

Data Protection Policy

1 Legal requirements

1.1 Trinity Money Advice Leicester (“TMAL”) will comply with the Eight Principles of good practice that are set out in the Data Protection Act 1998. These principles are legally enforceable.

1.2 The Eight Principles state that TMAL must:

- Obtain and process the information fairly
- Keep it only for one or more specified and lawful purposes
- Process it only in ways compatible with the purposes for which it was given initially
- Keep it safe and secure
- Keep it accurate and up-to-date
- Ensure that it is adequate, relevant and not excessive
- Retain it no longer than is necessary for the specified purpose or purposes
- Give a copy of his/her personal data to any individual, on request.

1.3 The Data Protection Act 1998 provides conditions for the processing of any personal data. It also makes a distinction between personal data and “sensitive” personal data.

1.4 Personal data is defined as, data relating to a living individual who can be identified from:

- That data;
- That data and other information which is in the possession of, or is likely to come into the possession of the data controller and includes an expression of opinion about the individual and any indication of the intentions of the data controller, or any other person in respect of the individual.

1.5 Sensitive personal data is defined as personal data consisting of information as to:

- Racial or ethnic origin;
- Political opinion;
- Religious or other beliefs;
- Trade union membership;
- Physical or mental health or condition;
- Sexual life;
- Criminal proceedings or convictions.

2 Management and security of TMAL’s data

2.1 Volunteers must comply with the following rules for handling TMAL’s information and equipment:

- TMAL files and e-mails should be organised logically in folders for quick retrieval and reference



- TMAL data must be backed-up regularly (minimum monthly) onto an external hard drive or disks
 - Computers holding TMAL data must be password protected
 - Desktops, laptops and any other TMAL owned equipment must be kept in a secure room/building (when unattended)
 - Laptops and any other TMAL owned equipment must not be left unattended in any public place. If left in a car, equipment must be out of sight and the vehicle locked. Equipment must not be left in a car overnight.
- 2.2 Failure to comply with these requirements leading to the loss of TMAL data or TMAL owned equipment could lead to management investigation and possible disciplinary action.
- 2.3 When a volunteer leaves TMAL, all data, and all equipment belonging to TMAL, must be handed back to the TMAL Manager
- 2.4 In line with TMAL's Confidentiality Policy, data held by TMAL that has been provided by a client will not be passed to third parties without the client's prior written agreement.
- 2.5 Sanitised data in an anonymous format may be passed to other reputable debt advice organisations such as our affiliated body Community Money Advice and Advice UK for statistical purposes only. This includes data collected in line with TMAL's Equal Opportunities Policy.
- 2.6 Neither TMAL nor Holy Trinity Church will contact clients for any reason other than under its normal working arrangement to deal with debt or money advice issues, unless specifically requested by the client.

3 Management and security of volunteers' data

- 3.1 TMAL maintains strict confidentiality regarding a volunteer's specific working relations with TMAL and any personal circumstances that the volunteer has shared with TMAL.
- 3.2 TMAL expects all volunteers to likewise maintain confidentiality by:
- Not disclosing any TMAL information communicated by TMAL Management as confidential to a third party organisation without authorisation
 - Exercising discretion when discussing TMAL with third parties and ensuring TMAL is not brought into disrepute
 - Referring all approaches from the media concerning TMAL to the TMAL Manager

