VHA Policy Document

IT Security Policy

Reviewed: June 2021

Next Review Due: May 2024

1.Use of IT

Care should be taken to ensure that PCs and terminals are not visible except to authorised staff and board members and that passwords are kept confidential. Logged-In PCs should not be left unattended without logging out or using a password protected screen saver.

Staff and board members are not permitted to send attachments containing the personal details of customers or colleagues to external email addresses, unless we have formal data sharing arrangements with the recipient organisation. This includes a prohibition on sending personal details to staff and board members' own personal email accounts

All staff and board members will have encrypted memory sticks issued to them. Any VHA information required to be saved and taken externally should only be saved on such devices.

Any staff and board members leaving VHA will have their accounts disabled immediately.

Managers are not to access team members' email accounts except in cases of suspected fraud

1. Home / mobile working

When working from home, staff and board members should:

- Not save any VHA documents on personal computers or laptops, or on personal memory sticks

When mobile working, staff and board members should

- Work exclusively on the network, and not save documents to the hard drive of the computer they are using
- not store the login / password information with or on the laptop they relate to

2. Information and Communications Systems Policy

Our electronic communications systems and equipment are intended to promote effective communication and working practices within our organisation and are critical to the success of our business.

This deals mainly with the use (and misuse) of computer equipment, e-mail, the internet, telephones, tablets and voicemail, but it applies equally to the use of fax machines, copiers, scanners, CCTV, and electronic key fobs and cards. It outlines the standards we require users of these systems to observe, the circumstances in which we will monitor use of these systems and the action we will take in respect of breaches of these standards.

All staff and board members are expected to protect our electronic communications systems and equipment from unauthorised access and harm at all times. Failure to do so

may be dealt with under our Disciplinary Procedure and, in serious cases, may be treated as gross misconduct leading to summary dismissal.

3. **Equipment security and passwords**

Staff and board members are responsible for the security of the equipment allocated to or used by them and must not allow it to be used by anyone other than as permitted by this handbook.

If given access to the e-mail system or to the internet, staff and board members are responsible for the security of their terminals. If leaving a terminal unattended or on leaving the office they should ensure that they lock their terminal or log off to prevent unauthorised users accessing the system in their absence. Staff and board members without authorisation should only be allowed to use terminals under supervision.

Desktop PCs and cabling for telephones or computer equipment should not be moved or tampered with without first consulting the Association's IT consultants or the CE.

Passwords are unique to each user. Passwords must be kept confidential and must not be made available to anyone else unless authorised by the CE. For the avoidance of doubt, on the termination of employment (for any reason) staff and board members must provide details of their passwords to the CE and return any equipment, key fobs or cards.

Staff and board members who have been issued with a laptop, mobile phone or tablet must ensure that it is kept secure at all times, especially when travelling. Passwords must be used to secure access to data kept on such equipment to ensure that confidential data is protected in the event of loss or theft. Staff and board members should also be aware that when using equipment away from the workplace, documents may be read by third parties, for example, passengers on public transport.

4. **Systems and data security**

Staff and board members should not delete, destroy or modify existing systems, programs, information or data which could have the effect of harming our business or exposing it to risk.

Staff and board members should not download or install software from external sources without authorisation from the CE. This includes software programs, instant messaging programs, screensavers, photos, video clips and music files. Incoming files and data should always be virus-checked by the Association's IT consultants, or those within the organisation suitably qualified/experienced to do so, before being downloaded. If in doubt, staff and board members should seek advice from the aforementioned persons. The following must never be accessed from the network: online radio, audio and video streaming, instant messaging and webmail (such as Hotmail or Yahoo) and social networking sites (such as Facebook, YouTube, Twitter). This list may be modified from time to time.

No device or equipment should be attached to our systems without the prior approval of the IT department. This includes any USB flash drive, MP3 or similar device, PDA or telephone. It also includes use of the USB port, infra-red connection port or any other port.

We monitor all e-mails passing through our system for viruses. Workers should exercise caution when opening e-mails from unknown external sources or where, for any reason, an e-mail appears suspicious (for example, if its name ends in .exe). The IT consultants and CE should be informed immediately if a suspected virus is received. We reserve the right to block access to attachments to e-mails for the purpose of effective use of the system and for compliance with this part of our handbook. We also reserve the right not to transmit any e-mail message.

Staff and board members should not attempt to gain access to restricted areas of the network, or to any password-protected information, unless specifically authorised.

Staff and board members using laptops or wi-fi enabled equipment must be particularly vigilant about its use outside the office and take any precautions required by the IT consultants or the CE from time to time against importing viruses or compromising the security of the system. The system contains information which is confidential to our business and/or which is subject to data protection legislation. Such information must be treated with extreme care and in accordance with our Data Protection Policy.

5. **E-mail etiquette and content**

E-mail is a vital business tool, but an informal means of communication, and should be used with great care and discipline. Staff and board members should always consider if e-mail is the appropriate means for a particular communication and correspondence sent by e-mail should be written as professionally as a letter or fax. Messages should be concise and directed only to relevant individuals.

Staff and board members should not send abusive, obscene, discriminatory, racist, harassing, derogatory or defamatory e-mails. Anyone who feels that they have been harassed or bullied or are offended by material received from a colleague via e-mail should inform their manager or the CE.

Staff and board members should take care with the content of e-mail messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract. Staff and board members should assume that e-mail messages may be read by others and not include anything which would offend or embarrass any reader, or themselves, if it found its way into the public domain.

E-mail messages may be disclosed in legal proceedings in the same way as paper documents. Deletion from a user's inbox or archives does not mean that an e-mail cannot

be recovered for the purposes of disclosure. All e-mail messages should be treated as potentially retrievable, either from the main server or using specialist software.

In general, staff and board members should not:

- send or forward private e-mails at work which they would not want a third party to read;
- send or forward chain mail, junk mail, cartoons, jokes or gossip;
- contribute to system congestion by sending trivial messages or unnecessarily copying or forwarding e-mails to those who do not have a real need to receive them;
- sell or advertise using our communication systems or broadcast messages about lost property, sponsorship or charitable appeals;
- agree to terms, enter into contractual commitments or make representations by e-mail unless appropriate authority has been obtained. A name typed at the end of an e-mail is a signature in the same way as a name written at the end of a letter;
- download or e-mail text, music and other content on the internet subject to copyright protection, unless it is clear that the owner of such works allows this;
- send messages from another worker's computer or under an assumed name unless specifically authorised; or
- send confidential messages via e-mail or the internet, or by other means of external communication which are known not to be secure.

Staff and board members who receive a wrongly-delivered e-mail should return it to the sender. If the e-mail contains confidential information or inappropriate material (as described above) it should not be disclosed or used in any way.

6. **Use of the internet**

When a website is visited, devices such as cookies, tags or web beacons may be employed to enable the site owner to identify and monitor visitors. Such a marker could be a source of embarrassment to the visitor and us, especially if inappropriate material has been accessed, downloaded, stored or forwarded from the website. Such actions may also, in certain circumstances, amount to a criminal offence if, for example, the material is pornographic in nature.

Staff and board members should therefore not access any web page or any files (whether documents, images or other) downloaded from the internet which could, in any way, be regarded as illegal, offensive, in bad taste or immoral. While content may be legal in the UK, it may be in sufficient bad taste to fall within this prohibition. As a general rule, if any person (whether intended to view the page or not) might be offended by the contents of a page, or if the fact that our software has accessed the page or file might be a source of embarrassment if made public, then viewing it will be a breach of our Information and Communications Systems Policy.

Staff and board members should not under any circumstances use our systems to participate in any internet chat room, post messages on any internet message board or set up or log text or information on a blog or wiki, even in their own time.

7. **Personal use of systems**

We permit the incidental use of internet, e-mail and telephone systems to send personal e-mail, browse the internet and make personal telephone calls subject to certain conditions set out below. Personal use is a privilege and not a right. It must be neither abused nor overused and we reserve the right to withdraw our permission at any time.

The following conditions must be met for personal usage to continue:

- use must be minimal and take place substantially out of normal working hours (that is, during lunch hours, before 9 am or after 5.00 pm);
- personal e-mails must be labelled "personal" in the subject header;
- use must not interfere with business or office commitments;
- use must not commit us to any marginal costs; and
- use must comply with the policies set out in this handbook including the Equal Opportunities Policy, Anti-harassment Policy, Data Protection Policy and Disciplinary Procedure.

Staff and board members should be aware that personal use of our systems may be monitored and, where breaches are found, action may be taken under the disciplinary procedure. We reserve the right to restrict or prevent access to certain telephone numbers or internet sites if we consider personal use to be excessive.