Vectis Housing

VHA Policy Document

Information and Communication Systems Policy

Reviewed: August 2024

Next Review Due: August 2027

Vectis Housing

Information and Communications Systems Policy – Board Members

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 policy deals with the use (and misuse) of computer equipment, e-mail, the internet, telephones, personal digital assistants (PDAs) and voicemail, but it also applies 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.

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 deemed a breach of the Code of Governance and dealt with as a disciplinary matter. In serious cases, this may be treated as gross misconduct requiring the individual concerned to stand down or be removed from the Board.

Equipment security and passwords

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 specifically authorised by this policy.

If given access to the e-mail system or to the internet, Board members are responsible for the security of their equipment.

Passwords are unique to each user and must be changed regularly to ensure confidentiality. 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 standing down from the Board (for any reason) members must provide details of their passwords to the CE and return any equipment, key fobs or cards.

Board members must ensure that mobile handsets are 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.

Systems and data security

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.

Board members should not download or install software from external sources onto equipment provided for the purpose of accessing VHA data 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 should seek advice from the aforementioned persons.

The following should not be accessed using the VHA 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. Board members 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 .ex). 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.

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.

E-mail etiquette and content

Board members will be provided with an exclusive VHA email address. E-mail is a vital business tool, but an informal means of communication, and should be used with great care and discipline. Under no circumstances should abusive, obscene, discriminatory, racist, harassing, derogatory or defamatory e-mails be sent. 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.

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. Unless properly encrypted or passworded, e-mail messages may be read by others and should 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, Board members using their VHA address should not:

- send or forward private e-mails that they would not want a third party to read;
- send or forward chain mail, junk mail, cartoons, jokes or gossip;
- 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 confidential messages via e-mail or the internet, or by other means of external communication which are known not to be secure.
- 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.

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.

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.

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.

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:

- 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 our policies relating to Equal Opportunities, Anti-harassment, Data Protection and Disciplinary Procedure.
- 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.