

# Security & Confidentiality Policy

## *Policy and Procedures*

Security for Money Lifeline (ML) falls into three categories:

1. The management and protection of ML client, employee, volunteer & management team data, in order to carry out day to day operations and to comply with legal obligations
2. Confidentiality
3. Workplace safety

### **Data management and security**

Personal data relates to a living individual who can be identified from that data. Identification can be by the information alone or in conjunction with any other information in the data processor's possession or likely to come into such possession. The processing of personal data is governed by the General Data Protection Regulation (the "GDPR").

This policy describes how ML will collect, handle and store personal data in order to comply with its obligations under the GDPR and ML expects all volunteers/employees to manage ML data and confidential information in line with this policy.

Volunteers/employees must comply with the following rules for handling ML information and equipment:

- ML client data will be stored on the Community Money Advice case management software (Catalyst) and in paper files which will be organised logically in accordance with ML procedures to enable quick retrieval and reference
- E-mails with ongoing value which relate to a particular client will be printed out as a PDF and stored in that client's Client Files within Catalyst. Some older emails may still be held in clients' paper files
- When not required confidential papers and files should be kept in a locked cupboard or filing cabinet
- Files, copies of emails or printouts should not be left out where unauthorized people can see them
- ML electronic data not held on Catalyst will be backed-up regularly onto an external drive or disks
- Data will be securely destroyed when it is no longer needed or if the volunteer/employee/client requests the destruction of their data
- Computers holding ML volunteer, employee or client data will be password protected and advisers will use a password protected screen lock on the computer. Advisers must lock the computer they are using whenever they leave the office temporarily and must log out of Catalyst and close down the computer before they leave at the end of an advice session
- Desktops, laptops and any other ML owned equipment will be kept in a secure room/building (when unattended). Advisers must lock the office door whenever

the room is left, however briefly, with no adviser present. All filing cabinets and the office door will be locked at the end of each advice session

- Laptops and any other ML owned equipment will not be left unattended in any public place. All laptops and computers will be shut down when being transported away from a secure location. If left in a car, equipment must be out of sight and the vehicle locked. Equipment must not be left in a car overnight
- Failure to comply with these requirements leading to the loss of ML data or ML owned equipment could lead to management investigation and possible disciplinary action
- When a member of staff/volunteer leaves ML, all data, and all equipment belonging to ML, must be handed back to a member of the ML management team.

Under GDPR all ML clients are entitled to:

- Ask what information ML holds about them and why
- Be given paper copies of all documentation about them or their circumstances that they request
- Be informed how to ensure the information is up to date
- Ask how ML is meeting its GDPR obligations.
- Have the right to request their personal data is erased where it is no longer necessary for ML to retain such data
- Have the right to withdraw consent to the processing of their personal data at any time
- Have the right to complain to the Information Commissioner's Office (ICO) should they be unhappy as to the way their data is being used or processed

ICO contact details

Tel: 0303 123 1113

Webchat: <https://ico.org.uk/global/contact-us/>

An ML client can request to see a copy of ML's Privacy Notice and any data that ML holds about them by contacting their adviser. Proof of identity will need to be received prior to any information being released.

All ML clients will be given a copy of their agreed financial statement and offered copies of all paperwork generated in line with the Financial Conduct Authority regulations.

## **Confidentiality**

ML believes that principles of confidentiality must be integrated across all aspects of its services and management. We believe our clients deserve the right to confidentiality in order to protect their interests and preserve the debt advice service. Therefore, no information regarding a client will be given directly or indirectly to any third party external to the staff of the centre and CMA support staff without the client's prior consent.

The postal address, email address and contact telephone numbers of any centre staff are treated as confidential and will never be disclosed without express permission of the person involved. Personal information about a colleague within ML should not be discussed with other colleagues or people outside of ML and CMA support staff without permission of that colleague.

We recognise that all clients should be able to access our services in confidence and that no other person outside the centre staff and CMA support staff should ever know that they have used our service, without their consent in writing.

Clients need to feel secure in using the service in a confidential manner and therefore, where required, they will be afforded confidential interview space. We will also ensure that as far as possible, there is no inadvertent breach of confidentiality.

All advisers will ensure that where any action is agreed to be taken by ML on behalf of a client that the client will firstly sign an authorisation form which will be kept in the client's file. A scanned copy of any authorisation will be uploaded to their Client Files within Catalyst. All hard copy case records will be kept in a locked secure filing cabinet when not in use, as will all information relating to clients such as notebooks, correspondence, calculation sheets and any other source of information. All electronic records will be suitably password protected.

All advisers will check with clients what methods of contact are acceptable such as sending letters to their home address, phoning at home or work, email, text and personal visit, before any contact is made in these ways.

Statistics gathered to monitor the service for the purposes of identifying any policy issues and to support funding applications will be produced in anonymous form to prevent identification of individual users.

### **Necessary breaches of confidentiality**

ML acknowledges that on rare occasions it may be necessary to break the basic rules of confidentiality. These may broadly be 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 may have to be made regardless of the consent of the person involved, for example where staff become aware of risk to a child, risk to life or of potential terrorist activity. Decisions that are made, and the reasons for them, will be properly recorded.

If an adviser feels that confidentiality should be breached **the following steps must be taken:**

If the adviser is not also a trustee of ML:

- the adviser should raise the matter immediately with a trustee of ML who is also an adviser.
- the adviser must discuss with the trustee the issues involved in the case and explain why they feel confidentiality should be breached and what would be achieved by breaching confidentiality. The trustee should take a written note of the discussion.
- the trustee is responsible for discussing with the adviser what options are available in each set of circumstances.

If the adviser is also a trustee, or if an adviser raises the matter with a trustee, that trustee is responsible for making an initial decision on whether confidentiality should be breached. If they decide that confidentiality is to be breached then they should take the following steps:

- the trustee should contact another trustee and brief them on the full facts of the case, ensuring they do not breach confidentiality in doing so. The two trustees constitute a committee of the trustees who have delegated authority to make a decision on behalf of the trustees in accordance with article 7(i) of the ML trust deed.
- if the two trustees decide to breach confidentiality, they should make a full written report on the case and any action agreed to be undertaken. The trustees may authorize one of the advisers to carry out some or all of the agreed action but one of those trustees should take responsibility for ensuring that all the agreed action is carried out.

- if the two trustees decide not to breach confidentiality then this is the final decision of ML.
- whatever the two trustees decide they should report their decision and subsequent actions to the next formal meeting of the trustees, in accordance with article 7(i), ensuring they do not breach confidentiality in doing so.
- the two trustees may informally consult other trustees before reaching a decision but there must always be at least one trustee with whom any breach of confidentiality is not discussed at this stage. This is to ensure that there is at least one trustee able to deal in an independent manner with any complaints or investigations arising from the proposed or actual breach in confidentiality.

When confidential information is divulged without consent the individual concerned will be, wherever possible, informed and an explanation of the action given, except where it might result in more harm to other people or when prohibited by law.

## **Complaints**

Any person, who feels that their confidentiality has been compromised, or who is concerned that inaccurate information is held about them, is encouraged to discuss the matter with a staff member. If the issue is not resolved to their satisfaction, they are entitled to make use of ML's published complaints procedure.

## **Data controller**

The person with overall responsibility for Data Processing within ML is David Evans.

His contact details are [mrdlevans@msn.com](mailto:mrdlevans@msn.com), 07970 165550.

David should be informed immediately of any breach of confidentiality or concern over data protection.

He is responsible for reviewing data protection procedures in line with ML's agreed schedule. The trustees of ML will review this policy annually. Any amendments should be proposed and agreed by the trustees.

David will arrange data protection training and advice for all ML staff.

## **ML safety**

ML aims to provide a safe environment for all clients, members of staff and volunteers. We also aim to properly manage any incidents that occur so as to minimise injury and other forms of loss. A well-managed workplace safety programme benefits our organisation and its people in countless ways.

David Evans with the rest of the management team will be responsible for developing and organising this program with input from ML staff.

David has drawn up a risk assessment based on the HSE example found at <https://www.hse.gov.uk/simple-health-safety/risk/risk-assessment-template-and-examples.htm> which will be reviewed in line with ML's agreed schedule.

ML is committed to ensuring the physical safety of staff and clients within the advice centre environment. However due to the stressful situations in which clients may find themselves ML staff may experience hostilities from clients such as physical and verbal assaults, threats, coercion and intimidation, which all constitute acts of violence.

In the event of an act of violence ML staff will:

- look to try and defuse the person's anger so that he/she can cool down and talk calmly and rationally
- maintain composure

- try to signal for help from another adviser who can contact management, security, the police or paramedics
- listen attentively. Hostile individuals who feel that they have your attention are sometimes less likely to act out physically
- maintain eye contact which should help to calm the person down because the individual feels that he/she has attention
- be courteous and patient until help arrives
- if the client has a weapon, follow his/her instructions and stall for time
- never try to intercept the weapon or act aggressively against the individual
- retain the right to terminate any advice/employment forthwith.

ML staff will talk to a member of the management team immediately if they observe unusual behaviour in others, feel intimidated or have any concerns. These concerns will be discussed and recorded in ML's incident book.