Reg. Charity No: 1037518

Multicultural Arts and Media Centre

Confidentiality & Data Protection Policy

Section	Details
1. General Statement	MAMC recognises that a guarantee of confidentiality in the services it provides is an important factor in determining the level of trust and security its service users hold in the organisation. The purpose of this policy document is to establish a clear and agreed understanding of what confidentiality means within MAMC and its projects, to encourage uniformity in practice and ensure that service users know what they can expect from the organisation. The team service-user refers not only to individuals who use MAMC services, but also groups and organisations, which consult MAMC and its projects and share with it confidentiality information about their agency. The policy applies to all staff, volunteers and directors of MAMC and continues to apply after their service or involvement with MAMC has ended.
	Responsibilities and Arrangements for Confidentiality
2. The management committee	The Management Committee Members as the employer has overall and final responsibility for ensuring that MAMC meets its legal responsibilities regarding confidentiality in relation to criminal record checks, the Data Protection Act and any current or subsequent human rights legislation, which guarantees a right of policy. The Management Committee Members will review the operation of this confidentiality policy annually.
3. The Chief Officer	The Chief Executive has overall responsibility for ensuring that the confidentiality policy is put into practice. In particular the Chief Executive will ensure that: 3.1 Line managers are aware if their responsibilities to their staff and volunteers. 3.2 There are arrangements in place to properly monitor and implement this policy.
4. General principles	Information belongs to the person or agency entrusting it to a member of staff or volunteer of MAMC. Information remains personal and in the control of the giver. Once received by MAMC, it may not be used for any purpose other than which it was given; nor may it be passed on to any person or agency outside MAMC without the express permission of the giver. MAMC holds and is responsible for three types of data: • Personal – related to identifiable individuals – employee, volunteer and trustee details; • Sensitive – restricted to our employees but also equal opportunities monitoring data from job applicants; • Organisational – although information about organisations is not covered by the data protection act 1998, some organisational data can be considers personal where the contact details are an individual's home address.

	Details of all these data types and the procedures in place to protect them are in the document Guidelines for data procedures at MAMC. MAMC operates with CCTV inside and outside partnership house. It is being used in line with the "CCTV code of practice – revised edition 2008". The general principles are: a. There are signs displacing information that CCTV is in operation. b. Access to the CCTV saved images is stored securely (with password protection) as are copies are made of them. c. The CCTV saved images are viewed in a secure office.
5. Operational Practice	5.1 MAMC keeps extensive record systems, using paper files and computers. Where necessary, personal details of MAMC staff and users of a MAMC service are recorded in these systems. 5.2 Each staff member and individual user of MAMC services has the right to see any information that MAMC keeps on them in paper or computer files and to change that information where it is inaccurate if mutually agreed. If the recorded information is disputed between MAMC and a staff member/ individual user the data subject (see note 1) can have their view added to the records. Information that has been provided by a third party may be removed from a file prior to its examination. 5.3 MAMC will maintain an appropriate level of security, in accordance with the data protection act and this policy that will adequately protect information about individuals that is held in the systems. Paper files will be kept in a locked area and computer files will be password protected. 5.4 The use of information for reports, service development and funding applications will scrupulously avoid any specific detail about service user that might lead to their identification. The data provided by MAMC should not include information that could easily lead to the identification of service users. 5.5 Constructive liaison with other local agencies is sometimes essential if individuals and groups are to be offered an effective service by MAMC. However, users of MAMC's service must have given their permission before any information that is held by the MAMC about them can be passed on to a third party where that information specifically identifies them or might lead to their identification. 5.6 MAMC will not hold personal data on individuals without their knowledge and consent. 5.7 MAMC will only hold data for specified purpose and will inform data subjects what the purposes are. However, it will be clear condition of membership of MAMC that MAMC can decide what should happen to organisational data supplied (this does not include details of individuals within the organisation). 5.8 Data will be retained once it is no longer required for the specific purpose. 5.9 Compliance with data protection procedures has been designated a task in the PA to the Chief Executive at MAMC. 5.10 At the outset of any new project or type of activity the member of staff managing it will consult with the finance officer about any data protection implications. 5.11 In situations where MAMC works in partnership with other organisations on projects where data may be shared, MAMC will clarify who will be the data controller and will ensure that the data controller

	deals fairly with any data collected by MAMC. 5.12 All new staff induction will include full briefing on the data protection policy and procedures of MAMC. 5.13 Compliance with the data protection policy and procedures will be carried out and reviewed annually by the finance officer. 5.14 MAMC has notified the information commissioner of the data it holds and will ensure to renew this notification annually. A copy of the notification is kept by the finance officer and a copy is kept on our PQASSO evidence desk.
6. Disclosure	MAMC acknowledges that, on rare occasions, it may be necessary to break the basic rules of confidentiality. These may broadly defined as situations where the safety, rights and liberties of other people or the person giving information may be seriously at risk. Also, legal reports and reports requested by a funder may have to be made regardless of the consent of a service user. In such cases, staff should discuss the matter with their line manager and where necessary, the chief officer. Decisions that are made, and the reasons for them, must be properly recorded. When confidential information is divulged without consent, expect where it might result in more harm to other people, the individual concerned should be informed and an explanation of action given.
7.Sharing information within the MAMC	In order to give the best possible service to users of MAMC services, it is sometimes desirable to share information with other colleagues in the MAMC. Similarly, it is important that in supervision meetings, staff and volunteers should feel able to talk freely about their experiences. Information given to staff members or volunteers acting on behalf of MAMC is in these circumstances considered to be given to MAMC as an agency rather than to the individual staff member or volunteer. However, it should be absolutely clear to all attending such meetings that they are bound by the agency's rules of confidentiality and that confidential matters should not be discussed outside MAMC. Casual or social discussion about service users that is conducted amongst MAMC staff and outside MAMC premises is strictly prohibited.
8. Electronic Information	Internal Networks Each member of staff is responsible for securing (or limiting access to) documents and folders, which can be accessed via the internal network. On no account should confidential work be stored in shared folders. Personal folders should not be shared and confidential work should be password protected. Password details will be managed by the system administrator. Individual Workstations Workstations, which contain sensitive or confidential data should be password protected. Users should avoid disclosing passwords or security details to other staff, volunteers or external agents. It is advisable to change passwords every 4 months.
9. Data Protection	The data protection act 1998 requires organisations to register the information they hold about people, and what they do with it. It is the responsibility of the office manager (the Chief Executive) to ensure that this legal requirement is met MAMC Rochdale recognises that the data protection act now applies not only to computer systems but also to manual (paper) filing systems that are structured by reference to individuals (e.g. in a card index or filing

	systems) and CCTV. Where information relating to racial ethnic origin, political opinions, religious or other beliefs, trade union membership, health, sexuality, criminal proceedings and convictions are collected and processed, the individual concerned should give explicit consent, although there are some expectations under which the information can be collected without explicit consent. A significant exception is where information is being collected for the sole purpose of monitoring aimed at promoting equal opportunities. In such cases MAMC will inform the person about the purposes for which information will be used. MAMC will not use any information for the purpose of direct marketing (including fundraising) if the individual objects. In most cases this means informing people that the information may be used for direct marketing purposes, and giving them the opportunity to opt out.
10. Internet and e-mail	MAMC is aware of the various issues raised in relation to the disclosure of personal information via the internet and by email.
11. Email addresses	MAMC will not electronically store the email addresses of people making general enquiries. Only regular contacts should be stored in email address books and consent should be sought prior to any group postings. Staff should treat personal email addresses in the same manner as private telephone numbers. Where individuals or organisations subscribe anonymously to email network systems, an acceptance confirmation should be posted to the subscription address. MAMC staff should use standard signatures, which refer to confidentiality when posting email externally. Standard signatures are outlined in the MAMC ITC policy.
12.Website	MAMC does not use "cookies" in order to identify or market to specific users of our internet service. Any online information collected will only be used of our internet service. Any online information collected will only be used for statistical analyses as an aggregate. If personal information is sought directly then details of privacy will be published online and will include details of the processing related to the collection, registration, preparation, storage or destruction of that information.
13. Management Committee Members	The Management Committee Members of MAMC adhere to this policy, in addition Committee Members adhere to additional codes of conduct which relate specifically to their duties.

Date of first implementation: 9th April 2009
Date for next review: 8th December 2011
Date for next review: 6th December 2012
Date for next review: 18th September 2013
Date for next review: 21st October 2014
Date for next review: 26th November 2015
Date for next review: 3rd July 2016

Signed (Chair): _____ Dated: _____