigations into a breach of confidentiality for example). This would be processing data originally collected for a different purpose, but still in Macc's legitimate interest. Any data processed from the point at which this policy is invoked will only inform the organisation for the benefit of implementing this policy. All data is held securely and accessed by, and disclosed to, individuals only for the purposes of this policy. Inappropriate access or disclosure of personal data which includes employee, volunteer, trustee, service user, consultant data constitutes a data breach and should be reported in accordance with Macc's GDPR and data protection policy immediately. It may also constitute a disciplinary offence, which will be dealt with under the organisation's disciplinary procedure.

Macc

Statement of Confidentiality

Macc is committed to providing a confidential service to all users of its services and believes that principles of confidentiality must be integrated across all aspects of the organisation. Macc believes that users of its services deserve the right to confidentiality to protect their interests and to safeguard the organisation.

The purpose of this policy document is to establish a clear and agreed understanding of what confidentiality means within Macc, to encourage uniformity and to ensure that users of its services know what they can expect from the organisation. Users of its services refers not only to individuals who use the services of Macc but also organisations. The policy document applies to all staff, volunteers, trustees and consultants of Macc and continues to apply after their service or involvement with Macc has ended. Any breach of confidentiality will be treated as a serious matter and may result in disciplinary action being taken.

Declaration of Confidentiality

I have read and understood the Confidentiality Policy and all the policies referred to in the policy and agree to conform with its requirements as outlined in the statement above.

Signed: ……

Name (block capitals): ……

Date: ……