Acceptable Use Policy

Contents

1. Introduction

1.1 The Acceptable Use Policy covers all Mobile phones and tablet devices and installed applications across the ng group and any reference to ng homes will also refer to the ng group. The policy specifically covers (mobile phones, tablets and accessories) issued by ng homes to individuals for business use. This policy is designed to provide all users with clear guidelines on the use of such devices.

1.2 Modern mediums of communications make it easier for information to be shared electronically. This policy also covers email, the internet, social media, and rules governing the sharing and storage of the company's data as well as other electronic communications.

1.3 We recognise that the potential for misuse or improper use exists and this policy has been developed to reflect how we will manage this with principles and procedures which are consistent with other more traditional forms of communication within and outside the Association and it is designed to provide all users with clear guidelines on acceptable use. Customer service and customer care are central to these, as are the principles associated with freedom of information and data protection/confidentiality. This Policy is designed to support users to operate safely, securely and legally and as such, the Association will never ask you to breach the law whatever the circumstances.

2. Who does this policy apply to?

2.1 This policy applies to all staff, Board members of the Association (including remote users) and consultants working on behalf of the organisation or within the organisation and refers to how any issued devices should be handled by individuals whilst carrying out work on behalf of the association.

2.2 Any person who uses the Association's electronic communications facilities consents to all the provisions of this policy and agrees to comply with all its terms and conditions and with all applicable laws and regulations.

2.3 Any user of the electronic communications facilities, whose actions violate this policy, or any other Association policy or regulation, may be subject to limitations or elimination of these privileges as well as other action in relation to the breach as per the Staff Conditions of Employment and/or the staff Code of Conduct / Code of Conduct for Board Members. External contractors or consultants who may have breached the terms of the policy will be subject to investigation. If after investigation it is concluded that a breach of the policy has occurred, then it will be at the discretion of the Association to impose penalties up to total exclusion from the Association's systems and contracts.

3. Aims of the Policy

3.1 The Policy aims to cover the following:

- To ensure that use of any phones or tablet provided by the Association is used and is consistent with its own internal policies, all applicable laws, and the individual user's job responsibilities.

- To clarify the principles and guidelines for appropriate use and care of all electronic resources and electronic communication. A serious breach of these provisions by a staff member could lead to disciplinary action. If anyone is unsure about anything they propose to do, and it might breach this policy they should speak to their manager for advice first.

- To ensure that all users of the Association's computer resources do so in a manner consistent with the values and objectives of the Association, whilst ensuring the security of the Association's computer network systems. They must be used in a manner that is consistent with the Association's standard terms of business conduct and as part of your specific job responsibility.

- Instructions of any guidelines on Cybersecurity should also be followed.

These provisions are designed to minimise the legal risks the Association runs when you use email, internet, mobile devices and social media using equipment provided by the Association. They are also designed to tell you what you may and may not do in this area.

Managers are responsible for the day-to-day implementation of the policy and ensuring that those they are responsible for use the system in the appropriate manner.

4. Privacy: Your Expectations

4.1 You must have no expectation of privacy in anything you create, store, send or receive on the company's computer system or mobile devices. Emails, internet and mobile device usage can be monitored without prior notification if ng homes deem this necessary. Regular random checks on the use of all IT resources may be made to ensure compliance with this policy.

4.2 Since Association resources are being used to create and store files, users should understand that the Association must assign certain individuals with the responsibility for maintaining, repairing, and further developing those resources. Some individuals, by virtue of their positions within the Association and their specific responsibilities, may have special access privileges to hardware and software and therefore its content.

4.3 The Association will strive to protect individual privacy by ensuring that the number of individuals with this level of access is strictly limited and that such individuals are selected for their judgment and ethics, as well as their technical expertise. Such positions, and the individuals who hold them, will be governed through defined responsibilities and procedures.

4.4 Users need to be aware that the email and file systems are part of the daily back up procedure covering all the Association's computer data.

5. Use of the Internet

5.1 Users of the internet are reminded that Web browsers such as "Explorer", "Firefox" and "Google Chrome" leave "footprints" providing a trail of all sites visited by users.

5.2 Business systems will maintain a log of all web activity for all users and any abuse of internet access will be reported to the relevant line manager.

5.3 Employees or other users must not access the internet or email facilities for personal use without prior permission from their relevant manager. However, users may obtain permission for personal access to sites during agreed contractual rest periods such as lunchtime.

5.4 Web filter software (Cisco Umbrella) has been installed which restricts access to forbidden sites via corporate browsers. This can be updated manually at any time and staff, Board members and anyone using the internet are asked to advise the Deputy CEO (Finance) of any known offensive sites in order that they may be added. In addition, sites that may be blocked but are harmless or categorised incorrectly can also be added as acceptable sites, again you should advise the Deputy CEO (Finance) of such sites.

5.5 Registration as a user of specific websites for work purposes is encouraged, but authorisation must first be obtained from your line manager.

6. Use of Email

6.1 Email is a very informal medium. It is closer to speech than a written communication, and yet there is a permanent written record. It typically lacks the care given to a written communication, and can often be stilted, abbreviated and conversational. In addition, it is often the case that people ''say'' things in email and on-line which they might not otherwise feel comfortable communicating to others.

6.2 The following guidelines must be strictly observed in the use of email:

- You must make sure you do not send defamatory statements in emails, text and multimedia messages or other electronic means as the Association could be liable for damages and this may result in disciplinary action.
- Users must not send unsolicited, irrelevant or inappropriate email to multiple mailing lists on the internet or make other use of unsolicited email.
- Email communications are not guaranteed to be private.

- Personal email and Internet services must not be used for formal communications.
- Users must not transmit confidential, personal or other sensitive information via their personal email on the Internet.
- Do not open attachments on email messages unless certain of the source.
- You also have the right to raise a grievance should you receive offensive email or are concerned about a colleague's general use of the internet/email resources.
- Users should take care not to infringe copyright when downloading material or forwarding it to others.
- If you are on holiday or otherwise absent from the office for any period of time in excess of 24 hours (1 working day), you must redirect your incoming email messages to state that you are out of the office and that if the email is urgent that it should be retransmitted to the appropriate person (giving both email and telephone contact details). Also, workflow should be set to 'out of office' and invoices redirected to another staff member.
- Emails which are received through ng homes' website or external emails received from customers by individuals should be brought to the attention of your line manager. Similar to all other correspondence, emails from/to residents should be scanned into their electronic file.
- You need to be careful not to introduce viruses on to the system. Do not open emails or attachments you are not familiar with.
- Some people will send an email with content that they would never say in person. Take a minute before you compile and send an email message. Be careful about what words you use and how you say them. Remember that messages can be printed or forwarded. Do not say things you will regret later.
- The Association has secure means of email and data transmission based on the computer package egress. On all occasions when tenant, employee or other data is being transmitted either internally or externally then consideration should be given to using egress. The other advantage of using egress is that it removes issues that can arise with the size of the file that is being transmitted.

- Where egress is not being used then any files including sensitive data should be sent in a password protected format. The password should be sent separately from the data file.

7. Use of Mobile Devices

7.1 This section is to define standards, procedures, and restrictions for staff, Board members and consultants who use a private or an Association provided mobile device that can access the Association's electronic resources. This applies to, but is not limited to, all devices and accompanying media that fit the following device classifications:

- Mobile phones & Smartphones
- Laptop/Tablet computers such as iPads
- Any mobile device capable of storing Association data and connecting to an unmanaged network.

7.2 These guidelines are to protect the integrity and confidential data that resides within the Association's technology infrastructure. It intends to prevent this data from being deliberately or inadvertently stored insecurely on a mobile device or carried over an insecure network where it can potentially be compromised. A breach of this type could result in loss of information, damage to critical applications, financial loss, and damage to the Association's public image.

7.3 Addition of new hardware, software, and/or related components to provide additional mobile device connectivity will be managed at the discretion of IT and the Deputy CEO (Finance). Unauthorised use of mobile devices to back up, store, and otherwise access any Association related information / data is strictly forbidden. The following should be observed:

Mobile Phones/Smartphones

- The sim card must not be transferred to another device unless to another company issued mobile. The sim card must be password protected immediately from first use. In addition, the mobile itself must be password protected. Not to do so or removing the passwords may be the subject of disciplinary action.

- If lost or stolen the user must immediately contact their manager, Deputy CEO (Finance) or IT System Administrator (IT Consultants) to report the incident. The user should also contact the service provider and have the sim blocked.
- Do not install any software on devices without prior authorisation from the Deputy CEO (Finance) or IT System Administrator
- Do not sign up to any services that impose ongoing charges without prior approval from your manager. If incurred the cost of any unauthorised charges may be recovered from the user.
- Always keep the device physically secure when you have it in your possession.
- Do not allow anyone to use the device (if the sim card is activated) to make calls or otherwise.
- Do not send texts (from devices that have voice/text active) that could be deemed offensive.
- Do not send confidential, personal or other sensitive information via text from your device. Use of the Egress system should be accessed for such information.
- In the event of damage, loss or a stolen device this must be reported to your manager and then IT immediately.
- It is the user's responsibility to ensure safekeeping of their mobile phone and associated accessories e.g. chargers, earphones etc. In the event of loss the user may be responsible for the cost to replace such items. This excludes normal "wear and tear".
- Should a mobile device be returned to ng homes for any reason then all items issued with the phone must also be returned. Failure to do so may result in the person being liable for the cost of replacing such items.
- It is the users responsibility to keep accessories in a safe manner.

The Association recognises that users may, on occasion, have to make personal calls or send personal text messages during working hours or outside normal working hours. Where it is deemed that an unreasonable amount of personal calls/texts have been made using

the phone, the Association reserves the right to deduct these costs, either through deduction of pay or otherwise. Disciplinary procedures may be followed where the use is excessive.

The user agrees that upon termination of employment, should the user not return their mobile phone (including accessories provided), or should the phone be in a unsatisfactory condition, the costs of replacement or a proportional amount of this as decided by the Association, may be deducted from any final monies owing, or the user will otherwise reimburse the Association.

Laptop/Tablet computers such as iPads and other mobile device

Only laptop/tablet and similar mobile devices provided by ng homes may be used to capture company information. These devices are set-up to connect either via Wi-Fi or Ethernet cabling and are configured to operate in a certain way.

- Connection to the company systems is achieved using two factor authentication. A two-stage process: Confirm who you are by accessing a code on your mobile phone followed by a second username and password to access systems resources.
- No data relating to the organisation should be stored on the hard drive of the laptop/tablet, iPad or similar device.
- Strong passwords and screen locks must be maintained during operation.
- Devices must not be left unattended at any time.
- Mobile Device Management software exists on the device as per our MDM policy.
- System updates and anti-virus software will update automatically.
- No applications or programs are to be installed on these systems unless authorised by your manager, the Deputy CEO (Finance) or the IT System Administrator.
- The laptop or tablet should be transported in a safe way (preferably in a suitable case/bag/cover).
- The user is responsible at all times for the safekeeping of their devices.

8. Social Media

8.1 The growth of Social Media provides a new opportunity to engage directly with tenants and other organisations as well as the general public. It is fast moving and reaches vast audiences such as public and private sectors, politicians, key decision makers and influencers. The most commonly used social media platforms are: Twitter, Facebook and LinkedIn. Social Media is an additional form of communication to be used alongside traditional and other communication channels such as press releases, printed publications, emails and websites.

8.2 Only authorised staff are permitted to post material on a social media website in ng homes name and on our behalf. Any breach of this restriction will be dealt with through the Association's disciplinary procedures and this may amount to gross misconduct. Although social media delivers significant positive benefits to business, it is also high risk and open to abuse or misuse and occasionally to negative engagement with potentially abusive parties or those who pose a risk to the Association's reputation.

8.3 The Association understands that Board members and staff as well as external consultants may engage with the organisation using social media. This section sets out the standards expected of ng homes' employees, consultants and agency staff when using social media tools whether that be in connection with ng homes' business or in the case of social media platforms the expression of views that contradict, oppose or infringe on the purpose, ethos, values or principles of ng homes.

- any person who uses ng homes' communication tools consents to all the provisions of this policy and agrees to comply with all its terms and conditions and with all applicable laws and regulations.
- the policy aims to ensure that use of social media among ng homes' users is consistent with its own internal policies, all applicable legislation, and the individual user's job responsibilities.

8.4 The following is a guide on ng homes' standards and related to proper use although this list is not exhaustive:

- Inappropriate messages are prohibited including those which contradict, oppose or infringe on the purpose, ethos or principles of ng homes and its subsidiaries.
- If a member of staff is in receipt of such messages, they should raise any concerns with their line manager immediately.
- Staff also have the right to raise a grievance should they receive offensive communication messages via social media from a fellow employee.
- If there is concern over a colleague's general conduct using social media this must be raised immediately with their line manager.
- users should not send potentially defamatory communication messages which criticise other individuals or organisations.
- Users should not access or download inappropriate material, such as pornography from social media.
- Users should take care not to infringe copyright when downloading material or forwarding it to others.

9. Social Media Platforms

9.1 ng homes respects the right to a private life and that includes joining any social media platforms. However, information posted on such sites is classed as public and not private. Staff are therefore not allowed to disclose confidential information relating to ng homes or its subsidiaries, its customers, partners, suppliers, Board members, employees, or stakeholders on any social networking platforms. It is also prohibited to post any comments on people and events connected to ng homes or its subsidiaries or make any remarks which could potentially bring ng homes or its subsidiaries into disrepute. Any such actions could result in disciplinary action, including dismissal.

If using social media platforms staff are expected to adhere to the following;

- keep profiles set to private and protect tweets.
- ensure all passwords are kept private.

- we prohibit employees from listing ng homes or any of its subsidiaries as their employer.

All staff should be aware of the language and content of their posts – in particular where there is an association with their employer e.g. linked with colleagues.

10. Telephone System

10.1 The telephone system (including the fax system) is a business system and as such should primarily be used only for work purposes. Monitoring of the system (call volumes and call details etc.) takes place and reports are produced for reviewing and improving customer service. You may make and take personal calls on the telephone system or on personal mobile phones during working hours provided that use is occasional and reasonable and does not otherwise interfere with your allocated responsibilities.

11. Policy Breaches

11.1 Any line manager concerned about an employee's breach of this policy, e.g. excessive use of social media, should not unilaterally seek to gain access to a user's electronic communications. Instead, the manager should:

- review whether expectations and standards in this area have been well communicated and made clear to the user.
- pursue direct communication with the user regarding the issue.
- Contact HR and follow the appropriate policy / procedure, this may include the Association's disciplinary procedures.

The following are some examples of breaches of this policy however this list is not exhaustive:

- concealment or misrepresentation of names or affiliations in posts.
- any use of social media linked to ng homes or its subsidiaries for commercial or private business purposes is prohibited.

- use of social media, in a way that unreasonably interferes with or threatens other individuals.
- use of social media that degrades or demeans other individuals – whether ng homes employees or others.
- the purchase or sale of personal items through advertising on the internet.
- the use of social media to harass employees, vendors, customers, and others.
- the use of social media for political purposes.
- the release of untrue, distorted, or confidential information regarding ng homes' or its subsidiaries business via social media.

12. General

12.1 As mentioned earlier, the Association provides electronic mail (email), internet facilities and where appropriate, mobile devices to support its communication, learning and service activities and associated administrative functions. Any use of the facilities that interferes with these activities and functions or does not respect the image and reputation of the Association is therefore improper.

12.2 The following are examples of improper use of email/internet/ messaging however this list is not exhaustive:

- Intentional transmitting/accessing material, which is obscene. If the graphic or written content in the email would be inappropriate for a standard letter then DON'T send the email e.g. inappropriate messages including those which are sexually harassing or offensive to others on the grounds of age, physical ability, race, religion or gender or any protected characteristics under the Equality Act 2010.
- Use of email, which unreasonably interferes with or threatens other individuals.
- Use of email that degrades or demeans other individuals – whether Association employees or others.
- Downloading or attempting to downloading inappropriate material, such as pornography, from the internet.

- Breaking through or bypassing ANY internal or external security controls.
- Threatening an individual's privacy or reputation either through libel or the passing of unauthorised personal data.
- Political lobbying or private business.
- Doing anything that is illegal.
- Breaching of intellectual copyright.
- Any activities, which could cause congestion and disruption of networks and systems.
- Concealment or misrepresentation of names or affiliations in email messages.
- Alteration of source or destination addresses of email.
- Use of email facilities for commercial or private business purposes.
- Commercial use - any form of commercial use of the internet is prohibited.
- Solicitation - the purchase or sale of personal items through advertising on the internet is prohibited.
- Political - the use of the internet for political purposes is prohibited.
- Misinformation/confidential information - the release of untrue, distorted, or confidential information regarding Association business is prohibited.
- Viewing/downloading purely entertainment sites or material where there is no benefit to the Association in terms of its learning, communication or service aims described earlier.

13. Actions in Response to Policy Breaches

13.1 ng homes may respond to policy breaches by an employee or other user as follows (please note that this list is not exhaustive):

- Denial of internet access;
- Disciplinary action;
- Civil proceedings;

- Passing of information to the Police for possible criminal proceedings.

14. Systems

14.1 All IT systems are the property of the Association and are provided for business-related purposes only and any and all data created using the Association's IT systems remains the sole property of the Association. It is expressly prohibited to attempt to access any IT system using a username and password other than those issued to you. You must not divulge your username and/or password to any third party. In particular, you should not write your username or password and leave it where it can be easily found. Please remember that you will be held accountable for any activities, which are conducted using your username/password, except where you have alerted IT of a possible security breach.

14.2 There are anti-virus measures in place to protect the Association's systems against loss of data and serious disruption to the Association's business and only the IT System Administrator is authorised to check or load external disks or data, software or electronic files.

14.3 No changes are to be made to the software installed on any of the Association's IT systems unless those changes are agreed with your manager and are made by the IT System Administrator. This includes the installation of screensavers or desktop background images.

14.4 Any documents created by you on IT systems which is not the property of the Association, and which you intend to access or modify using the Association's IT systems must be checked for viruses by IT prior to their introduction to the system. This includes, for example, documents, which have been created using your own personal computer and brought into work on portable media such as USB memory sticks, CD's, DVD's and camera storage disks.

14.5 If you are taking any electronic documents off-site, please be aware that you are still responsible for Association confidentiality under the Data Protection Act, and those documents should not be made available to any person who is not a member of the Association's staff, except where expressly required for conducting the Association's

business. Normally data should be stored in encrypted format if taken off site on appropriate media. The IT System Administrator can advise on this.

14.6 Under no circumstances should any equipment supplied by the Association be used for illegal activities.

14.7 You must not attempt to circumvent any system security measures.

14.8 You must not attempt to take copies of any files or copyrighted material or systems software using ng homes' IT systems.

14.9 Staff, Board members or other users must not forward any virus warning of any kind to anyone other than the IT System Administrator. It does not matter if the virus warnings have come from an anti-virus vendor or by any larger computer company. All virus warnings should be sent to the IT System Administrator alone.

15. Security

15.1 Security, including protection from viruses as well as security of Association information, is a concern with both internet and email use. Access to email and the internet is restricted to authorised persons.

15.2 Users are responsible for the security of their own passwords, which protect against unauthorised access. Users should keep personal log-on and passwords confidential and change passwords on a regular basis as instructed by procedures.

15.3 Failure to adhere to this policy jeopardises network security and puts users at risk of potential misuse of the system by other individuals. Network users may be held responsible for all actions taken using their personal network access permissions.

15.4 In a further effort to ensure the security of our systems and the information placed on it by users. Virus detection software is installed on all desktops on the network and users are responsible for virus checking of downloaded files.

16. Standards for IT System Administrators

16.1 IT System Administrators (IT Consultants) have specific responsibilities and access capabilities and in line with these they are expected to exercise special care in order to protect the privacy of the individuals whose electronic communications they handle.

16.2 The IT System Administrators will maintain the following standards:

- Use machine headers and machine-generated messages in order to return undeliverable mail
- Avoid reading message content to the greatest degree possible
- Inform users of procedures for providing service, and assiduously attempt to respect privacy
- Inform users and be straightforward if something goes wrong, in order to maintain trust
- Keep confidential the content of any message that was inadvertently read in the course of redirecting undeliverable mail
- Consult with users first if it seems necessary to go beyond machine-generated explanations
- Be informed about and follow Association policy regarding privacy in electronic communication.

17. Use of laptops

17.1 You may not bring your own laptop, IPAD, tablet, palm top or other computer or device into work to surf the internet or send emails during working hours unless you have been permitted to do so by your line manager.

17.2 If you have access to and the use of the Association's laptops, use of the same is restricted to business use only by authorised personnel and for no other purpose.

17.3 You are not permitted to arrange your own internet access on the PC on your desk. All internet access must be officially sanctioned and put in place by the IT System Administrators.

18. Copyright

18.1 Most information available electronically is protected by copyright. The Copyright, Designs and Patents Act 1988 sets out the rules. Be careful not to breach copyright. The Association could be subject to legal action and you could be subject to disciplinary procedures which could include dismissal. It is easy to copy electronically, but this does not make it any less an offence.

18.2 The Association's policy is to comply with copyright laws. The Association does not allow the use of pirated or copied computer software. All software must be licensed. The Association takes this very seriously and undertakes regular audits to check the position.

18.3 Do not assume that because a document or file is on the internet or the Association's internal system or website that it can be freely copied. Sometimes information is made available on other people's websites and they say you may freely copy it. However, occasionally someone may post information on the internet other than the copyright owner and copying it may therefore not be a protection from breach of copyright. There is a difference between information in the "public domain" (which is certainly then no longer confidential or secret information, but is still copyright protected) and information, which is not protected by copyright. Copyright and Database Right Law can be complicated. Speak to the Deputy CEO (Finance) for guidance if you are unsure about anything connected to copyright.

18.4 There is a lot of information available on the internet describing what copyright conditions are. Read these before downloading or copying. For example, the Department of Trade and Industry produce guideline notes on areas relevant to business. Whilst these may be downloaded you may not be permitted to reproduce them in a book or other Association document without obtaining separate consent.

19. Trademark, Links and Data Protection

19.1 The Association's name is a trademark. If anyone is using the same or a similar name, please advise the Chief Executive. No new domain names or trademarks relating to the Association's name or products anywhere in the world shall be registered, unless the Association has authorised it. The Association's web pages shall not be linked to any third party's web pages or website without the prior consent of the Chief Executive.

19.2 The Association operates in accordance with the Data Protection Act 1998, Data Protection Act 2018 and the UK General Data Protection Regulation 2021. These laws specify how the Association deals with and handles "personal data" whether by email or any other means. Personal data would be information such as names and addresses or other personal details.

19.3 Certain data such as descriptions of people's race or religion is called "sensitive personal data" and subject to even stricter rules that require that explicit consent is obtained from the data subject before its dissemination. It is imperative that personal data is treated in accordance with the principles of the law.

20. Legal Compliance

This policy complies with the following:

- Electronic Communications Act 2000
- Copyright, Designs and Patent Act 1988

21. UK General Data Protection Regulation 2021

The organisation will treat your personal data in line with our obligations under the UK General Data Protection Regulation 2021 (UK GDPR) and our own Data Protection Policy. Information regarding how your data will be used and the basis for processing your data is provided in our Fair Processing Notice.

22. Other Related Policies

- Data Protection

- Freedom of Information and Environmental Information Policy and Procedures
- ng homes Staff Terms and Conditions of Conditions of Employment
- ng2 Ltd Staff Terms and Conditions of Employment
- ng homes Disciplinary and Grievance Procedures
- ng2 Ltd Disciplinary and Grievance Procedures
- Code of Conduct for Staff
- Code of Conduct for Board Members
- Flexible Working
- Home Working
- Hybrid Working
- Dignity at Work
- Equality and Diversity

23. Equality Impact Assessment

This Policy is equally applicable to all and has no detrimental impact on protected characteristic groups under the Equality Act 2010.

24. Policy Review

This Policy will be reviewed every three years or earlier in line with regulatory or legislative guidance/changes or good practice guidelines.