Data Protection Policy and Procedures

Introduction

This policy sets out how Macc processes personal data. It explains what data we keep and why and how we make sure this information is kept safe and is as accurate as possible. The policy provides guidelines on individuals' rights to see their data and the circumstances under which we may disclose data to others. It applies to all personal data that we process regardless of the way that information is stored (e.g. on paper, electronically or other means). 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.

Policy Statement

Macc is committed to protecting the rights and privacy of individuals, voluntary, community and social enterprise (VCSE) group members, trustees, staff, volunteers and others in accordance with The General Data Protection Regulation (GDPR) and Data Protection Act 2018. The policy applies to all Macc workers.

As a matter of good practice, other organisations and individuals working with Macc, and who have access to personal information, will be expected to have read and comply with this policy. It is expected that any staff who deal with external organisations will take responsibility for ensuring that such organisations sign a contract agreeing to abide by this policy. For more formal partnerships / joint delivery, a joint data protection agreement may be needed and Macc workers should consult Martin Preston, Information Governance lead at an early stage of discussions.

Macc takes compliance with the Act and this policy very seriously. Any breach of The GDPR and Data Protection Act 2018 or Macc Data Protection Policy is considered as misconduct and in that event, Macc disciplinary procedures apply. A significant or deliberate breach of this policy, such as accessing a data subject's personal data without authority or unlawfully obtaining or disclosing a data subject's personal data (including for a third party) without Macc's permission constitutes gross misconduct and could lead to dismissal. If you are not an employee, you may have your contract with us terminated immediately.

Legal Requirements

Data is protected by the GDPR and Data Protection Act 2018, which came into effect on 25 May 2018. Its purpose is to protect the rights and privacy of individuals and to ensure that personal data is not processed without their knowledge, and, wherever possible, is not processed without their consent.

The Act requires Macc to register the fact that we hold personal data and to acknowledge the rights of 'data subjects' – VCSE group members, trustees, staff and volunteers must have the right to copies of their own personal data, and to know that we are processing this data lawfully.

Managing Data Protection

For the purposes of GDPR Macc is a Data Controller. Responsibility for data protection begins with the board of trustees and runs through all levels of the organisation. Martin Preston is Macc's Information Governance lead and has day-to-day responsibility for leading on Data Protection and Information Governance at Macc.

Macc ensures that our details are registered with the Information Commissioner. The current Notification expires in **10 September 2018**. 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

Data Protection Principles

Under the GDPR, there are six data protection principles that Macc must comply with, personal data we hold must be:

1. **Processed lawfully, fairly and in a transparent manner**
   Macc have robust internal systems in place to ensure we are clear about the purpose and lawful basis of our personal data processing. There are six lawful basis for processing laid down in the GDPR. Macc hold an Information Assets Register to record the lawful basis of our processing. This is maintained by our Digital Services Working Group. To aid transparency we have developed a Privacy Policy and privacy notices appear at all points where personal data are requested.

2. **Collected only for legitimate purposes that have been clearly explained and not further processed in a way that is incompatible with these purposes**
   Macc will not use data for a purpose other than those agreed by data subjects (VCSE group members, trustees, staff, volunteers and others). If the data held by Macc are requested by external organisations for any reason, this will only be passed if data subjects (voluntary and community group members, trustees, Macc workers and others) explicitly agree. There may be some limited exceptions to this, for example in cases of fraud or safeguarding where Macc is legally required to pass on information. (See Privacy Notice for Staff and Privacy Policy) Macc must be satisfied the data will be handled safely, external organisations must state the purpose of processing, agree not to copy the data for further use and sign a contract agreeing to abide by The Data Protection Act 2018 and GDPR and have a Data Protection Policy.

3. **Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed**
   Macc will monitor the data held for our purposes, ensuring we hold neither too much nor too little data in respect of the individuals about whom the data are held. Macc have

developed an organisation wide process for reviewing, anonymising and deleting data where relevant, via the Digital Services Working Group.

4. **Accurate and, where necessary kept up-to-date**
   Macc will provide our data subjects (VCSE group members, trustees, Macc workers and others) with a copy of their data once a year for information and updating where relevant. All amendments will be made immediately and data no longer required will be deleted or destroyed. It is the responsibility of individuals and organisations to ensure the data held by Macc are accurate and up-to-date. Completion of an appropriate form (e.g. Macc Civi Database form) will be taken as an indication that the data contained are accurate. Macc workers should notify Macc of any changes, to enable personnel records to be updated accordingly. It is the responsibility of Macc to act upon notification of changes to data, amending them where relevant.

5. **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**
   Macc discourages the retention of data for longer than it is required. Retention periods vary depending on the type of data and it is the responsibility of each team within Macc to keep its retention policy under careful review. Macc is drafting a Document Retention and Archiving Policy.

6. **Processed in a way that ensures appropriate security of the personal data**
   This means appropriate technical and organisational measures should be in place against unauthorised or unlawful processing of personal data and against accidental loss or destruction of data.

   All Macc computers have a password protected log in system and the Macc Civi Database is password protected, which allow only authorised personnel to access personal data. Passwords on all computers are changed frequently. All personal and financial data is kept in a locked filing cabinet and can only be accessed by the Chief Executive, the Deputy Chief Executive and the Finance and Facilities Manager. When Macc workers are using the laptop computers and other electronic equipment out of the office care should always be taken to ensure that personal data on screen is not visible to non-Macc workers. Macc operates a clear desk policy. Great care should be taken when dealing with requests for information from third parties. See dealing with requests for data sharing below, and if in doubt always refer to a line manager or supervisor. Never give out personal details over the phone and only give details that are in the public domain (i.e. relating to an organisations public contact details and available on our public website) should be shared. Never share information from the Civi Database without permission from the data subject. All staff, volunteers, interns and apprentices at Macc will receive Data protection training on the procedures specific to their teams at induction. Appropriate security is kept under review by the digital services working group, more specific information on security measures for Macc workers can be found on the shared drives.

   Macc has a suite of Information Governance Policies and policies linked to data security are. Macc workers can access these on the shared drive:
   Confidentiality
   Bring Your Own Device
   Acceptable Use

Working from Home
Dealing with requests for data sharing. <To be drafted>
Information Security

Types of Personal Data held by Macc

Personal information is any information about an individual from which that person can be directly or indirectly identified. It does not include anonymised data, i.e. where all identifying particulars have been removed. There are also **'special categories'** of personal information and personal information on criminal convictions and offences, which requires a higher level of protection because it is of a more sensitive nature. The special categories of personal data are information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation, and genetic and biometric data.

In addition to the six lawful basis for processing personal data special category data must also have a separate condition for processing. This will usually be the explicit consent of the subject, but there are also other conditions. Whilst it is accepted that data of this nature may sometimes be used for monitoring purposes, strict safeguards will always be in place to ensure that individuals cannot be identified.

Macc collects uses and processes a range of personal information. This may be about staff, contractors, volunteers, trustees, voluntary and community group members.

Purpose of Data held by Macc

Macc holds data for the following purposes:

1. Staff volunteer and trustee administration
2. Fundraising
3. Realising the objectives of a charitable organisation or voluntary body
4. Accounts and records
5. Advertising, marketing and public relations
6. Information and database administration
7. Journalism and media
8. Processing for not for profit organisations
9. Research

Individual 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:

GDPR Privacy Notice for Staff
GDPR Privacy Policy

2. **The right of access.** Individuals have the right to access their data; (known as Subject Access) to help them understand how their data is being used and if this is being done lawfully. This request can be made verbally or in writing (via any format including social media) and can be made to any member of Macc staff. Macc will respond to the request within one month. The individual requesting access does not have to use any special forms or the words subject access for the request to be valid. Information will be provided free of charge. The only exception to this is if requests are received which are 'manifestly unfounded or excessive, in particular because they are repetitive' In this case an administration fee may be charged.

3. **The right to rectification.** Personal data can 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.

More details can be found in our privacy policy and privacy notices. Procedures for staff in dealing with requests from data subjects on any of the above rights can be found in our data subjects' rights policy and procedure (currently in draft in the meantime please refer to Martin

Preston or your line manger). Any such request should be reported to Martin Preston and logged in then Subject Access spreadsheet.

Personal Data Breach

A personal data breach happens where personal data is lost, destroyed, altered, corrupted or disclosed, accessed or passed on without proper authorisation. Or if the data is made unavailable and this causes significant negative effect to individuals. This includes breaches that are the result of both accidental and deliberate causes.

Personal data breaches can include:

- Access by an unauthorised third party
- Sending personal data to an incorrect recipient
- Computing devices (tablets, mobiles etc.) containing personal information being lost or stolen
- Alteration of personal data without permission
- Loss of availability of personal data

If a personal data breach occurs steps should be taken promptly to address it:

- All Macc workers should **immediately** inform their line manager/supervisor of any data security incident, and in their absence any other member of the Macc management team
- The manager will then immediately alert Martin Preston, Information Governance Lead, who will form a response team
- The response team will establish the likelihood and severity of any resulting risk to people's rights and freedoms because of the breach
- If it is likely there will be a risk then the ICO must be notified within 72 hours of Macc becoming aware of the breach
- If the ICO are notified then the Charity Commission and relevant funders will also need to be notified
- If the breach involves a high risk to the rights and freedoms of individuals then the individual must also be informed without undue delay
- Macc have a detailed Personal Data Breach Response Plan to guide managers in addressing any breaches that do occur

Definitions

Consent means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which they, by a statement or by clear affirmative action, signify their agreement to the processing of personal data relating to them.

Data subject means a living identified or identifiable individual about whom the company holds personal data.

Macc worker means any trustee, employee, apprentice, intern, volunteer, contractor or consultant employed or engaged by Macc.

Personal Data is any information relating to a data subject who can be identified (directly or indirectly) either from those data alone or by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, mental, economic, cultural, social, genetic identity of that data subject. It excludes anonymised data where all identifying particulars have been removed.

Processing is any operation or set of operations which is performed on personal data or sets of personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disclosing, disseminating, restricting, erasing or destroying. It also includes transmitting or transferring personal data to third parties.

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	MW	September 2017

	amended - web link to Macc's registration details on Information Commissioner's web site amended		
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 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		