MAPIS DATA PROTECTION POLICY

The following sets out the data protection policy for Mapis CIC. The Policy will be reviewed every year by the Board of Directors, sooner if legislation, best practice or other circumstances indicate this is necessary.

Data Protection Principles

As data controller, MAPIS CIC is required to comply with the principles of good information handling.

These principles require the Data Controller to:

1. Process personal data **fairly**, **lawfully and in a transparent manner.**
2. Obtain personal data only for one or more **specified** and **lawful purposes** and to ensure that such data is not processed in a manner that is incompatible with the purpose or purposes for which it was obtained.
3. Ensure that personal data is **adequate**, **relevant and not excessive** for the purpose or purposes for which it is held.
4. Ensure that personal data is **accurate** and, where necessary, **kept up-to-date.**
5. Ensure that personal data is not kept for any longer than is necessary for the purpose for which it was obtained.
6. Ensure that personal data is kept secure.
7. Ensure that personal data is not transferred to a country outside the European Economic Area unless the country to which it is sent ensures an adequate level of protection for the rights (in relation to the information) of the individuals to whom the personal data relates.

Consent

MAPIS CIC must record service users' explicit consent to storing certain information (known as 'personal data' or 'special categories of personal data') on file.

For the purposes of the Regulations, personal and special categories of personal data covers information relating to: ethnic origin, political opinions, religious beliefs, mental health or condition, sexual life, criminal offences, name and contact details, and genetic and/or biometric data of the service users'.

Special categories of personal information collected by MAPIS CIC will, in the main, relate to service users' physical and mental health. Data is also collected on ethnicity and held confidentially for statistical purposes.

Consent is not required to store information that is not classed as special category of personal data as long as only accurate data that is necessary for a service to be provided is recorded.

As a general rule MAPIS CIC will always seek consent where personal or special categories of personal information is to be held.

It should also be noted that where it is not reasonable to obtain consent at the time data is first recorded and the case remains open, retrospective consent should be sought at the earliest appropriate opportunity.

If personal and/or special categories of personal data need to be recorded for the purpose of service provision and the service user refuses consent, the case should be referred to the Managing Director for advice.

Obtaining Consent

Consent may be obtained in a number of ways depending on the nature of the interview, and consent must be recorded on or maintained with the case records:

1. face-to-face
2. written
3. telephone
4. email

Preliminary verbal consent should be sought at point of initial contact as personal and/or special categories of personal data will need to be recorded either in an email or on a computerised record. The verbal consent is to be recorded in the appropriate fields on the computer record or stated in the email for future reference. Although written consent is the optimum, verbal consent is the minimum requirement.

Specific consent for use of any photographs and/or videos taken should be obtained in writing. Such media could be used for, but not limited to, publicity material, press releases, social media, and website. Consent should also indicate whether agreement has been given to their name being published in any associated publicity. If the subject is less than 18 years of age then parental/guardian consent should be sought.

Individuals have a right to withdraw consent at any time. If this affects the provision of a service(s) by MAPIS CIC then the Project Co-ordinator should discuss with the Managing Director at the earliest opportunity.

Ensuring the Security of Personal Information

Unlawful Disclosure of Personal Information:

1. It is an offence to disclose personal information 'knowingly and recklessly' to third parties.
2. It is a condition of receiving a service that all service users for whom we hold personal details sign a consent form allowing us to hold such information.
3. Service users may also consent for us to share personal or special categories of personal information with other helping agencies on a need to know basis.
4. A client's and/or beneficiary's individual consent to share information should always be checked before disclosing personal information to another agency.
5. Where such consent does not exist information may only be disclosed if it is in connection with criminal proceedings or in order to prevent substantial risk to the individual concerned. In either case permission of the Managing Director should first be sought.
6. Personal information should only be communicated within MAPIS CIC's staff and volunteer team on a strict need to know basis. Care should be taken that conversations containing personal or special categories of personal information may not be overheard by people who should not have access to such information.

Ethnic Monitoring

In order for MAPIS CIC to monitor how well our staff, volunteers and service users reflect the diversity of the local community we request that they complete an Equality and Diversity Monitoring form. The completion of the form is voluntary, although strongly encouraged. Responses are securely stored and held on a password-protected database for statistical purposes.

Use of Files, Books, and Paper Records

In order to prevent unauthorised access or accidental loss or damage to personal information, it is important that care is taken to protect personal data. Paper records should be kept in locked

cabinets/drawers overnight and care should be taken that personal and special categories of personal information is not left unattended and in clear view during the working day. If your work involves you having personal and/or special categories of personal data at home or in your car, the same care needs to be taken.

Disposal of Scrap Paper, Printing, or Photocopying Overruns

Be aware that names/addresses/phone numbers and other information written on scrap paper are also considered to be confidential. Please do not keep or use any scrap paper that contains personal information but ensure that it is shredded.

If you are transferring papers from your home, or your client's and/ or beneficiary's home, to the office for shredding this should be done as soon as possible and not left in a car for a period of time. When transporting documents, they should be carried out of sight in the boot of your car.

Computers

Where computers are networked, access to personal and special categories of personal information is restricted by password to authorised personnel only.

Computer monitors in the reception area, or other public areas, should be positioned in such a way so that passers-by cannot see what is being displayed. If this is not possible then privacy screens should be used on the monitor to afford this level of protection. If working in a public area, e.g. reception, you should lock your computer when leaving it unattended.

Firewalls and virus protection to be employed at all times to reduce the possibility of hackers accessing our system and thereby obtaining access to confidential records.

Documents should only be stored on the server or cloud-based systems and not on individual computers.

Where computers or other mobile devices are taken for use off the premises the device must be password protected.

Direct Marketing

Direct Marketing is a communication that seeks to elicit a measurable fundraising response (such as a donation, a visit to a website, sign up to Gift Aid, etc.). The communication may be in any of a variety of formats including mail, telemarketing and email. The responses should be recorded to inform the next communication. MAPIS CIC will not share or sell its database(s) with outside organisations.

MAPIS CIC holds information on our staff, volunteers, clients, beneficiaries and other supporters, to whom we will from time to time send copies of our newsletters, magazine and details of other activities that may be of interest to them. We recognise that clients, beneficiaries, staff, volunteers and supporters for whom we hold records have the right to unsubscribe from our mailing lists. Clients, beneficiaries, staff, volunteers, and supporters whom receive our newsletter will have the chance to unsubscribe from our mailing list should they wish to do so. This wish will be recorded on their records and will be excluded from future contacts

Specific consent to contact will be sought from our staff, clients and other supporters, including which formats they prefer (e.g. mail, email, phone etc) before making any communications.

The following statement is to be included on any forms used to obtain personal data:

We promise never to share or sell your information to other organisations or businesses and you can opt out of our communications at any time by telephoning 01344 203007, writing to MAPIS CIC, First

Floor, c/o Involve, The Court House, Broadway, Town Square, Bracknell, Berkshire RG12 1AE or by sending an email to admin@mapis.org.uk.

Privacy Statements

Any documentation which gathers personal and/or special categories of personal data should contain the following Privacy Statement information:

1. Explain who we are
2. What we will do with their data
3. Who we will share it with
4. Consent for marketing notice
5. How long we will keep it for
6. That their data will be treated securely
7. How to opt out
8. Where they can find a copy of the full notice

Personnel Records

The Regulations apply equally to volunteer and staff records. MAPIS CIC may at times record special categories of personal data with the volunteer's consent or as part of a staff member's contract of employment.

For staff and volunteers who are regularly involved with vulnerable adults, it will be necessary for MAPIS CIC to apply to the Disclosure & Barring Service to request a disclosure of spent and unspent convictions, as well as cautions, reprimands and final warnings held on the police national computer. Any information obtained will be dealt with under the strict terms of the DBS Code. Access to the disclosure reports is limited to the Senior Management Team. If there is a positive disclosure the Chief Executive will discuss this, anonymously, with the Chair of the Standards Committee and our insurers to assess the risk of appointment. Trustees and insurers should not see the report itself.

Confidentiality

Further guidance regarding confidentiality issues can be found in our Confidentiality Policy.

When working from home, or from some other off-site location, all data protection and confidentiality principles still apply. All computer data, e.g. documents and programmes related to work for MAPIS CIC should not be stored on any external hard disk or on a personal computer. If documents need to be worked on at a non-networked computer they should be saved onto a USB drive which should be password protected.

Workstations in areas accessible to the public, e.g. reception or trading office, should operate a clear desk practice so that any paperwork, including paper diaries, containing personal and/or special categories of personal data is not left out on the desk where passers-by could see it.

When sending emails to outside organisations, e.g. social worker or hospital staff, care should be taken to ensure that any identifying data is removed and that codes (e.g. initials or identifying code number, such as social services number, etc.) are to be used. Confidential and/or special categories of personal information should be written in a separate document which should be password protected before sending. Wherever possible, this document should be 'watermarked' confidential.

Any paperwork kept away from the office (e.g. learner's care plan kept at home by a worker) should be treated as confidential and kept securely as if it were held in the office. Documents should not be kept in open view (e.g. on a desktop) but kept in a file in a drawer or filing cabinet as examples, the optimum being a locked cabinet but safely out of sight is a minimum requirement. Enablers needing

to take paperwork away from a learner's home (eg unable to make a required phone call during the visit) must ensure that it is returned to the learner's home on the next visit.

If you are carrying documents relating to a number of clients when on a series of home visits, you should keep the documents for other clients locked out of sight in the boot of the car (not on the front seat) and not take them into the clients' home. When carrying paper files or documents they should be in a locked briefcase or in a folder or bag which can be securely closed or zipped up. The briefcase/folder/bag should contain MAPIS CIC's contact details. Never take more personal data with you than is necessary for the job in hand. Care should be taken to ensure that you leave a client's home with the correct number of documents and that you haven't inadvertently left something behind.

Retention of Records

Paper records should be retained for the following periods at the end of which they should be shredded:

1. Client records – 8 years after ceasing to be a client.
2. Staff records – 8 years after ceasing to be a member of staff.
3. Unsuccessful staff application forms – 8 years after vacancy closing date.
4. Volunteer records – 8 years after ceasing to be a volunteer.
5. Timesheets and other financial documents – 8 years.
6. Employer's liability insurance – 8 years.
7. Other documentation, e.g. clients care plan sent to a worker as briefing for a visit, should be destroyed as soon as it is no longer needed for the task in hand.

Archived records should clearly display the destruction date.

Computerised records e.g. Charitylog, to be anonymised 8 years after ceasing to have any services from us. (Anonymising will remove the personal and special categories of personal data but will not remove the statistical data.)

What to Do If There is a Breach

If you discover, or suspect, a data protection breach you should report this to your line manager who will review our systems, in conjunction with the Senior Management Team and/or Quality Assurance & Systems Manager, to prevent a reoccurrence. The QA & Systems Manager should be informed of the breach, action taken and outcomes to determine whether it needs to be reported to the Information Commissioner and also for reporting to the Board of Trustees. There is a time limit for reporting breaches to ICO so the QA & Systems Manager should be informed without delay.

Any deliberate or reckless breach of this Data Protection Policy by an employee or volunteer may result in disciplinary action which may result in dismissal.

The Rights of an Individual

Under the Regulations an individual has the following rights with regard to those who are processing his/her data:

1. Personal and special categories of personal data cannot be held without the individual's consent (however, the consequences of not holding it can be explained and a service withheld).
2. Data cannot be used for the purposes of direct marketing of any goods or services if the Data Subject has declined their consent to do so.
3. Individuals have a right to have their data erased and to prevent processing in specific circumstances:

- Where data is no longer necessary in relation to the purpose for which it was originally collected
- When an individual withdraws consent
- When an individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- Personal data was unlawfully processed

4. An individual has a right to restrict processing – where processing is restricted, Age UK Exeter is permitted to store the personal data but not further process it. Age UK Exeter can retain just enough information about the individual to ensure that the restriction is respected in the future.
5. An individual has a 'right to be forgotten'.

MAPIS CIC will not undertake direct telephone marketing activities under any circumstances.

Data Subjects can ask, in writing to the Managing Director, to see all personal data held on them, including e-mails and computer or paper files. The Data Processor (MAPIS CIC) must comply with such requests within 30 days of receipt of the written request.