Data Protection Policy and Procedures

Introduction

Macc recognises the importance of the correct and lawful treatment of personal data; it maintains confidence in the organisation and provides for successful operations. In order to ensure effective delivery of services, Macc is required to maintain certain personal data about individuals in order to carry out our work and legal obligations. This personal information must be collected and dealt with appropriately.

The aim of this policy is to ensure that everyone handling personal data is fully aware of the requirements and acts in accordance with data protection procedures.

The Data Protection Legislation (Data Protection Act 2018) governs the use of information about people (personal data). Personal data can be held on computer or in a manual file, and includes email, minutes of meetings, and photographs.

Macc will remain the data controller for the information it collects and holds. Macc, its board members, staff and volunteers will be personally responsible for processing and using personal information in accordance with the current legislation.

All board members, staff and volunteers working with in Macc who have access to personal information, will be expected to read and comply with this policy. None compliance with this policy could result in disciplinary action, loss of job (or volunteering placement), personal fines and potentially imprisonment.

You can find a definition of the key terms used in this policy at the end of the document. This Data Protection Policy is part of our Information Governance Framework and Macc workers should also read other policies in the framework on the shared drive here: M:\Macc Policy & Procedures\Information Governance

1. Principles

The Data Protection Legislation sets out seven key principles (Article 5(1)) which are summarised as follows:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

These principles specify the legal conditions that must be satisfied in relation to obtaining, handling, processing, transportation and storage of personal data and lie at the heart of the GDPR. Compliance with the spirit of these key principles are the fundamental building blocks for good data protection practice and compliance.

Macc fully endorses and adheres to these principles. Employees and any others who obtain, handle, process, transport and store personal data for Macc must adhere to these principles.

Macc will provide training to our staff and volunteers on Data protection and information governance, this takes place on induction and then annually as part of our mandatory training programme.

2. Responsibilities

Macc Board will ultimately take responsibility for the implementation of this policy and take into account legal requirements to ensure that it is properly implemented.

Macc is currently not legally required to have a Data Protection Officer. However, a Data Protection Lead has been identified and will be responsible for ensuring that the policy is implemented and will have the responsibility:

- To inform and advise the organisation, the board and its employees about their obligations to comply with Data Protection Legislation.
- To monitor compliance with Data Protection Legislation, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits.
- To ensure Macc continues to be registered with the Information Commissioner and that are details remain up to date,
- To be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc).

Staff and Volunteers are actively encouraged and supported through training and their line manager to report any concerns that they may have in order to improve both our data protection and services to users.

However, all staff and volunteers are also aware that a deliberate breach of the rules and procedures identified in this policy may result in disciplinary action being taken against them.

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to legislation. In case of any queries or questions in relation to this policy please contact the Macc Data Protection Lead:

Martin Preston
Macc Swan Buildings, Swan Street, Manchester M4 5JW

Macc ensures that our details are registered with the Information Commissioner. The current certificate expires in **10 September 2021**. A copy of the notification is located in the Macc office. You can see Macc's registration online on the Data Protection Register by going to https://ico.org.uk/ESDWebPages/Entry/Z9595019

3. Data collection

Macc will only collect data that is 'necessary' to conduct its operational and contractual requirements. It will identify the lawful basis for processing and ensure that this communicated clearly within its privacy notices and that appropriate documentation of our processing activities is recorded.
When collecting data, Macc will ensure that the Individual/Service User:

a) Clearly understands why the information is needed

b) Understands what it will be used for and what the consequences are should the Individual/Service User decide not to accept the purposes of processing

c) Where necessary, grants explicit consent, either written or verbal for data to be processed

d) Is, as far as reasonably practicable, competent enough to understand what processing would require and if necessary provide consent that has been given freely.

e) Has received sufficient information on why their data is needed and how it will be used.

f) Further information on the data we collect including its conditions for processing can be found within the Macc Privacy Notice.

4. Data Storage, Retention and Disposal

Information and records relating to service users will be stored securely and will only be accessible to authorised staff and volunteers.

Information will be stored for only as long as it is needed or required statute and will be disposed of appropriately. The retention period for relevant data shall be recorded with Macc's Retention Policy and Procedure

Macc will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure. The measures taken include:

- Personal Data will be kept in locked filing cabinets with access restricted to those people whom have authority to access the data
- Password protection on personal information files
- Restricted access to computer files and systems
- Use of secure VPN mechanisms to ensure personal data does not need to be duplicated unnecessarily
- Data, including personal data, is backed up daily and information kept off site
- Suitable encrypted attachments for sensitive personal information sent by email

Any deliberate unauthorised disclosure of personal data to a third party by an employee may result in disciplinary proceedings.

The Board and directors are accountable for compliance of this policy. A director could be personally liable for any penalty arising from a breach that they have made.

Any deliberate unauthorised disclosure made by a volunteer may result in the termination of the volunteering agreement.

It is Macc's responsibility to ensure all personal and company data is non-recoverable from any computer system previously used within the organisation, which has been passed on/sold to a third party. Any external destruction of data will be undertaken under contract and undertaken to any relevant British Standard.

Further information can be found in Macc's Retention Policy and Procedure

5. Data Accuracy

Macc will undertake reasonable steps to ensure data is kept accurate and up to date. This includes:

- To limit errors, data will only be held where necessary
- Asking data subjects whether there have been any changes to their information
- Ensuring that when inaccuracies are found that records are updated e.g. an out of date phone number is deleted from files
- Investigating and acting upon any notifications by individuals of inaccuracies.

6. Training

Training and awareness raising about the Data Protection Legislation and how it is followed in this organisation will take the following forms:

On induction: All new staff, trustees and volunteers will have an assessment of their understanding of Data Protection during the induction process. Following this assessment staff will have a session which will outline Data Protection regulations, the organisations policy and procedures in respect of Data Protection and their responsibilities as staff volunteers of Macc. Staff and Volunteers will be asked to sign a declaration confirming they understand and will adhere to the policy.

General training/ awareness raising: Information will be placed around the building and distributed via regular email updates to remind staff of the principles of data protection. This will be in the form of simple do's and don'ts. Staff will be reminded of their responsibilities at team meeting and in line management. Where required staff will offered additional training as part of staff training and professional development opportunities.

Macc will ensure that:

- Everyone managing and handling personal information is trained to do so.
- Anyone wanting to make enquiries about handling personal information, whether a member of staff, volunteer or service user, knows what to do;
- Any disclosure of personal data will be in line with our procedures.
- Queries about handling personal information will be dealt with swiftly and politely.

7. Data Protection by Design

Macc is committed to considering data protection and privacy issues upfront in everything we do. Macc are committed to integrating data protection into all our activities and practices, from the design stage right through delivery lifecycles. This includes:

- Anticipating risk and privacy invasive events through the organisational risk register and taking steps to prevent harm to individuals.
- Considering data protection issues as part of the planning, design and implementation of systems, services and delivery. Both through broader tools and Data Protection Impact Assessments as required.
- Only processing the personal data that we need for our purposes(s), and that we only use the data for those purposes.
- Providing the identity and contact information of those responsible for data protection both within our organisation and to individuals.
- Ensuring that data processors can provide sufficient guarantees of the measures for data protection.
- Using 'plain language' policy with any public documents and privacy notices so that individuals easily understand what we are doing with their personal data.

8. Individual Data subject rights

The GDPR provides the following rights for individuals:

1. **The right to be informed**. This includes an obligation on organisations processing personal information to provide fair processing information, typically through a privacy notice and be transparent over how they use personal data.

Detailed information about the type of personal information Macc collects how we do this, why we collect it, how we use it and how we keep it safe is contained in our Privacy Policy and privacy notices:

Privacy Notice for Staff
Privacy Policy
Individual project privacy notices

2. Right of access

Under legislation individuals have the right to access data held about them as well as the right to be 'forgotten' where there is no longer a compelling reason to continue processing.

A subject access request can be considered as any enquiry whether written (including email or webform) or verbal that asks for information you hold about the person

Individuals can only request access to their own data (or must provide evidence that they are legitimately acting on another person's behalf). Macc may request proof of identity to ensure this.

Macc may request further information on or clarification of the request

Information mentioning other people will be redacted if reasonable to do but may not be shared unless reasonable to do so or unless consent can be obtained for the relevant individual.

Where requests are manifestly unfounded or excessive, in particular because they are repetitive Macc may charge a fee or refuse to respond. However individuals will receive a response to this affect and details of an appeals process (within the next calendar month)

Macc will respond to any formal request within a calendar month. If there is a delay in obtain the information requested then the request shall still be acknowledged within this period with an explanation for the delay and an expected date of response.

Members of the public may request certain information from statutory bodies under the Freedom of Information Act 2000. The Act does not apply directly to Macc. However if at any time we undertake the delivery of services under contracts with relevant statutory bodies we may be required to assist them to meet the Freedom of Information Act request where we hold information on their behalf.

3. **The right to rectification.** Personal data will be corrected if it is inaccurate or incomplete.

4. **Right to erasure.** This is also known as the right to be forgotten. It allows an individual to request the deletion or removal of personal information where there is no compelling reason for its continued processing. E.g. it is no longer necessary for the purpose it was originally collected.

5. **Right to restrict processing.** Individuals have a right to block or suppress the processing of personal data. The data can still be stored, but must not be further used. The circumstances in which processing may be restricted could be where an individual contests the accuracy of personal data, and wants it to be verified, or where the organisation no longer needs the data, but the individual does (for a legal claim for example).

6. **Right to data portability.** This gives individuals the right to obtain and reuse their personal data for their own purposes across different services. This right only applies to data provided by the individual, based on consent or for performance of a contract and where processing is carried out by automated means.

7. **Right to object.** Individuals have the right to object to direct marketing and processing based on legitimate interests. Macc gives all our service users choices about their marketing preferences when they first contact us and these preferences can be changed at any time.

8. **Rights related to automated decision making including profiling.** This is related to automated individual decision making and profiling. At present Macc does not engage in this activity.

In case of any requiring further information on this aspect of the policy please read Macc Data Subject Access Request / Rights Procedure or contact the Macc Data Protection Lead.

9. Disclosure & Data Sharing

Macc may need to share data with other agencies such as local authorities, funding bodies and other voluntary agencies as part of its work.
The Data Subject will be made aware in most circumstances how and with whom their information will be shared as part of the Privacy Notice process. However, there are circumstances where the law allows Macc to disclose data (including sensitive data) without the data subject's knowledge.

These include:

1. When required to by law – This may as simple as providing information to HMRC for tax purposes or if required by the police in relation to a crime.
2. Protecting vital interests of a Data Subject or other person – This includes safeguarding concerns where an individual may be at risk or in cases of medical emergencies.
3. The Data Subject has already made the information public
4. Conducting any legal proceedings, obtaining legal advice or defending any legal rights

Macc regards the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal.
Macc will ensure that personal information is treated lawfully and correctly.
Staff or Volunteers who are unsure about whether they can legitimately disclose personal data to an individual or organisation should seek advice from their line manager or the Data Protection Lead.

10. Risk Management

The consequences of breaching Data Protection can cause harm or distress to service users if their information is released to inappropriate people, or they could be denied a service to which they are entitled.

This policy and the supporting policies and procedures are designed to minimise the risks and to ensure that the reputation of Macc is not damaged through inappropriate or unauthorised access and sharing.

Data Protection is everyone's responsibility if staff or volunteers know or suspect that a personal data breach has occurred, then they should immediately contact the Data Protection Lead.

Macc makes every effort to avoid data protection incidents, however, it is possible that mistakes will occur on occasions. Examples of how personal data incidents might occur include through:

- Loss or theft of data or equipment
- Ineffective access controls allowing unauthorised use
- Equipment failure

- Unauthorised disclosure (e.g. email sent to the incorrect recipient)
- Human error
- Hacking attack

In the event of a breach leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, Macc will promptly assess the risk to individuals concerned and if appropriate report this breach to the ICO (more information is available on the ICO website).

If a reportable breach has occurred MAcc is required to notify the Information Commissioner's Office as soon as possible, and not later than 72 hours after becoming aware of it.

Staff and Volunteers are actively encourage to report any incidents or concerns that they may have in order to improve both our data protection and services to users.

However, staff and volunteers are also aware that they can be personally liable if they deliberately or maliciously use service user's personal data inappropriately.

Macc have a detailed Personal Data Breach Response Plan to guide managers in addressing any breaches that do occur.

11. Related Policies

Data protection is an organisation wide process and this policy does relate to other policies and documents within the organisation including but not limited to Subject Access Requests Procedure, Archiving and Retention Policy and Procedure, Organisation Risk Register, IT Acceptable Usage Policy, and Business Continuity.

12. Policy review

This policy will be reviewed regularly by the Macc board (see schedule table below)

13. Further Information

If staff, volunteers or members of the public/or stakeholders have specific questions about information security and data protection in relation to Macc please contact the Data Protection Lead:

Martin Preston
Macc Swan Buildings, Swan Street, Manchester M4 5JW
data@macc.org.uk

The Information Commissioner's website (www.ico.gov.uk) is another source of useful information

Appendix i – Glossary of Terms
The following list contains definitions of the technical terms we have used and is intended to aid

Data Controller – The person who (either alone or with others) decides what personal information Macc will hold and how it will be held or used.

Data Protection Act 2018 – The UK legislation that provides a framework for responsible behaviour by those using personal information.

Data Protection Impact Assessments (DPIA) - is a process to help you identify and minimise the data protection risks of a project.

Data Protection Lead – The person(s) responsible for ensuring that Macc follows its data protection policy and complies with legislation.

Individual/Service User – The person whose personal information is being held or processed by Macc for example: a client, an employee, or member.

Information Commissioner (ICO)– The UK Information Commissioner responsible for implementing and overseeing the Data Protection Act 1998.

Processing – means collecting, amending, handling, storing or disclosing personal information.

Personal Information – Information about living individuals that enables them to be identified – e.g. name and address. It does not apply to information about organisations, companies and agencies but applies to named persons, including service users, individual volunteers or employees

Sensitive data – refers to data about:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation.

Policy Checklist

Data Protection Policy/Procedure

Date first adopted: 10 July 2007

Review dates:

Date of review	Amendments/Updates made	Reviewed & accepted as is ✔	Proposed next review date
8 August 2010		✓	8 August 2011
August 2011		✓	August 2012
17 June 2013	Policy amended to reflect volunteering roles in the organisation		
16 April 2014	Reviewed by Mike Wild and Mark Pritchard. Amendments: - correct name for Macc ORCA Database - 'Inland Revenue' changed to 'HMRC' - more specific distinctions between employees and volunteers	MW	July 2015
13 September 2016	Reviewed by Mike Wild and Martin Preston Amendments: - changed date of Information Commissioner registration to 10 September 2017 - 'voluntary and community group' changed to voluntary, community and social enterprise group' (VCSE) - changed 'Internal Operations Director' to 'Deputy Chief Executive' - web link to Link to Subject Access Requests good practice information amended - web link to Macc's registration details on Information Commissioner's web site amended	MW	September 2017
25 June 2018	Reviewed by LC/ DSWG Added introduction Changed DP Act to GDPR throughout Amended section on managing DP, added MP as IG lead Changed date of ICO registration expiry and checked link Changed description of DP principles and Inserted new links to six principles on ICO site. Also inserted links to Macc procedures where applicable to demonstrate compliance. Added hyperlinks for linked policy in data security section Added section on types of personal data we hold Expanded section on individuals rights Removed section on disclosure as this is	Trustees	July 2021

	now dealt with in privacy policy, but included in new section on principles Removed subject access requests- replaced by individual rights under GDPR section Removed employee/ volunteer monitoring- covered in privacy notice for staff (need to produce privacy notice for volunteers) Removed transfer out of EU- this is covered in privacy notices Removed records as this refers to employment records only and is covered in the DP team tables in greater detail and reference is made to retention periods earlier in the policy New section on breach Added Definitions		
15/04/2021	Updated links, updated language to simplify / aid understanding. Trustees to review July 2021.	LC for MT	July 2024

Declaration

I confirm I have read and understood Macc's Data Protection Policy and will act in accordance with it.

I am connected with this organisation in my capacity as a

- ☐ Member of staff
- ☐ Volunteer
- ☐ Trustee

Signature:
Print name:
Date:

Please return this form to Martin Preston