IT SECURITY POLICY
PROCEDURE AND GUIDANCE NOTES

Overview

The IT Security Policy confirms a set of principles for accessing and using Weaver Vale Housing Trust's IT systems, information and resources, and the measures required to protect the Trust's digital information and data assets from threats.

The IT Security Policy Procedure and Guidance Notes work in conjunction with the IT Security policy, all employees covered in the scope of the IT security policy will be expected to read and sign both documents. Acceptance of this policy is mandatory and breaches will be subject to investigation.

By signing this policy you are confirming that you understand the content of the policy and are agreeing to abide by the terms laid out within.

1.0 Internet Controls

1.1 All internet activity including that which is carried out on the trusts corporate wireless network is monitored to ensure compliance with this policy. Where necessary any inappropriate activity will be reported to line managers who will determine if the policy has been breached.

1.2 Occasional use of the Internet facility for personal use is accepted as long as it is not excessive or inappropriate and occurs during personal time and does not result in expense to the Trust.

1.3 The Trust will carry out reviews of internet activity looking for inappropriate internet usage by means of utilising the protective software reporting facility.

1.4 Employees may enter into transactions via the internet provided they pay for goods or services in advance i.e. by credit or debit card. By signing this agreement, employees accept full responsibility and liability for any goods purchased, and acknowledge that Weaver Vale Housing Trust shall not be held responsible for the costs of any such goods in any manner.

1.5 The Trust will not be liable for any loss of personal information as a result of a person entering in to any such agreement

1.6 Any requests to provide information from Internet logs will only be provided in line with HR guidelines.

2.0 Email Controls

2.1 Occasional use of the email facility for personal use is accepted as long as it is not excessive or inappropriate and occurs during personal time and does not result in expense to the Trust. Any enhanced use of the Email facility should be agreed with the person's line manager.

2.2 The Trust makes use of an email archive system, that stores and indexes every email sent to and from the Trusts email system. Upon request any email can be retrieved in line with HR guidelines.

2.3 All incoming and outgoing emails will be automatically scanned for viruses and other unsuitable content. Emails that are blocked are monitored and investigated where appropriate. Any request to have email unblocked must be directed to the IT Helpdesk, and such email will only be released after they have been security checked.

2.4 All emails (And or attachments) to be sent externally which contain personal sensitive data /information must be encrypted.

2.4.1 If you need to encrypt the contents of an email, there are two options:

- Send the information instead as an encrypted attachment, using MS Office 10.
- Ask the IT team to give you access to their temporary EGRESS license.

The full procedure for sending encrypted emails can be found in Appendix C, Section 7 Transfer of Data Information, of the Data Protection Policy Procedural Guidance Notes.

3.0 Virus Controls

3.1 All external storage media e.g. USB Memory sticks, or CD/DVD's, must be scanned by a member of the IT Team prior to use, to request a scan to be carried out on any devices please log a call via the IT helpdesk.

3.2 Anti-Virus software is to be installed on all PC's and will be subject to regular virus definition updates.

3.3 The Trusts antivirus system will be checked on a daily basis and all alerts will be investigated.

3.4 All servers will be regularly scanned for viruses. Virus definitions should be updated on all servers in line with updates to PC's.

3.5 All email attachments on inbound or outbound messages, are to be automatically scanned for viruses by the email scanning system prior to delivery to the intended recipient or recipients.

4.0 **Physical Access Controls & Responsibilities.**

4.1 Once logged in to the network, if a person leaves their work area they should protect their computer system by locking it e.g. by use of CTRL-ALT-DEL, or the Windows key and L.

4.2 It is your responsibility to ensure that your computer is secured and used in accordance with the IT Security policy.

4.3 The IT team will arrange to have external penetration testing performed on a regular basis of its internet facing controls, and internal network infrastructure and security.

4.4 The IT team will review the security configuration of the Trusts firewalls on an annual basis.

4.5 Access to secured areas will be restricted to named individuals this includes entry in to the Comms room, and access to the media safe stored remotely.

5.0 **System Access Controls**

5.1 Any additional rights/privileges within a system will be controlled and monitored where possible. Expiry dates for additional access rights should be obtained and monitored to ensure that additional access rights are not granted for longer than necessary.

5.2 Failing to act responsibly whether knowingly or unknowingly may result in your user account(s) being disabled without prior warning by members of the Trusts IT team.

5.3 Services and access to business critical applications will be managed in such a way as to deliver maximum continuity and availability, meeting the requirements of current KPIs and Service Level Agreements.

5.4 The IT manager will arrange for periodic reviews of security access rights for Trust employees.

6.0 **Preventing Unauthorised System Access.**

6.1 When a user no longer requires access to a system through a change in job role or responsibility, IT must be informed so that access rights to that system can be revoked.

6.2 Access to Information Systems will be monitored in order to identify potential misuse of systems.

6.3 Access to another person's resources i.e. home drive\mailbox must be requested by a member of the Leadership team or above, and where possible approval from the individual must also be obtained. If this is not possible, then HR must authorise the request.

6.4 Data on the Trusts network shall be secured against unauthorised access and against loss and corruption in line with Audit requirements.

7.0 **Preventing Unauthorised User and Computer Access**

7.1 All users will access systems via their own username. It is the responsibility of the user to ensure that their username and password details are kept secure.

7.2 Users will not disclose passwords to any other person or use another person's username and password or write them down.

7.3 The use of accounts shall be monitored where possible in order to identify any accounts that have not been used for 1 month, such accounts will be locked. If the account remains unused for a further 2 months, the account and associated user data e.g. emails, home drive etc. will be deleted unless requested otherwise.

7.4 The following security measures are in place for access to the Trusts data network. Where these can't be set that systems maximum password security settings will be used.

- Passwords should be changed every 45 days, and meet the requirements mentioned in the Password guide in appendix A

- A password history exists that prevents a password from being used that is the same as any one of the last 24.

- After 5 failed logon attempts to the domain, the users account will be locked, until unlocked by a member of the IT team.

- User accounts will be locked after a maximum of 5 unsuccessful login attempts on any system that allows this.

7.5 High level system passwords such as those used to administer a system will be recorded and kept in a secure location. Access to this location will be restricted to named and authorised users.

7.6 Users will not leave desktop PC\Terminal\Laptop equipment unattended whilst still logged on. The PC\Terminal\Laptop must be locked when not in use.

7.7 At the end of each day, all PC's\Terminal's\Laptop's must be completely shut down unless there is a valid business requirement.

8.0 **Authorised use of Computer Equipment**

8.1 Users will only have access to and the ability to run software they are authorised to run.

8.2 Software must only be installed on to a device by the IT team; any attempt to install unauthorised software will be considered a breach of the IT security policy and may result in disciplinary action.

8.3 Users will contact the IT helpdesk if in doubt over any actions relating to computer equipment and software.

8.4 Where possible, access to systems should be logged by the appropriate system

8.5 Where possible, access and event logs should be monitored regularly to investigate any anomalies.

9.0 **Protection of network services**

9.1 Physical access to network devices (servers, switches, hubs) is to be restricted to named, authorised personnel.

9.2 Accounts used by the Trusts support partners, will be disabled when not in use unless otherwise agreed by the IT Manager. Remote access to any systems will only be enabled when the identity of the requester has been identified, and the reason for remote access has been established and logged.

9.3 Access to the Trusts systems by 3rd parties must be agreed in either

- The support contract with the company
- The Trusts IT code of connection
- All access over public networks i.e. the internet, must be properly authenticated and encrypted.
- For VPN connections, idle sessions will be disconnected and cleared after 60 minutes.

10.0 **Telecommunications**

10.1 All telephone calls to and from the Trust are recorded, and upon request can be retrieved and replayed in line with HR guidelines. Once this policy is signed, you are accepting and acknowledging that these recordings are taking place and being used in line with the aforementioned HR guidelines.

10.2 Calls made from the Trusts telephone system are recorded for budgetary purposes. These reports contain details of dialled numbers and the cost to the Trust and anomalies are routinely investigated.

10.3 Access to call details and recording from all telecommunication equipment will be in accordance with the following procedure.

10.4 No requests for access to call recordings are to be actioned without the knowledge of the person whose calls were recorded, or where authorised by HR.

10.5 All requests will be first logged on the IT Helpdesk and HR will be informed.

10.6 Requests for access to recordings will only be considered when a member of the Leadership team or above have made the request.

10.7 Once recordings have been located, access to the recordings will be provided in a secure manner i.e. in the Comms room. No copies of recordings will be supplied\downloaded without confirmation from HR and potentially the Trusts Data Protection Officer (where appropriate.) This is to ensure the security of the recordings.

10.8 Cost monitoring is carried out on all trust issued mobile phones. All personal calls identified must be paid for, in-line with the current mobile phone billing procedure.

10.9 Calls and texts to premium rate numbers such as those associated with competition lines, racing lines, chat rooms etc. must be identified and paid for by the employee. Calls and texts to these types of numbers are very expensive and charges can also be made when receiving calls and messages. It is recommended that premium rate lines are not used at all in order to prevent high costs from being incurred.

10.10 Trust mobile telephones are provided primarily for business use in order for employees to carrying out official Trust business. Where Trust mobiles are used for personal calls it is expected that the personal usage will be reasonable in terms of time of usage and the volume of calls. All usage on Trust phones is monitored and excessive personal use of a mobile phone may be highlighted to the Employee and the Manager even if the calls are being repaid. Whilst there are several reasons for this it is also to try and prevent employees incurring excessive costs without being aware.

10.11 Transmission of any offensive material in in either voice text or image from Trust owned mobile device is strictly forbidden.

11 **Mobile Devices**

11.1 The Trust reserves the right to restrict the use of mobile devices if employees do not abide by this policy and the procedures outlined in the IT security policy procedure and guidance notes

11.2 Limited exceptions to the policy may occur where there is business need, however a risk assessment must be conducted by management and written approval provided in advance.

11.3 In order to connect mobile devices to the company network, devices must meet the following requirements:

- Devices must be configured with a secure password that complies with the Trust's password policy.
- Only devices managed by the IT team will be allowed to connect directly to the internal network, including the Trust's private wireless network.
- Devices will be subject to valid compliance rules on security features such as encryption, passwords, key lock (PIN), remote wipe etc. These policies will be enforced by the IT team using Mobile Device Management Software.
- Employees must report all lost or stolen devices to the Trust's IT team immediately.
- Jailbroken (IOS) or rooted (Android) mobile devices are strictly forbidden from accessing the company network.
- Devices must be kept up-to-date with manufacturer or network provided patches and software releases.
- Employees are responsible for the back-up of their personal data and the company will accept no responsibility for the loss of files due to a non-compliant device being wiped for security reasons.
- Employees must not use Trust PC's or Laptops to back-up or synchronise personal mobile device content, such as media files, unless such content is required for legitimate business purposes.
- The mobile device must lock itself if idle for five minutes and be reactivated with a password or PIN.

11.3 The IT team must give permission for the device to access the network and must be made aware of any new devices.

11.4 The employee is expected to use his or her mobile device in an ethical manner at all times and adhere to the company's IT Security Policy at all times.

11.5 In the event the IT team has to remotely wipe a device, all mobile data on the device will be lost, including personal data. It is the employee's responsibility to take additional precautions, such as backing up email, contacts, photographs, media files etc.

11.6 Actions which may result in a full or partial wipe of the device or other interaction by the IT team include but are not limited to the following:

- A device is found to be jailbroken/rooted.
- A device contains an app known to contain a security vulnerability (If not removed within the given time-frame given by the IT team)
- A device is lost or stolen
- A user has exceeded the maximum number of failed password attempts.

11.7 The Trust reserves the right to disconnect mobile devices or disable services without prior notice.

11.8 Lost or stolen Trust issued devices must be reported to the IT team immediately, employees are responsible for notifying their mobile carrier upon loss of a personal mobile device.

11.9 The employee is personally liable for all costs associated with his or her mobile device of a personal nature.

11.10 If an employee suspects that unauthorised access to company data has taken place via a mobile device, they must report the incident to the IT team immediately.

12 **Removable Media Policy**

12.1 The Trust will ensure controlled use of removable media devices to store and transfer information by all employees who have access to information systems and IT equipment, for the purpose of conducting official Trust business.

12.2 Trust policy is to discourage the use of removable media as far as reasonably practical, where there is no practicable alternative then removable media may only be used in compliance with the IT security policy.

12.3 All removable media will be automatically blocked by the Trusts Anti-Virus system.

12.4 Where there is a legitimate business requirement for the use of removable media, the request must be made by the employees line manager.

12.5 All such requests are recorded for audit purposes and reviewed annually.

12.6 Data stored on removable media must only be done so temporarily and removed at the earliest opportunity, Data should not be permanently held on removable media.

12.7 Before introducing removable media devices on to the Trusts network, they must first be scanned for viruses by the Trusts IT team.

12.8 Each employee is responsible for the appropriate use and security of data and for not allowing removable media devices and the information stored on the devices to be compromised in anyway whilst in their care or under their control.

12.9 Damaged or faulty removable media devices must not be used. It is the duty of all users to stop using removable media when it is damaged.

12.10 Removable media devices that are no longer required must be disposed of securely to avoid data leakage. Any previous contents of any reusable media must be erased.

12.11 Any Trust owned removable media devices that are no longer required must be returned to the IT team for secure disposal.

13 **Security of Data and Encryption**

13.1 Encryption technologies exist at the trust to provide a level of protection for the storage, transmittal retrieval and access to data.

13.2 The Trust uses two forms of encryption, email encryption and full disk encryption for Laptop PC's

13.3 Full disk encryption is installed on Trust owned Laptop PC's unless they have been identified as an exception. A documented list of exceptions is maintained by the IT team.

13.4 The IT team will ensure that any Laptop PC's provisioned for use by Trust employees are protected with appropriate encryption technology.

13.5 Information containing sensitive data that is sent outside of the Trusts network must be encrypted using the Trust's email encryption facility.

13.6 There are two methods of encrypting emails, guidance on how to do this can be found in the trusts Data Protection Policy Procedural Guidance Notes. Please refer to section 2.4 Email Controls of this document for more information.

13.7 It is the responsibility of the employee to have read and understood the requirements within the Data Protection and Information management procedure and guidance notes, specifically in relation to identifying email correspondence that requires encrypting.

Appendix A

Best practice for setting secure passwords.

- DO not use your login name or any variation of your login name.
- DO not use any part of your name, or the name of your spouse/partner/child(ren).
- DO not use any information that others can easily obtain, such as your car make or registration, telephone numbers or street name.
- DO not use a word that would be contained in a dictionary, as this makes the password easier to access. Combinations of words are more secure than single words.
- DO not use a password that you have set elsewhere e.g. online banking.
- DO use a password with mixed upper and lower case alphabetic characters.
- DO use a password that contains digits or non-alphanumeric characters such as punctuation marks.
- DO use a password that you will be able to remember, so that you don't need to write it down.
- DO use a password this is at least 8 characters long.

Passwords must never be written down or disclosed to others. This is a serious breach of information security, and this policy, which will be reported to the employee's line manager and HR immediately.

If someone else requires access to your resources, then a request must be made as per section 10 'Preventing unauthorised system Access.'

Where possible a different password should be used for each system that needs to be accessed.