NOTTINGHAM CITY HOMES

ICT SECURITY AND ACCEPTABLE USE POLICY

FEBRUARY 2018

Contents

1.0 Introduction

ICT is an essential enabler to how we work but we need clear rules to protect the company, staff and our customers. We value the capabilities ICT offers to authorised users for management of information, flexible and mobile working and communication.

NCH provides ICT facilities, including computers, telephone services, peripheral devices, e-mail and internet access to support staff when carrying out activities on behalf of Nottingham City Homes. These facilities are intended for work purposes, but authorised users may benefit from making limited personal use of these facilities in accordance with this policy. This document represents the Company's policy on how these facilities should be used in the context of both work and personal use. It will be subject to review at least every two years.

2.0 Monitoring of Use

2.1 NCH via NCC will monitor your use of its IT facilities and business communications over e-mail and internet traffic for reasons which include:

- Providing evidence of business transactions
- Ensuring that the Company's business procedures, policies and contracts with employees are adhered to
- Ensuring compliance with any legal obligations
- Monitoring standards of service, employee performance and for employee training and safety
- Preventing or detecting unauthorised use of the Company's communications systems or criminal or unlawful activities
- Maintaining the effective operation of the Company's communications
- Business continuity purposes

2.2 NCH is ultimately responsible and accountable for all business communications transmitted by and stored on its information and communications systems. This applies equally through use of the facilities in the office or connection to the facilities from a remote location including via personal wifi from home. To maintain your own personal privacy, you must be aware that all communications and files passing through the Company's e-mail, computer and telephony systems are classed as business communications and may be required as legal records.

2.3 As far as possible and appropriate, NCH will respect your privacy and autonomy while working, however monitoring activities cannot

distinguish between personal and business items, therefore the Company may unavoidably record sensitive personal data about you which may arise from any personal use you make. The Company will not intentionally discover or copy non-business personal data but it cannot assure that this does not happen. By carrying out such activities using NCH's facilities you consent to our processing any sensitive personal data about you which may be revealed by monitoring.

2.4 You must be aware that NCH may need to access your allocated electronic mailboxes and view your e-mails or computer files for business purposes whilst you may be absent, for example for business continuity purposes. This will be carried out in accordance with Nottingham City Council procedure for Information Management Services.

2.5 All records, materials or items produced in the course of your work, including e-mails created, received or used in the course of our business, are considered to be the property of the NCH. When you leave your employment or relationship with NCH you are responsible for ensuring all personal e-mails or files are deleted and for making arrangements to transfer to colleagues any business electronic information.

3.0 Computing Guidelines

3.1 You should never leave any NCH mobile ICT equipment unsecured or unattended. They must always be kept with you or stored in a secure location.

You are accountable for all screen activity & transactions entered through your User ID whether or not you were present at the time.

3.2 You must ensure that any computer or laptop is connected to NCH's network at least once every 30 days to receive critical updates for protecting the equipment.

3.3 Whenever you are away from your desk always 'lock' your computer screen to protect your work and access to any sensitive information you may have access to. To do this either press the "windows key" and L or 'Ctrl Alt Delete' and then choose 'lock' your workstation.

3.4 Always take suitable precautions to ensure the security of data during and after transmission and to ensure it cannot be accessed by anyone apart from the intended recipient. Failure to apply appropriate precautions may constitute a breach of GDPR / the Data Protection Act.

3.5 If for any reason you lose a laptop/desktop/tablet PC report this to the ICT team immediately. If you lose a smartphone, camera or other mobile device report this to your line manager.

4.0 Password Guidelines

4.1 Passwords must NEVER be disclosed to anyone, if you suspect the confidentiality of your password has been compromised you must change it immediately.

You will be held responsible for any action taken using your User ID /password

4.2 Accounts should have strong passwords and should consist of a minimum of 8 characters containing 3 out of the following 4 categories - upper case, lower case, numeric and special characters e.g. %£*& etc. Avoid words found in a dictionary. From time to time changes to the password strength may occur due to NCC network requirements.

4.3 Protect your password and do not write it down. If you forget your password ICT will be happy to reset it for you.

5.0 Access Control

5.1 Access to systems will be granted where there is a business need. The New Starter and/or Role Change Forms must be approved and submitted by line managers and passed onto ICT for processing.

5.2 It is the line manager's responsibility to inform ICT if a member of staff has left NCH or moved role so that unnecessary system access permissions can be removed. Any breaches once staff has left their role will be responsibility of the line manager and ICT must be notified immediately.

5.3 It is a staff member's responsibility to stop using systems relating to past roles and to inform their line manager in order to contact ICT so that access can be removed.

5.4 A staff member must not access systems where access is not approved for their role

5.5 It is a breach of this policy to knowingly log-in to a system using someone else's log-in credentials.

6.0 Conduct when accessing systems for which you have authorisation

6.1 We expect the highest standards of professional conduct from our staff when using NCH systems, and behaviour should be in line with the requirements of your job role and company business processes. In particular, you must not engage in:

- malicious damage to system configurations/settings/data or to equipment.
- Interference with the operation of any security features or software installed on the computer e.g. anti-virus or firewall software
- engaging in any hacking related activities
- data theft.
- sharing of data or equipment with unauthorised individuals or organisations.
- excessive use of office ICT equipment and services for non-work purposes

Accidental incidents of the above should be reported immediately to your line manager so that remedial action can be taken.

7.0 Corporate Software

7.1 NCH is committed to achieving and ensuring software use in compliance with all license agreements. Only authorised and licensed software can be used on a computer or mobile device owned by NCH.

7.2 Do not download or attempt to load any software on NCH computer equipment without approval of the ICT Team. The use of a personal mobile 'App' will be accepted provided that the requirements stated in paragraphs and of this Policy are understood and adhered to.

7.3 Unauthorised duplication of software may subject users and / or NCH to both civil and criminal penalties under the Copyright Designs and Patents Acts, 1988.

8.0 Corporate Hardware

8.1 ICT will maintain an asset register of ICT devices and which members of staff they are issued to. Hardware must be returned to ICT by line-managers when staff leave or change teams. This allows equipment to be reallocated where needed and the maintenance of accurate asset registers.

8.2 Users will not connect any hardware to any NCH-owned ICT device, unless authorised by NCH ICT.

8.3 Users must not remove or deface any asset registration numbers or device serial numbers on NCH owned ICT devices.

9.0 Internet

9.1 Reasonable personal use of the Internet is allowed; this should be during your own time for example: during lunch breaks or outside of normal working hours. Internet use is monitored. Significant personal use detected during the employee's working time will be classified as misconduct.

9.2 All Internet access will be subject to filtering that restricts access to certain categories of web sites. If you require access to a web site for business purposes which has been blocked by NCH's content filtering service you should submit a request to the ICT Team for review.

9.3 You must not use the Internet to display, generate and /or pass on any material which may be regarded as offensive and / or discriminatory. You must not use the Internet to convey information which conflicts with the values of the company or its objectives. It is each member of staff's personal responsibility to police their own use and to flag to managers when access is made in error. This applies to areas which may be seen to be humour based content but which may be offensive and / or discriminatory to others. Where staff engage in such use of the Internet this is considered to be a fundamental breach of trust which amounts to gross misconduct.

9.4 Users may not transmit defamatory material, carry out freelance work online, download media files e.g. films or other potentially large files. Under no circumstances should you download programs from the Internet, without the consent of a senior member of the ICT Team (for exceptions see section 12).

10.0 Information Security

10.1 Confidential information should never be downloaded, sent, e-mailed or otherwise transferred to personal (not belonging to NCH) computers, personal memory sticks or other portable storage devices or to unauthorised individuals and/or organisations.

10.2 All electronic forms of information are covered by this policy including information in the form of digital photographs.

10.3 All electronic work documents and files should be stored in corporate filing system on one or more of the central systems provided for that purpose (for example, the 'S: Drive' or Serengeti). The U: Drive is to be used in a limited manner - only for files related to your own personal employment and not for work files that someone else or your successor in a role might need to access. Local PC hard-disks are not suitable locations to store important work-related information as the disks are not backed-up and so data will be lost if the machine fails or is re-built by ICT.

10.4 Where users access Government Connect Secure Extranet (GCSx) type services, facilities or highly sensitive information, under no circumstances should non-NCH owned equipment be used.

11.0 E-Mail

11.1 NCH e-mail accounts are primarily for NCH business purposes. If you use the company's e-mail system for sending and receiving personal e-mails, then you signify your agreement to abide by the conditions as outlined in this policy and your consent for monitoring of personal e-mail in accordance with Section 2.0.

11.2 Treat unsolicited e-mails with caution. You should not open any e-mail from a suspicious sender. If in any doubt, do not open any attachment and delete the e-mail without opening it.

11.3 You must not use the e-mail system to display, generate and /or pass on any material which may be regarded as offensive or discriminatory. The use of obscene language or swear words or similar alternative words is prohibited. You must not use the Internet to convey information which conflicts with the values of the company or its objectives. It is each member of staff's personal responsibility to police their own use and to flag to managers when access is made in error. This policy applies to areas which may be seen to be humour based content but which may be offensive to others. Where staff engage in such use of e-mail this is considered to be a fundamental breach of trust which amounts to gross misconduct. Any inappropriate e-mails received into the company must be deleted and the sender informed that such contact is not permitted by NCH.

11.4 Exercise discretion in the use of e-mail. Other communication methods may be more appropriate and effective when:

- An answer is needed quickly
- There is doubt that the reply will be received within the required period
- Confidential or sensitive information needs to be communicated
- The subject matter may require explanation or discussion to be understood by the recipient

11.5 When available, your employee photographic ID will be displayed within e-mail messages (internal only) to aid identification and communication. You may request for the photograph not to be displayed by making a request to ICT through your line manager.

11.6 Remember that e-mails can be disclosed in the course of legal proceedings and can also be disclosed on request under GDPR, the

Data Protection Act 1998, 2018, or Freedom of Information Act or via the EIR regulations.

12.0 Mobile Devices

12.1 NCH provides mobile devices including mobile phones, smartphones, tablets, PDAs and digital cameras to staff to support mobile working. These are provided primarily for business use. Any installed antivirus software on your mobile device must not be removed as it is essential to counter the risk of connecting infected devices to the company network/services.

12.2 Anyone wishing to install any personal 'Mobile App' onto a NCH mobile device connected to NCH systems must consult ICT before doing so. The installation of an infected app can not only damage the device operating system but can potentially also lead to problems with any NCH IT systems that the mobile device connects to

12.3 Where a non-approved mobile app is required a request should be passed to ICT for a check of the app security and appropriateness for installing on a NCH smartphone.

12.4 Where any app conflicts, or may conflict, with mobile device security or system operation the ICT Team reserve the right to remove those apps.

12.5 If you stop using an app, remove it from your mobile device.

12.6 Mobile device costs are monitored and usage is automatically reported to senior managers for review. Cost for private calls, texts, e-mails and data usage remains an individual's responsibility to monitor and to reimburse NCH in the event of personal use.

12.7 Any mobile device must be returned to the ICT Team when instructed by your line manager or ICT Team. It must also be returned on change of job role where mobile devices are not required or on termination of employment with NCH.

13.0 Social Media

13.1 Reasonable personal use of the Internet is allowed under the rules given above and does include access to social media sites (e.g. Twitter and Facebook). Note however that the Company has a strict policy on the use of social media in connection with NCH business.

13.2 The company has comprehensive social media guidance (see 'Social Media Guidelines') which sets out every employee's responsibilities

and can be found within the Guidelines section in the Communications and Marketing area of the Intranet and reproduced below:.

Social Media Guidance for employees:

- Be aware of the need to use social media responsibly both in and outside of work.
- Anything you put online has the potential to be seen outside your immediate circle of friends or followers.
- Defamatory, offensive, obscene, libellous, discriminatory or harassing online behaviour is not acceptable – including on personal accounts.
- Making derogatory/negative comments about NCH, its staff or its customers will be treated as a potential issue of misconduct under the Disciplinary Procedure and may lead to action up to and including dismissal.
- Anything negative or damaging you say about NCH, its staff or its customers has the potential to be seen by your employers.
- Don't use social media during work hours for non-work purposes.
- Don't post any information that you've come by through the course of your work that may be personal or confidential.

13.3 All employees must maintain the standards expected of them and keep to their contractual obligations when in an online environment, just as they are expected to when representing the company at work and in the wider world.

14.0 GDPR and Data Protection Act 1998, 2018

14.1 All staff are responsible for information security and therefore must understand and comply with the NCH Data Protection Policy.

14.2 Data Protection guidelines, information and policy is available from the NCH website as a link on the 'About Us' page, currently the direct hyperlink is: Data Protection and Freedom of Information

15.0 Memory Stick usage

15.1 Appropriate use of ICT issued memory sticks is permitted (approval from your line manager required); these are pre-encrypted and password protected to provide the best level of protection for our data.

15.2 Encrypted memory sticks must be requested from ICT by the line manager of the intended recipient

15.3 Non ICT issued memory sticks (i.e. USB Drives) and other removable media for storing data must not be used with NCH equipment or with NCH data.

16.0 Non NCH computer equipment and / or mobile devices

16.1 At this time, NCH limits access to ICT systems to authorised individuals issued with NCH supplied desktop computers or laptops.

16.2 NCH allows personal smartphones and tablets of staff to be connected to NCH ICT systems in line with the requirements of company issued equipment.

Staff wishing to connect their devices to NCH systems must:

- Agree to all terms and conditions of this policy
- Ensure that access is made via the Mobile Device Management (MDM) application. This is offered to staff at no cost. Installation of MDM software will configure the device to require a PIN number and automatically lock after 5 minutes of inactivity
- Be responsible for ensuring that their personal device is backed up to prevent the loss of any personal data
- Be aware that NCH will not be responsible for the loss of any information resulting from the installation of this application
- Be aware that they remain responsible for the costs of calls/data used on their device, although access to wireless on enabled corporate sites will be offered at no cost

Connecting a personal device to NCH's Mobile Device Management service will enable ICT to make changes to the policy of your device. The software does not provide the capacity for ICT to:

- View any personal e-mail or SMS messages
- View personal files or photographs

Additionally, ICT will not use the ability to locate the device or wipe the device unless explicitly requested to do so or if there is a risk to the company.

NCH IT is not responsible for the configuration of any personal equipment or changes to these resulting from the connection to NCH's networks. It is the sole responsibility of staff to provide anti-virus protection, personal firewall protection and to configure their mobile device settings to provide the appropriate security settings to control access.

16.3 Access to Web-based services intended for external access such as Pentana, Microsoft Exchange Mail via Outlook Web Access; TP Tracker and ReACT. Access is allowed only according to the restrictions of this policy and staff accessing such systems outside the company network must not compromise the system or data security.

17.0 Recovery of Costs

17.1 Where members of staff deviate from this policy in any way that results in a financial loss to the Company, NCH reserves the right to recover such costs from an employee's salary.

18.0 Exceptions

18.1 Exceptions to this policy are by written agreement of the Director of Investment and Business Services and subject to annual review.

18.2 Changes to this policy are to be requested by formal application to and approval by the Director of Investment and Business Services.

19.0 Breach of this Policy

19.1 Any breach of this policy may be dealt with under the NCH Disciplinary Procedure and, in serious cases, may be treated as gross misconduct leading to summary dismissal

20.0 ICT SECURITY AND ACCEPTABLE USE POLICY SIGN-OFF

This Policy contains important information which is relevant to all employees. It is your responsibility to be familiar with the contents and comply with the policy. Once you have read and understood this Policy, please sign and return this slip to the ICT Team.

NCH provides equipment and systems to help colleagues with their work. This policy provides clear rules designed to protect Company, staff and customers.

I agree to comply with the terms of this policy governing the access to NCH systems and data. I understand that any breach of this policy could lead to action taken against me under the NCH Disciplinary Policy**.**

Print Name: _____ Signature: _____

Date: _____/_____/_____ Dept.: _____

Document Change History				
Date	**Issue No.**	**Section/Page**	**Details of Change**	**Authorised by**
Nov. 2012	1.4	All	Full Revision	Robert Barton
Nov. 2013	1.5	All	Review and update	Beth Lawton
Sept. 2016	1.6	All	Review and update	Phil Walker
Sept. 2016	1.7	All	Review and update	Robert Allen
Sept. 2016	1.8	Various	Updated with BID/ICT feedbac	Robert Allen
26/09/16	1.9	Section 11 – Email Policy	Added clause regarding staff photographs in emails – as per request from Head of O&D	Caroline Foster
29/09/16	2.0 draft	Highlighted sections	Added cameras/photography references. Incorporated final ICT Team feedback. Formatted to new company Procedure and Policy template	Robert Allen
13/10/16 to 7/11/16	3.2	various	Incorporated policy elements and other changes	PC
July 17	4b	Various	Feedback from stakeholders and corrections	FM/JS
August 17	4c	Various	Feedback and corrections	CD/JS
December 17	5	Various	Added BYOD, reviewed in line with NCC policies	Sue Smith