Salford Dadz – Little Hulton

Confidentiality and Data Protection Policy

Document Control

Document Name:	Confidentiality and Data Protection Policy		
Date	7/4/2015	**Release:**	Draft
Author:	Steve Mortlock		
Owner:	Steve Mortlock		
Last Reviewed:	Never		
Document Number:	SD_CDP_001		

Note: This document is only valid on the day it was printed

Revision History

Date of next revision:

Revision Date	Prev Rev Date	Summary of Changes

Approvals

This document requires the following approvals. A signed copy should be filed.

Name	Signature	Title	Date of Issue	Version


Salford Dadz

Index

1. General Principles.

1.1 The organization, its officers, staff and volunteers will treat all personal information, however obtained, in line with the common law duty of confidence. In general, this means that any information about an individual given or received in confidence for one purpose may not be used for a different purpose or passed to anyone else without their explicit consent.

1.2 The organization will comply with all relevant legislation, and will operate in accordance with the principles of the Data Protection Act 1998 with regard to information about individuals which should be:

- fairly and lawfully processed
- processed only for specified and lawful purposes
- adequate, relevant and not excessive
- accurate and, where necessary, kept up-to-date
- not kept for longer than is necessary
- processed in line with the rights of the individual whom the information is about
- kept secure against unauthorized or unlawful use and against accidental loss, destruction or damage
- not transferred outside the European Economic Area unless the rights and freedoms of the person are adequately protected.

1.3 The organisation will notify the Information Commissioner, and data will be processed only within the organisation's notification, which must be kept up-to-date.

1.4 Broadly, "processing" includes obtaining, disclosing, recording, holding, using, erasing or destroying personal information.

1.5 Within their work, Directors, staff and volunteers might get or have access to personal information. They should treat all such information in the strictest confidence in accordance with this Policy.

1.6 The organisation may use such information (in aggregated and/or statistical form where possible) to plan, deliver and improve its work. Only those who need to know this information will have access to it.

1.7 Every individual about whom the organisation holds personal information should be fully informed about what information is held on them and the identity of the person who controls it. When the organisation records personal information, it should tell the individual to what uses it may be put and obtain their explicit consent for this.

2. Safeguarding information.

2.1 Any individual has the right under the Data Protection Act 1998 with regard to personal information held by the organisation about them:
(a) to take action to rectify, block, erase or destroy inaccurate information
(b) to prevent use likely to cause damage and distress
(c) to prevent use for the purposes of direct marketing
(d) to know the logic behind automated decision-making
(e) not to have significant decisions based solely on the results of automatic processing.

2.2 Ensuring the security and accuracy of information about individuals is the responsibility of all staff and volunteers.

2.3 The storage and disposal of all information about individuals (in whatever form) must protect confidentiality. To prevent any unauthorised access to such information, all staff and volunteers will:
(a) store it in secure, locked cabinets or containers
(b) when received, immediately give it to the relevant person or lock it away until they can give it to them, and
(c) when disposed, permanently destroy it by shredding or other effective means.

2.4 Security measures must be in place to protect computerised information. All staff and volunteers must make sure that:
(a) only they can access records on computer about individuals, and
(b) any work in progress about confidential matters is not left unattended and accessible on computer terminals.

2.5 All staff and volunteers should make sure that unintentional breaches of confidence do not occur by:
(a) not leaving work in progress on confidential matters unattended
(b) sending information about individuals only to secure sources, marked confidential
(c) double-checking for accuracy any transmission of information – including all contact numbers and addresses – against a reliable source before it is sent
(d) not holding conversations or interviews about confidential matters in situations where unauthorised persons may hear them (while ensuring the safety of themselves and others).

2.6 Where any agency or individual other than Directors, staff or volunteers is involved in carrying out the organisation's functions, they must confirm that they will act in accordance with this Policy.

3. Access to information about individuals.

3.1 Unless the law directs otherwise, only the individual concerned and appropriate staff will have access to information that:
(a) is about the individual, or
(b) might enable the individual to be identified or appear to be identified.

3.2 Such information will only be revealed to someone else if:
(i) the individual gives their explicit and informed consent (preferably written) to this for a particular purpose, or
(ii) on a "need to know" basis if the use of the information (anonymised where possible) can be justified for use in helping to deliver, plan and manage services effectively, or
(iii) the information is required by statue or court order, or
(iv) it can be justified for other reasons (usually for the protection of the public).

3.3 Only in exceptional circumstances, and where reasonable, will the organisation reveal information without the individual's consent. In such circumstances, the Chief Executive will be the only person with the authority to reveal such information. They will do this only after seeking appropriate advice (which is likely to include legal advice).

3.4 If there is any doubt about a person's right of access to information about an individual, this should be checked with the Chief Executive, who will get advice as appropriate. Similarly, if there is any doubt about a person's identity, this should be confirmed beyond doubt before they get access to any such records or information.

3.5 The organisation will communicate nothing to any other body or person without the individual concerned having clearly approved this.

4. Keeping individuals informed.

4.1 When the organisation holds personal information about an individual it will seek to ensure, so far as practicable, that the individual has, is provided with, or has made readily available to them:
(a) a description of what information is held about them and its source(s)
(b) a description of the purpose(s) for which the information is intended to be used
(c) the identity of the person responsible for the information

(d) the identity of any other person nominated as their representative
(e) a description of those to whom the information will or may be disclosed
(f) any further information which is necessary, given the specific circumstances, to enable use of the information to be fair
(g) notification of this Policy and how to get access to it.

4.2 This should be:
(i) done, where possible, before the individual is asked to give information
(ii) presented in forms understandable to the individual, and
(iii) where appropriate, available for general purposes as well as for individuals.

4.3 All information relating to an individual will be made available to them promptly on request, and in any case within 40 days. A fee may be charged within the statutory limits.