IT Acceptable Use Policy

Jigsaw

Contents

1 Policy Aims

1. To ensure that everyone who uses Jigsaw Homes Group IT systems and equipment does so in a way that keeps data secure, and that uses technology for the purposes it was introduced.

2 Policy Scope

2. The scope of this policy extends to all departments, employees, contractors, vendors and partner agencies who use/access the Group's ICT facilities. Some partnership projects may have policies specific to their needs, which will need to be approved by the Director of Corporate Services. A separate document - the IT Security Policy - outlines the approaches applied by the Group's IT services to ensure its data is kept securely.

3. This policy has been updated to take account of altered working practices arising from the lockdown response to the Coronavirus pandemic. In particular, it addresses the following changes:

- Increased number of staff accessing the Group's network and applications working at home
- Increased number of staff logging onto the Group's network and applications on personal devices
- The introduction of MS Teams to promote collaboration of staff working in physical separation from each other.

3 Policy Statement

4. The Group is committed to ensuring that data held on its computer systems, devices and websites are kept securely and made available for us to do our jobs. IT security involves many steps managed by our IT and systems specialists. However, this policy directly addresses all employees and other users in achieving this aim.

5. The way users behave is critical to IT security. For example, the following actions can expose the organization to significant risk:

- failing to apply basic access controls such as password security
- losing mobile devices holding data
- transferring data to third parties without adequate controls
- visiting compromised websites or downloading unauthorized material from the internet can introduce viruses and malware to the Group's network.

6. To influence behaviour positively, the requirements of this policy will be communicated to staff using different media and approaches, as well as making this policy available on the network.

7. In addition to the protection of corporate data, this policy sets guidelines that protect IT assets and ensure the technologies in place are used appropriately.

8. Breaches of personal or confidential data, even if accidental, must be reported to the Data Protection Officer promptly (dpo@jigsawhomes.org.uk). Breaches of this policy may result in disciplinary action being taken against the user and may constitute gross misconduct, with self-reporting of breaches considered a mitigating factor.

3.1. IT Equipment Use

9. As an authorized user of the Group's network, you have been provided with a username and password. You must:

- Log-on using only that username and password
- Keep the password private - not sharing it with anyone or recording it in a way that someone else could find it.
- Set and update passwords that meet the Group's password standards (see appendix 1)

10. The Group makes available to users desktop devices such as PCs, thin-clients and laptops. As a user of a desktop device you must:

- Lock the screen before moving away from your work station or desk
- Log-off and power down the computer, switching off the monitor, when you finish work for your day/shift.
- Report to the IT Service Desk immediately any warnings visible on screen from the Group's Antivirus/Anti-malware software about identified/detected threats.

11. You must not:

- Move static desktop devices (i.e. PCs, winterms, 10zigs) to other locations without approval from the IT Service Desk.
- Plug-in or insert equipment, that has not been officially issued by the Group, into the desktop device
- Install software to a desktop device
- Tamper with (e.g. remove covers or unscrew fixings) or mishandle desktop devices.

12. There are further requirements if you are a user equipped with a PC. You must not, without explicit permission from IT team:

- save business data or files to the local hard drive of the PC,
- save business data or files to removable storage (e.g. USB, DVD)
- save business data or files from the PC to a personal (i.e. non-Group owned) mobile device.

13. The Group enables users based away from its main offices and staff with home working entitlements to log into its network using a secure connection. You must follow the guidance issued when granted ‘remote access’, including use of two-factor authentication and keeping your log-in information secure.

14. Users working from home may only log-in using their own personal IT equipment with the express permission of the IT Service Desk or through the home-working mobilization project of 2020. Employees must ensure that their personal equipment:

- Has log-in security - password, code or biometric
- Has a modern operating system (Windows 10, Chrome OS or Mac equivalent) with updates applied
- Utilises Firefox or Chrome as its browser for accessing Citrix.

15. Employees experiencing problems with their personal equipment (either technical or practical issues, such as screen size) should request use of a Group device via their Director/Assistant Director. With the exception of trouble-shooting Citrix connection issues, no further assistance will be provided by the IT Service Desk to employees using personal equipment.

3.2. Mobile Devices (Phones, Smart Phones, Tablets and Cameras)

16. If a mobile device is required to fulfil your work role the Group will provide you with a phone or tablet.

17. As a mobile device user, you must:

- Follow the requirements set out on your device agreement (signed when receiving the device), which covers personal use and what to do in case of loss or theft of the device. Contact the IT Service Desk to receive a copy of the agreement.
- Have security measures active on the device (e.g. password or pass-code, encryption), including when tethering another device (e.g. lap-top without connectivity) to it.
- Keep the device, if a phone, switched on and charged during your working hours or when on-call, except when it would be inappropriate to take a call (e.g. during meetings or when in restricted areas such as the Connect offices).

- Minimise the personal data held on the phone by setting the email synchronization period to no more than 14 days. Only devices configured by the IT Service Desk for the purpose should be used for email.
- Be aware of your surroundings when making confidential phone calls, including when participating in video conference calls.
- Email images or recordings made on your device to your Group mailbox so they can be transferred to the relevant Group system at your first opportunity and delete the image or recording from your device.

18. As a mobile device user, you must not:

- Add hardware (including memory cards), or related components to the mobile device without the approval of the IT Service Desk.
- Swap SIM cards from one mobile handset to another
- Swap handsets with another user, or pass the device issued to you to another user, unless authorised by the IT Service Desk
- Attempt to access the Group's network using your own or a non-Group device.
- Record conversations or images without the knowledge or consent of the individuals concerned.
- Use the device when driving or controlling a vehicle - other than for accepting incoming calls on a hands-free mode, when it is safe to do
- Remove protective equipment (e.g., screen protection) from the device.

19. You are not permitted to use personal mobile devices for work activity (without permission of the IT Service Desk, or as a result of the home-working mobilization project of 2020) or connect personal devices to the Group's networked IT equipment.

20. The Group reserves the right to monitor use of mobile devices, which may have mobile device management software loaded enabling remote access to your device.

3.3. Internet

21. The internet is a vital tool for business purposes and an increasing number of the Group's information systems are internet/cloud based. This section is concerned with internet usage outside of those services officially procured by the Group. A separate section on social media/networking follows.

22. The internet can be a source of malware and viruses. You must:

- Always follow any warnings about internet site security - avoiding those sites
- Not click links on emails received from unfamiliar sources.

- Inform the IT Service Desk promptly if you are suspicious about a website that you have visited.

23. You should take care when contributing material to a website or other internet service, avoiding:

    - Revealing any commercial or confidential Group information
    - Participating in discussions that may bring the Group into disrepute
    - Discussion of work-related items. If you are aware of colleagues doing this, you must report it as a potential security risk to the IT Service Desk.

24. Personal use of the Internet is allowed in work breaks and outside of your working hours. You may not:

    - Use the internet for trading or personal business purposes
    - Stream media, such as radio or TV programmes, for non-work related purposes
    - Download video, music files, games, software and programs for non-work related purposes.
    - Access files from a personal cloud storage service (e.g. Dropbox, One Drive).

25. If you use the Internet to buy goods or services, the Group will not accept liability for default of payment or for security of any personal information you provide.

26. Many Internet sites that contain unacceptable content are blocked automatically by the Group's systems. However, it is not possible to block all ”unacceptable” sites electronically. You must not therefore deliberately view, copy or circulate any material (except where part of your work - e.g. investigating ASB complaints) that:

    - Is sexually explicit or obscene.
    - Is racist, sexist, homophobic, harassing or in any other way discriminatory or offensive.
    - Contains material the possession of which would constitute a criminal offence.
    - Promotes any form of criminal activity.
    - Contains images, cartoons or jokes that will cause offence.

27. You may receive an email or mistakenly visit an Internet site that contains unacceptable material. If this occurs, you must inform the IT Service Desk so they can investigate and block.

28. All Internet sessions should be terminated as soon as they are concluded.

29. The Group records the details of all Internet traffic. This is to protect the Group and users from security breaches, including hacking, and to ensure that ‘unacceptable’ sites are not being visited.

3.4. Social Media

30. Social media are on-line services that enable communication and sharing with other participants. It includes, but is not limited to, services such as Facebook, Twitter, Instagram and YouTube.

31. The Group uses official social media accounts, managed by our Communications and Marketing team, to communicate with customers, stakeholders and the public. Employees in roles such as Neighbourhood Development, Communications and Development may at their Director's discretion, set up 'professional' accounts to assist them with their work.

32. Employees may use personal social media at work, using Group IT equipment, in line with the requirements for internet use. Because activity on personal social media may be seen by customers and colleagues and so associated with the Group, employees should at all times understand and use the appropriate privacy settings on social media accounts. In use of personal social media accounts, the following should be avoided:

- posting or participating in exchanges that might bring the company into disrepute, or have the potential to adversely impact upon the reputation of the company.
- conducting themselves in a way that is detrimental to the company.
- posting or indicating support for abusive, offensive, hateful or defamatory messages, especially those which concern the company, its residents, colleagues and managers.
- posting information that could constitute a breach of copyright or data protection legislation
- seeking to communicate with or responding to issues raised by customers
- posting messages to Jigsaw's public social media accounts.

3.5. Email

33. Email is a key business tool for internal and external communication. It should not be considered a secure form of communication (unless you are using a secure email service). You should always use email professionally as the content you send can be used as evidence and can create a binding contract.

34. You must not use the email system in any way that is insulting or offensive. You must not deliberately view, copy or circulate any material (except where part of your work - e.g. investigating ASB complaints) that:

- Is sexually explicit or obscene
- Is racist, sexist, homophobic, harassing or in any other way discriminatory or offensive
- Contains material the possession of which would constitute a criminal offence

- Promotes any form of criminal activity
- Contains unwelcome propositions
- Contains images, cartoons or jokes that will cause offence
- Appears to be a chain letter
- Promotes a political viewpoint
- Promotes business interests that you have outside of work.

35. If you receive an email that is inappropriate or abusive, you must report it to the IT Service Desk immediately, who will take the appropriate action. If the sender is known to you, inform them that they should cease sending the material.

36. Email is used by 'cyber criminals'. To protect the Group and yourself, you should not:

    - Put access details (username, password) in an email, even if you have received a request that appears to be from the service provider
    - Follow links in emails that come from sources not known to you.

37. If you receive a suspicious email you should forward it to the IT Service Desk. If you become aware of an email 'scam', pass the details to the IT Service Desk. Please do not circulate the information to colleagues.

38. E-mail should not be used for communicating confidential information about customers externally - e.g. personal or financial information about named customers, or customers that could be identified by the content of message (e.g. home address) - unless it has been encrypted, using a secure email service. Contact the IT Service Desk for information.

39. You should balance the ease of communication by email with the dilution of its effectiveness if it is over-used. You should apply the following guidelines:

    - Address emails only to those individuals who need to see the content. Use email/office group addresses sparingly.
    - Do not attach large files to emails. Save files into shared drives and send your intended contacts a link to the file.
    - Save the content of emails relating to your casework to the appropriate corporate system and delete the email.
    - Purge your mailbox of emails with personal data regularly so only emails related to your current work are retained.
    - Use the 'out of office' function for any working days when you will not be checking your in-box.

40. The content of incoming email is automatically scanned to detect computer viruses and inappropriate content. The actual text of the email is not viewed as part of this process but the Group reserves the right to look at text if the automatic scanning highlights any issues and the text may be read if you have requested IT assistance with email.

41. A disclaimer is automatically attached to all emails sent from the Group informing the recipient that the email is intended solely for them, is confidential, may be legally privileged and may contain personal views that are not those of the Group.

42. Where an employee is absent, only the employee's Director or member of HR management may authorise access to a Group email account to obtain messages that are work-related. The manager will inform the employee of this access on the employee's return.

3.6. MS Teams and Skype for Business (SfB)

43. The MS Teams collaboration tool was rolled-out to employees in April 2020. Some staff retain access to Skype-for-Business until the corporate telephony project is concluded in 2020.

44. Combined, these products offer the following communication methods:

- Secure messaging
- Team messaging
- File sharing
- Voice calls and conferencing
- Video calls and conferencing
- Screen sharing.

Messaging

45. Acceptable use of messaging builds upon its advantages as a communication method:

- It is immediate and relatively informal (e.g. use of emoticons and gifs)
- All members of a team or channel can view the messages and contribute to discussions
- Messages appear and are stored in 'channels' focused on a specific subject or team
- Links to files can be shared, enabling colleagues to work together on a single document.

46. To ensure that the business benefits from messaging:

- Limit the amount of personal use so that it does not disrupt the conduct of your or colleagues' roles.
- Do not allow informality to become unprofessional (see examples in Email section, above)
- Formal requests (e.g. of a line manager) and communication related to Group procedures should be completed by email or in hard-copy.

47. Messaging is monitored by the Group in the same ways, and for the same purposes, as email traffic. Teams and Skype for Business are the only messaging services supported by the Group.

48. The following practices are required to fulfil data protection requirements:

- Sensitive personal information about customers, stakeholders or colleagues should not be disclosed. The content of messaging is subject to Data Protection legislation and may be requested by a data subject in a subject access request.
- Shared files containing personal data should be saved to private channels, all the members of which should have a business reason for accessing the file
- Business data should not be downloaded/exported from the Teams application to personal devices.
- Images of people should only be shared with the subject's consent.

Voice and Video Calls

49. For employees working at home, voice and video calls are a very important means of keeping in touch and bridging the gap created by remote working.

50. Voice and video calls may be recorded if the meeting organizer has the appropriate MS licence. If that is the case, the recording can be started and stopped by any of the participants. All participants are notified on their screen that a recording has started. However, any participant intending to record a call must notify participants before starting the recording. Personal information about customers, stakeholders or colleagues should not be disclosed on recorded calls. The content of recordings is subject to Data Protection legislation and may be requested by a data subject in a subject access request.

51. To ensure the business benefits from voice and video conference calls:

- This functionality is for business use only
- The organizer or nominated 'chair' should ensure that all participants know who else is on the call - perhaps by drawing attention to the facility that shows participants' identities
- Participants should be reminded to mute themselves when not talking to cut out background noise

- In larger conferences (five or more people), it is recommended that the organizer/chair works through an agenda and introduces participants to prevent people speaking at the same time.

52. Other video and tele-conference services (e.g. GoTo meeting, Zoom), may be used if you are invited to a conference by a third party. MS Teams and Skype-for-Business are the only services supported by the Group.

4 Home-Working

53. Some home-working requirements are mentioned in other parts of this policy. However, this section consolidates information on acceptable practice while working on IT equipment at home into a checklist.

Do

- Try to find a room where you can work away from other members of your household to avoid the possibility of data being shared with other persons who do not work for Jigsaw
- Shut down your home device when you have finished working on it. Chromebook users should log-out of their Citrix session and their device when finishing work.
- Take extra care and precaution when dealing with sensitive personal data. Think about people's privacy and the consequences if someone gained unauthorised access to the information.

Don't

- Divulge personal data about a customer when leaving a voicemail message on a colleague's phone. It could be a wrong number and this would be a data breach
- Store any Jigsaw information on home devices
- Use your mobile phone in the garden or anywhere in your home where you might be overheard if you are discussing or disclosing sensitive personal data
- Open emails from unknown sources or download attachments or click on links you don't think are genuine
- Leave paper or electronic files where they could be accidentally viewed by others, including family members
- Use free public wi-fi networks, eg. in supermarkets, to conduct Jigsaw business. These are not secure
- Dispose of confidential paper documents at home, unless you have a shredder.
- Securely store the documents until you can bring them back into work and dispose of them securely)

5 Monitoring and Delivery

54. Service Desk records will be reviewed to identify the type and source of IT security risks or incidents which may result in updates to the policy being required.

6 Legislation and Regulation

55. The policy has been developed to comply with the following legislation

56. • The Data Protection Act (2018)

57. • Computer Misuse Act (1990)

58. • Regulation of Investigatory Powers Act (2000)

- The Malicious Communications Act (1998)

59. • Human Rights Act (2000)

7 Related Policies and Procedures

- IT Security Policy
- Data Protection Policy
- Employee Privacy Notice
- Social Media/Networking Policy
- Disciplinary and Grievance Procedure
- Incident Management and Business Continuity Plan
- Mobile device agreement.

8 Glossary

60. Cloud storage - digital storage on servers remote from the user, usually owned by a hosting company

61. Cyber crime - use of a computer and network in a criminal act

62. Encryption - the process of converting information or data into a code, especially to prevent unauthorized access

63. Malware - software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system

64. Thin-client devices - a lightweight computer specifically designed to provide a user with access to central server resources for computing e.g. winterm or 10Zig. PCs can also be used in a thin-client manner.

65. Two-factor authentication - a security process in which a user provides two forms of authentication of their identity (e.g. password and code received on mobile device)

9 Document Control

Responsible Officer/s:	Director of Corporate Services
Date of Approval:	April 2020
Approved by:	Executive Management Team
To be Reviewed Every:	Two years

10 Appendix: Password Procedures

66. The Usernames and Passwords are a means of validating a user's authority to access the group's IT services. Members of staff who require access to the Group's IT network and the various programs within it will be provided with a unique username and password for the network and each application that requires a username and password. Where default passwords are issued to users new to systems, users must change the password at the first opportunity.

67. Line Managers are responsible for requesting all usernames and passwords for their new staff. This must be done by sending a completed New User form/request to the IT Service Desk at least seven days before the new user is due to start work.

68. The login to the network, allows the user access to general programs and functions such as Microsoft Office, files, print, emails, internet and business specific applications. Some key systems require their own additional login authentication and have their own password rule.

69. Network password standards for length and complexity are enforced by each of the legacy networks. Through the work to converge our systems and technology a common network password standard will be implemented. Users are recommended to adopt this standard before it becomes enforced. The password rule for the login to the Jigsaw network will become:

70. • Passwords must be a minimum of ten characters. Users are recommended to use a phrase that is memorable. The phrase must avoid:

- Their own name or that of family members
- Personal information - date of birth, address, favourite football team or musician
- Words such as 'password', 'computer'

71. • The password/phrase must not also be used for non-work log-ins.

72. Where a password has been incorrectly entered more than five times, the account will be locked out until the user's identity has been confirmed.

73. Passwords for other applications should also be a minimum of eight characters with a mix of letters and numbers; or if letters only, at least 15 characters. This applies to applications hosted on the Group's network and those hosted externally.

74. Requiring users to have multiple passwords for different systems and services is acknowledged by security experts to create insecurity as users take short-cuts to help them remember their details. To avoid this, passwords will only be required for applications on the Jigsaw network which hold significant quantities of personal or commercial data. These include: Northgate, QL, Chris21, HR21, React.

75. These rules may be varied where a specific application has its own requirements or limitations.

76. The misuse of username and password can result in unauthorized transactions occurring on the user's account therefore it is essential that network and application passwords are kept secure. Specifically, users must adhere to the following

77. • Any records of your passwords must be kept securely (e.g. in a locked drawer for which you are the only key-holder, or on using a Group-approved application/software for password recording).

78. • Do not tell anyone your password.

79. • Do not allow anyone else to use your PC/Winterm/10Zig whilst you are logged in.

80. • Always log off from your PC/Winterm/10Zig when you are not using it or away from your desk on breaks, meetings etc.

81. Care should be taken when entering a password so that no one can see what is being entered. Users who believe their password is known to others or is being used by some one else must inform their Line Manager and contact the IT Service Desk immediately.

82. On finding or suspecting that someone other than the allocated user is using a username and password, the IT team will disable it immediately. To have the username and password re-enabled, the user's line manager must contact the IT team.

83. When a member of staff gives notice of his/her intention to leave employment, the HR Team inform the IT team of the employee's leaving date so that their login facility to the system can be programmed to expire after their last working day. However in the event of staff dismissal or sudden departure then the Line Manger must inform the IT Team of this incident so the IT Team can take the appropriate security measures.

Jigsaw

Creating homes. Building lives.

Jigsaw Homes Group Ltd.

Cavendish 249
Cavendish Street
Ashton-under-Lyne
OL6 7AT

https://www.jigsawhomes.org.uk
0300 111 1133
info@jigsawhomes.org.uk

Regulated by the Regulator of Social Housing Registration No. LH 4345

Registered under the Co-operative and Community Benefit Societies Act 2014 Registration No. 29433R

Document produced on 14 July 2020.