Volunteers: Data Protection , Acceptable use of Information, Communications and Technology (ICT) Policy

Version Number	2
Date of Equality Impact Assessment	17/12/15
Date approved by HWWB Board	
Author	Jo Karasinski
Date Implemented	
Last revised	03/04/18
Next revision due	03/04/19
Volunteer Training delivered	As per Volunteer training timetable

The policy on the HWWB website is the only policy that is updated. Please note that it is the individual HWWB staff, board member or volunteer to ensure that they are reading the most current version of this policy. This can be done by checking the version number shown above against the version number of the policy filed here: www.healthwatchwestberks.org.uk

If required this policy can be supplied in different formats
Tel: 01635 886 210 or email: contact@healthwatchwestberks.org.uk

All personal data collected in relation to this policy will be held in accordance with Data Protection Legislation.

Responsibilities

1 HWWB Board

Have overall responsibility for volunteers within HWWB

2 HWWB Chief Executive Officer (CO)

HWWB Board have delegated to the HWWB CO the responsibility for developing policies and procedures for volunteering at HWWB and to ensure these are implemented effectively.

3 HWWB Staff and volunteers

All HWWB staff and volunteers are required to read and implement the volunteer policies and procedures. /

Volunteers: Acceptable Use of ICT Policy

1. Purpose

The information contained within this policy is designed to ensure that Healthwatch West Berkshire's (HWWB) ICT (Information and Communications Technology) equipment is used effectively, safely, and legally and to further the aims of the organisation.

HWWB recognises that the internet and the use of email and other electronic communications tools are crucial to conducting its business in an efficient way and for supporting its values, such as advancing knowledge, developing potential, developing business and promoting quality of life.

However, the use of IT resources raises a number of legal issues including confidentiality, data protection, copyright and harassment. Whilst recognising that volunteers only rarely use the HWWB IT facilities there are risks attached to using these resources, volunteers have an obligation to comply with current legislation and to reduce these risks by using resources sensibly and appropriately. Advice contained within this policy is also relevant to safe usage of personal computers

2. Communicating the policy

The policy will be communicated to board members and volunteers via the Volunteer induction training and through provision of timely updates whenever the policy is amended.

3. Misuse of IT equipment

- failure to comply with the appropriate use of IT resources may disrupt other legitimate IT uses and could lead to loss of business or cause HWWB's reputation to be damaged. In addition, use of IT resources in breach of the organisation's policy may expose HWWB to legal liability
- volunteers found using IT resources in breach of this policy will be subject to action as described with HWWB's Volunteer - Code of Conduct. In situations where there is a reasonable belief that illegal activity has occurred, this activity may also be reported to the police

4. Personal use of equipment

- HWWB permits volunteers reasonable, limited personal use of its equipment whilst within the HWWB offices. 'Reasonable' use of equipment, including internet access, specifically excludes the use of systems by an individual to conduct his or her private business affairs.

- 'Reasonable' personal use of email is defined as the occasional sending and receiving of emails to and from private individuals not connected with the business purposes of HWWB. This specifically disallows private emails containing confidential information, and defamatory or abusive emails.
- 'Reasonable' personal internet use is defined as occasional access to external websites not specifically related to HWWB's business purposes.
- 'Reasonable' personal use of the telephone is defined as making occasional brief local/national calls which are non-work related.

5. Internet use

- the internet is a largely unregulated space and poses a number of risks for individuals and organisations. HWWB has a duty of care to protect volunteers from being exposed to some of these threats. Web filtering software is used to eliminate as much offensive material as possible. However, board members and volunteers should remain vigilant and not attempt to access illicit material if they come across it on the internet. This includes sites which contain obscene, pornographic, hateful, racist, or other objectionable content
- users of HWWB internet facilities must not use it to send offensive, defamatory or harassing material to other users
- volunteers must not use HWWB computers to perpetrate any form of fraud, or software, film or music piracy not to introduce any form of malicious software into the corporate network.
- the current web filtering software uses a traffic light approach to identify legitimate sites. A green tick against the item indicates that the page is compliant with the web filtering policy. An orange question mark denotes a site which has not yet been classified by the web filter and should be treated with caution. A red cross is displayed against items which violate the filtering policy; this also shows the category against which the page has been prohibited
- volunteers using HWWB internet access should be aware that all internet access is logged automatically in system log files. While these are not actively monitored, details from the log files can be used if active monitoring is carried out when an employee is suspected of a serious breach of the acceptable use policy. See the section on 'Monitoring' below for further details.

6. Email use

Email is perhaps the most prevalent communication method in the modern office. Its ease of use sometimes obscures the pitfalls which may result from its misuse. Email should be treated in the same way as any other form of written communication and volunteers should give it the same due care and attention with regard to content and presentation.

The following is a list of key Dos and Don'ts around email usage:

DO

- ensure all emails sent to external recipients clearly identify the sender, including full name, organisation and contact details. All emails sent to external recipients have a standard disclaimer text automatically attached to the bottom of the message.
- Inform the sender immediately and delete the message if you receive an email in error from an external recipient.
- exercise care with cc messages. Before sending a reply to the original message, consider who is on the recipient list. Confidential information could potentially be disclosed to the wrong person by automatically including all of the original recipients in the reply.
- when communicating by email, no unauthorized person should indicate, either openly or obliquely, that they are entering into a binding agreement/contract, without the expressed permission of the CEO.
- if sending an email to group of people, consider the use of the BCC method of copying them in on the email. In this way the recipients of the email will be not be able to see the email addresses of the other persons to whom it has been addressed. In such cases, consider inserting the 'enquires' email address as the main recipient and BCC the remainder.

DON'T

- open anything which appears suspicious; it may contain a virus or other malicious code – if in doubt, delete the message. This applies in particular to messages received from unknown third parties.
- make obscene or defamatory or otherwise offensive remarks about another person or company over email, even where distribution is restricted to the organisation, or forward such emails received to other addresses. Remarks of this nature may be construed as harassment.
- forget that e-mail messages sent to external recipients via the internet are not secure. Sensitive or commercially valuable information should not be sent via unencrypted email. If complete confidentiality is required, confidential information must not be sent by email over the internet.

7. Social media

Healthwatch West Berkshire corporate social media use

- social media tools (Facebook, Twitter, blogs, wikis, etc) play an increasingly important part in engaging with our members online. They can bring the organisation much closer to its supporters and can provide instant feedback on issues which affect people
- however, by their very nature, these tools pose real security and reputational risks if they are not used in an appropriate way. Many of the caveats above regarding internet and email usage, such as avoiding defamatory or offensive remarks, apply equally to social media, which is essentially just another communications platform
- only authorised staff should post to HWWB's official social media accounts, such as Facebook and Twitter. Contributing staff should always be aware that they are representing the organisation and should adhere to the following basic rules: postings should not bring HWWB into disrepute, for example by criticising colleagues or suppliers, making defamatory comments about individuals or other organisations or groups, or by posting images, or links to images, that contain inappropriate content. confidentiality should be respected at all times; do not reveal confidential commercial or other information relating to HWWB or an individual working at the organisation, or discuss HWWB's internal workings or future plans which have not yet been communicated to the public.
- do not breach copyright by using copyrighted images or written content without permission or by failing to give acknowledgement where permission has been given to reproduce something.

Personal social media usage

It is also recognised that many people use social media sites, including personal websites, for personal purposes. However, HWWB must also ensure that confidentiality and its good reputation are protected.

Volunteers should follow these guidelines when using private social media:

- do ensure that you conduct yourself in a manner not detrimental to HWWB
- be aware that social networking websites are a public forum do not assume that postings on any social website will remain private.
- restrict the amount of personal information supplied to these sites to minimise the risk of identity theft. Social networking sites allow people to post detailed personal information such as date and place of birth, and their pet's name, information which can form the basis of security questions and passwords on other sites.
- do not use offensive or defamatory language on social media sites, or any language or behaviour that could be construed as harassment.
- do not post sensitive, confidential or corporate proprietary information on public forums, blogs or wikis.
- do not identify yourself as a volunteer for HWWB unless strictly necessary, for example when using networking sites such as LinkedIn which can support continuous professional development and achievement of business objectives.

- do not do anything on these sites which could damage the working relationships between members of staff and HWWB volunteers or the organisation itself
- do not download any software from social media sites, including plug-ins for games or other embedded features onto any office equipment.
- do not publish defamatory or knowingly false material about HWWB, colleagues or others on social networking sites, blogs, wikis or any online publishing format.

8. Data Protection

- the Data Protection Act 1998 places strict legal requirements on the use, storage and transmission of data concerning living individuals. All volunteers have a duty to ensure that they comply with the provisions of the Act. The Data Controller for HWWB is the CO Andrew Sharp
- All personal data stored electronically or manually is subject to the Act. All such databases must be registered with the register of data controllers maintained by the Information Commissioner's Office.
- If in any doubt on any aspect of data protection, staff should seek guidance from the Volunteer Lead.

9. Harassment/abuse

- IT users must not send or request indecent, sexist, obscene, racist or otherwise offensive material by email or harass, insult, threaten or intimidate colleagues or others by email or by any other electronic method. Users must not send unsolicited mail (whether offensive or otherwise) or send or solicit bulk mail, chain letters, jokes, games, etc, which may cause aggravation or distress, lead to lost productivity, or introduce problems into the IT system.

10. Malware

- 'Malware' covers a variety of malicious programs which are designed to gain unauthorised access to systems, disrupt or degrade a legitimate service, compromise a user's privacy, or otherwise harms the computer user.
- HWWB maintains up-to-date anti-virus scanning software. Nonetheless, it is the responsibility of IT users to exercise caution when opening emails received, especially where these are from unknown sources and/or contain attachments.

11. Security and passwords

- To safeguard the network against external threats, HWWB will implement regular password changes to maintain the integrity of the network access policy. Users must ensure that login and password details remain secure and

are not advertised anywhere near the PC, nor given to other users (other than to authorised staff for support purposes). Do not use obvious passwords such as your own name, the name of children or pets, etc.

- Users must log off from the network and switch off their computers before leaving the office at the end of the working day. During the day, users who are away from their desks should exercise caution when leaving their computers unattended, by closing down confidential documents and setting password-protected screensavers which run after a specified period of inactivity.

12. Monitoring

- HWWB reserves the right to monitor the use of IT resources and examine material stored on, transmitted through, or accessed from its facilities, and to carry out active monitoring if a user is suspected of serious violation of the acceptable use policy, in which case his or her right to privacy will be superseded by the organisation's requirement to safeguard its position.
- Where appropriate, HWWB will endeavour to inform an affected person of the reasons for monitoring and how monitoring will take place. In such circumstances, the CO of HWWB will authorise a proactive monitoring exercise, and will agree which areas (eg email usage, web surfing, telephone calls, etc.) need to be monitored. The monitoring will be undertaken by Indigo, under the strict guidance and control of the CO HWWB. Results of the monitoring will be reported back to the CO for further action if necessary.

Equality Impact Assessment Form

Screening determines whether the policy has any relevance for equality, i.e. is there any impact on one or more of the protected characteristics as defined by the Equality Act 2010. These are:

- Age
- Disability
- Gender Reassignment
- Marriage and Civil Partnership
- Pregnancy and Maternity
- Race
- Religion or belief Including lack of belief)
- Sex
- Sexual Orientation

1 Name of policy/procedure being assessed:	HWWB – Policies - Volunteers – Acceptable use of ICT Policy
2. Is this a new or existing policy/procedure?	New
3. What is the function of the policy/procedure?	To guide board members and volunteers on the procedures HWWB has in place to promote acceptable use of ICT
4. What is it trying to achieve and why?	Ensure volunteer understanding of acceptable ICT usage
5. Who is intended to benefit and how?	HWWB as an organisation. Board Members and Volunteers
6 Is there any potential for differential impact (negative or positive) on any of the protected characteristics?	No
7. Is there any possibility of discriminating unlawfully, directly or indirectly, against people from any protected characteristic?	No
8. Could there be an effect on relations between certain groups?	No
9. Does the policy explicitly involve or focus on a particular equalities group i.e. because they have particular needs?	No
Signed – **Signature: Jo Karasinski** **Name: JO KARASINSKI** **Position: Development Officer** **Date:17/12/15**	