Merton Mencap

Information Technology, Personal Internet Presence & Social Networking

Policy

August 2017

Merton Mencap

Information Technology, Personal internet presence and social networking

Policy

This policy has been adopted by Merton Mencap through its Executive Committee which remains responsible for its review.

Original signed version is kept at the Merton Mencap office.

Signed: _____ Date: _____

Name: _____

Chair of Executive Committee

Signed: _____ Date: _____

Name: _____

Chief Executive

Record of adoption and review of this policy and procedure:-

Adopted: 28 February 2012
Reviewed: 11 March 2014
Reviewed: 2 December 2014
Reviewed: 14 August 2017

Merton Mencap

Information technology, Personal internet presence and social networking

Policy

1. Introduction

Merton Mencap provides relevant staff with resources and facilities to communicate electronically and access the internet, such as computers, tablets and mobile phones. This policy provides information to staff in relation to use of these resources and facilities, including Information technology.

Further, Merton Mencap recognises the popularity of the internet, including social networking and personal internet sites. All staff should be aware, however, that the internet is not a private or confidential system and that Merton Mencap has a legitimate interest in protecting the charity, its staff and service users from abuse or harm to reputation resulting from information published on the internet.

2. Definition

This policy applies to any activity on the internet, including personal internet sites, personal web pages and blogs, and social networking sites including Facebook, MySpace, Twitter and Web2.

This policy applies to all staff (employees, bank workers and volunteers, including Trustees). Breach of the provisions in this policy by staff may lead to disciplinary action which could include summary dismissal on the first occasion.

This policy should be read with reference to Merton Mencap' *Staff Code of Conduct* and the policies and procedures of *Safeguarding Adults at Risk*, *Safeguarding Children,* and *Data Protection, Confidentiality and Security of Information.* Reference should also be made to Merton Mencap's *Media Policy & Procedure*.

3. Policy statements and rules

- Staff must not access the internet for personal use during work time, which includes accessing web sites for holidays, gaming, dating, shopping or auctioning. In any case, staff must not use Merton Mencap resources or facilities to create, edit, access or disseminate pornographic, sexist, racist material or any other material likely to cause offence to anyone, or assist or support any illegal activity, via e-mail, internet or any other method.

- Under the provisions of the *Computer Misuse Act 1990*, unauthorised access to computers (hacking) is illegal and must never be undertaken by staff

- Staff must not store personally owned files such as music and photographs on Merton Mencap computers and its servers, unless permission has been obtained by a senior manager.

- Staff who make reference on the internet to their employment/volunteering with Merton Mencap must use the following disclaimer: "*The views contained in these web pages are my personal views and do not represent the views of Merton Mencap.*" **Staff should note, however, that this disclaimer does not exonerate them from their responsibility to adhere to all statements and rules in this policy.** Staff should not post the Merton Mencap logo or the charity's contact details on the internet.

- Staff should regard all information posted on the internet as being available to the public. This includes text and photographs. In this respect, staff should have no expectation of privacy in relation to information on the internet. The charity does not recognise any 'privacy setting' which renders any postings unreadable or restricted.

- Staff who publish details of their employment/volunteering with Merton Mencap, or when it can be reasonably worked out that staff are employed by/volunteer for Merton Mencap, should be aware that they are responsible for these details. Staff must advise the Chief Executive if they intend to make any reference to Merton Mencap on the internet.

- Staff must avoid posting any content on the internet which may bring the charity into disrepute. Staff must not comment on, criticise or abuse colleagues, suppliers, affiliates, partners or service users of Merton Mencap or their families. Staff are prohibited from using copyrighted materials, unfounded or derogatory statements, misrepresented material and should not name anyone in relation to Merton Mencap.

- Staff should not reveal any information confidential to Merton Mencap, a colleague or service user and their family. This includes data, personal data and sensitive personal data (also see *Merton Mencap's Data Protection, Confidentiality and Security of Information Policy & Procedure).*

- Staff receiving any press or media contact in relation to the information they have posted on the internet about Merton Mencap must advise the Chief Executive immediately.

- Official Merton Mencap presence on the internet, such as a web site or social media account, may only be set up and maintained with the permission of the Chief Executive

- The protection offered to 'whistleblowers' by the Merton Mencap *Whistleblowing Policy and Procedure* does not extend to protection from disciplinary action if staff publish a whistleblowing allegation on the internet.

- If staff are in any doubt as to whether they should publish content on the internet, they should consult the Chief Executive.

Audit Guidance

No audit guidance provided for the policy document. However, the charity reserves the right to access the social media accounts of staff and volunteers to ensure the provisions in this policy are being adhered to.
