cadder
HOUSING ASSOCIATION

Policy Title: **Information and Communication Technology Policy**

Date Approved by Management Committee:

Approved: **23 August 2018**

Next Review Date: **August 2021**

This document will be made available in different languages and formats on request, including Braille and audio formats.

ENGLISH This information is available on request in other languages, in large print, in Braille and on audio format. If you would like this information in one of these formats please contact Cadder HA on **0141 945 3282**

POLISH Niniejsze informacje dostępne są na żądanie w innych wersjach językowych, dużym drukiem, językiem Braille'a oraz w formacie audio. Aby otrzymać powyższe informacje w jednym z wymienionych formatów, proszę skontaktować się z Zespołem ds. Cadder HA pod numerem telefonu **0141 945 3282**

FRENCH Ces informations sont disponibles sur demande dans d'autres langues, en gros caractères, en braille et en format audio. Si vous souhaitez obtenir ces informations dans l'un de ces formats, veuillez contacter Cadder HA au **0141 945 3282.**

هذه الـمعـلومة مـ توفـ رة تـ حت الـ طـ لب بـ لغات أخرى، بـ طـ باعة بـ أحرف CIBARA
آبـ يرة ، بـ طريـ قة بـ رايـ ل و عـ لى شريـ ط صوتـ ي. إذا آنـ ت تـ رغب فـ ي
الـ حـ صول عـ لى هذه الـ مـ علومة بـ أي من هذه الـ صـ يغ، الـ رجاء أن
ناكسإلل وكسالآ ةيعمج ةسايس قيرفـب لصتت Cadder HA
3282عـلى الـرقـم ***0141 945***

SOMALI Warbixintaan waxaa, haddii la dalbado lagu heli karaa luuqaddo kale, daabacaad weyn, Farta ay dadka indhaha la' akhriyaan (Braille) iyo qaab cajaladdo maqal ah. Haddii aad doonayso inaad warbixintan ku hesho mid ka mid ah qaababkaas, fadlan kala xidhiidh Kooxda Xeerarka ee Cadder HA telefoonka ***0141 945 3282***

rsiايـن مطالـب را مـی تـ وانـ يد بـ ه زبـ ان های ديـ گر، بـ ه شـكل چاپ بـ ا حروف درشت يـ ا aF
حروف بـ ريـ ل (بـ رای نـ ابـ يـنايـ ان) و بـ ر روی نـ وار صوتـ ی درخوا ست نـ مايـ يد. در صورتـ ی آه
مايل به دريافت اين مطالب به يكی از شكل های فوق هستيد لطفاً با دفت Cadder HA تماس
تـ لـ فن شماره .آنـ يد حا صل
0141 945 3282

RUSSIAN Данная информация может быть
предоставлена по требованию
на других языках, крупным шрифтом, шрифтом Брайля и в аудиозаписи.
Если вы хотите получить данную
информацию в одном из этих
форматов, обратитесь в Cadder HA по телефону ***0141 945 3282***

Information and Communication Technology Policy

Contents

ICT Policy

1.0 Introduction

1.1 This Information and Communication Technology (ICT) Policy details the rules for, and gives guidance to, staff on the use of electronic systems and media within Cadder Housing Association (the Association).

1.2 The Association depends fundamentally upon information that is stored and transmitted in electronic form. Much of this information is valuable or difficult to re-create. There is often an essential requirement for accuracy and instant availability of both the information and the systems that deliver it. Some types of data may also be sensitive for the Association, users, customers or business partners and the Association may be subject to contractual restrictions.

1.3 The failure to adequately protect these information assets can have an impact on business, customer satisfaction or market reputation. It is therefore imperative that staff take adequate steps to safeguard the Association's systems, networks and information.

1.4 Failure to comply with the ICT Policy is viewed extremely seriously and any such breaches are likely to be dealt with under the Association's Disciplinary Procedure. Serious breaches of the ICT Policy may result in dismissal.

2.0 Responsibilities

2.1 The Association is responsible for securing its facilities to a reasonable and economically feasible degree against unauthorised access and /or abuse. This responsibility includes informing users of expected standards of conduct and the resultant consequences of not adhering to them.

2.2 It is the responsibility of the Senior Staff Team to ensure that all staff within their department are aware of this policy. In addition, this policy should be covered, for new employees, at induction.

2.2 It is the responsibility of the Finance & Corporate Services Manager to ensure that the policy is kept up to date and to monitor staff's awareness of the policy.

2.3 Responsibility for the provision of appropriate equipment and its maintenance rests with the Finance & Corporate Services Manager.

2.4 Responsibility for the provision of a correct and safe environment for the storage and usage of ICT equipment rests with the Finance & Corporate Services Manager.

2.5 Responsibility for maintaining an appropriate data back-up strategy and disaster recovery procedures rests with the Finance & Corporate Services Manager.

2.6 Responsibility for insurance of all IT systems at an appropriate level rests with the Finance & Corporate Services Manager.

2.7 It is the responsibility of all staff to read and understand the requirements of this ICT Policy. In particular staff are asked to note that their use of the IT facilities and, in particular the internet and e-mail, may be monitored by the company from time to time using monitoring tools, techniques or applications. The company may retrieve the contents of messages for the purpose of: monitoring whether the use of the e-mail system is legitimate; or internet downloads to assist in the investigations of wrongful acts; or to comply with any legal obligation.

2.8 Staff will be required to agree to and sign the ICT Policy prior to being issued with access rights to IT systems.

3.0 Equipment and Software

3.1 Network

3.1.1 The Finance & Corporate Services Manager shall ensure that the Association's IT Service Provider provides effective management, maintenance and administration of the Association's IT hardware as outlined in the support contract and service level agreement.

3.1.2 Access to and usage of the Servers is restricted to authorised staff.

3.2 Hardware (PCs, Laptops, Notebooks, Printers, Modems, etc.)

3.2.1 The requirement for ICT equipment will normally be identified within the context of an ICT strategy, which will accompany the ICT policy for the Association. This strategy will outline the pro-active and planned replacement of equipment.

3.2.2 The Association's IT Service Provider will purchase, install, configure and maintain all computer equipment within the Association on the direction of the Finance & Corporate Services Manager . Staff members should not, without previous permission of the Director, Finance & Corporate Services Manager or the IT Service Provider, install or configure any hardware or software applications onto their PC.

3.2.3 All equipment purchased by the Association will meet all latest statutory regulations in relation to health & safety and security.

3.2.4 Computer equipment registers will be maintained by the IT Service Provider / Finance & Corporate Services Manager to ensure full tracking of equipment. The inventory will include details of the make, model, specification and serial number and, in respect of software, details of licence numbers and expiry dates. Details will also be held of the location and use of the equipment, the purchase date and warranty details.

3.2.5 In the event that any staff member requires new or replacement hardware they should present a report to the Finance & Corporate Services Manager detailing the business case for new or replacement hardware or software applications.

3.2.6 The deployment of new equipment or re-deployment of existing equipment is undertaken by the Director or Finance & Corporate Services Manager.

3.2.7 The relocation or disposal of hardware within or out with the Association will be decided by the Director or Finance & Corporate Services Manager. The Finance & Corporate Services Manager will ensure that computer equipment registers and insurance policies are updated accordingly.

3.2.8 The disposal of any IT equipment that may have held personal data must be disposed of by means that includes certified destruction of the hard drives/ data storage.

3.2.9 The security and safekeeping of portable and other equipment used out with the Association’s offices is the responsibility of the member of staff using it. In cases where sensitive or business-critical information is held on a laptop, tablet or mobile device adequate controls must be applied by the member of staff using the device to prevent unauthorised access, corruption or accidental loss of information. As a minimum devices should have PIN’s/passwords set to access them. Any personal data held on the device must be in keeping with the Association’s Data Protection and Privacy policies and must be password protected or encrypted.

3.2.10 All members of staff are responsible for the proper usage, care and cleanliness of the computer equipment they use. Section Managers should ensure that staff maintain the cleanliness of their machines.

3.2.11 Problems with hardware should be reported to the IT Service provider in accordance with the Service Level Agreement and agreed IT Help Desk procedures.

3.2.12 Only equipment and software approved for use by the Association is to be used by staff. All IT equipment supplied by the Association to staff for completion of their duties is approved for use. Any personal IT equipment or IT equipment not supplied through the Association must **not** be connected in any way to the Association's network or used for any Association work unless approval is given by the IT Service Provider and Director or Finance & Corporate Services Managers.

3.3 Software & Software Applications

3.3.1 The requirement for IT equipment will normally be identified within the context of an ICT strategy for the Association and more specifically within a planned software upgrade programme.

3.3.2 The IT Service Provider will purchase, install configure and support software and software applications used within the Associations network services. They will also support third party software suppliers and staff to install, configure and support software application used by the Association.

3.3.2 All software purchased by the Association will be properly licensed and purchased from reputable resellers.

3.3.3 Software, including screensavers, must not be installed by users without prior authorisation from the Finance & Corporate Services Manager or IT Service Provider. This includes programs downloaded from the Internet.

3.3.5 The Association will treat the installation of unlicensed software by users as a serious breach of the ICT Policy.

3.3.6 Software licence registers will be maintained by the IT Service Provider/Finance & Corporate Services Manager to ensure compliance with legislation.

3.3.7 Software disks will be kept securely in a safe by the Finance & Corporate Services Manager.

3.3.8 Requirements for new software/software applications should be discussed in advance with the Finance & Corporate Services Manager /IT Service Provider to assess the detailed specification and implications.

3.3.9 Problems with software should be reported to the ICT Service Provider or other support helpline as appropriate, e.g. the SDM Helpline.

3.3.10 Requests for modifications, enhancements and upgrades of existing software applications should be presented to the Finance & Corporate Services Manager in a report format detailing the business case for the request.

3.3.11 Unauthorised copying of software is not permitted.

3.4 Data/Electronic Information

3.4.1 Data Management should be in accordance with the current format of the server;

3.4.2 Section Managers are responsible for maintaining the format of the server relating to their section thus ensuring consistency and quality of the computer-held data processed by their staff.

3.4.3 The individual user is responsible to their line manager for the quality of the computer data they have personally processed.

3.4.3 Section Managers are responsible for ensuring compliance with Data Protection legislation and the Association's Data Protection Policy and Privacy Policy with regards to data processed within their Departments.

3.4.5 The Finance & Corporate Services Manager, in conjunction with the IT Service Provider, will keep abreast of data protection legislation, advise accordingly and ensure applications and databases are registered in accordance with the legislation and internal organisational data management policies.

3.4.6 All information/data held on the organisation's systems is deemed the property of Cadder Housing Association.

3.4.7 As a condition of employment, staff consent to the examination of the use and content of all data/information processed and/or stored by the staff member on the organisation's systems as required.

3.5 Back Up

3.5.1 The Finance & Corporate Services Manager is responsible for ensuring that the IT Service Provider implements an effective back-up strategy for server-held software and data. The Finance & Corporate Services Manager shall liaise with the IT Service Provider to ensure that any procedural requirements of the Association's staff are understood and adhered to.

3.5.2 Users of networked desktop PCs should not store data on their local hard drives. Data stored in this format may be lost if a problem develops with the PC, and the IT Service Provider may not be able to assist in its recovery. Data should be stored within the file directory (folder) structure used by the office.

3.5.3 Remote and laptop PC users must ensure they back up their data regularly. The IT Service Provider will provide advice and assistance.

3.6 Anti-Virus Protection

3.6.1 The Finance & Corporate Services Manager is responsible for ensuring the IT Service Provider provides an effective virus security strategy. All machines, networked and standalone, will have up-to-date anti-virus protection.

3.6.2 The installation of anti-virus software on all machines is the responsibility of the IT Service Provider.

3.6.3 The IT Service Provider will ensure the regular updating of the anti-virus software on networked desk-top PCs.

3.6.4 Remote users and users of portable machines will assist in the upgrade of anti-virus software in accordance with specified mechanisms agreed with the IT Service Provider, e.g. internet updates.

3.6.5 Staff should virus-scan all media (including zip disks and CDs) before first use. The IT Service Provider / Finance & Corporate Services Manager will provide assistance and training where required.

3.6.6 On detection of a virus staff should notify the IT Service Provider and the Corporate Services Officer who will provide assistance.

3.6.7 Under no circumstances should staff attempt to disable or interfere with the virus scanning software.

4.0 Computer Users

4.1 Health & Safety

4.1.1 Health and safety with regards to computer equipment and computer work stations should be managed within the context of the general and any specific Health & Safety policies and procedures within the Association. The Corporate Services Officer will provide advice.

4.1.2 The Section Managers are responsible for ensuring health & safety legislation and procedures with regards to computer equipment are implemented within their Departments.

4.1.3 The Finance & Corporate Services Manager, in close liaison with the IT Service Provider, will keep abreast of IT-related legislation and advise accordingly.

4.2 Training

4.2.1 It is the responsibility of Section Managers to ensure appropriate computer training for their staff is identified. The Corporate Services

Officer or IT Service Provider can advise on computer-related training issues.

4.2.1 Staff also have a responsibility to identify any training needs to their Section Manager informally or through their appraisal, which will form the individual staff' members training plan for the forthcoming year.

4.3 Passwords

4.3.1 The Finance & Corporate Services Manager will ensure password management is part of the ICT security strategy of the Association.

4.3.2 Users should change their passwords when prompted by the system in the case of networked machines or on a regular basis for standalone machines.

4.3.3 Staff are responsible for the security of their password which they should not divulge, even to colleagues. Staff are responsible for all use of IT systems under their own identity and should, therefore, take steps to protect their passwords from abuse by others.

4.3.4 Where access to any of the Association's systems is controlled by a password, it is forbidden to disclose the password to anyone else

4.3.5 Passwords must not be written down or transmitted by e-mail.

4.3.6 Problems with passwords should be reported to the IT Service Provider or Corporate Services Officer.

4.4 System Usage

4.4.1 Computers should be locked or shut down when left unattended for any significant period of time.

4.4.2 Staff must not attempt to "probe" the security of any system or network or to engage in any type of computer hacking activity, whether internal or external.

4.4.3 With regards to file management, Section Managers will determine the top-level folders/directories and associated permissions for their department and inform the IT Service Provider and Corporate Services Officer. The IT Service Provider will create or modify the folders accordingly.

4.4.4 Within their respective top-level folders, staff with agreement of their section manager or the ICT Working Group can create sub-folders to facilitate the storage of data. These sub-folders will ensure the storage of data pertaining to the relevant section and task of the Association, thus ensuring a consistency in the storage and accessibility of data. Staff cannot create new top-level folders.

5. ICT System Usage

5.1.1 E-Mail Usage

5.1.1 The Association's e-mail system is a core business application. It should not be used for political, business or commercial purposes not related to the Association.

5.1.1 The Association's e-mail system must not be used to send illegal, inappropriate or offensive material.

5.1.2 Limited personal use of e-mail is permitted. The IT Service Provider will monitor e-mail usage as appropriate to ensure there is no abuse of this privilege.

5.1.3 It is a condition of employment that all staff consent to the examination of the use and content of their e-mail accounts as required, including any personal e-mails on the system.

5.1.4 Staff are responsible for the general housekeeping of their e-mail account and should regularly delete out of date messages and correspondence that is no longer relevant. Folders should be set up and messages filed accordingly.

5.1.5 Staff should utilise the archiving facility within the e-mail system

5.1.6 Confidential material sent by e-mail should be so marked but sent only with caution. Any personal data sent by e-mail must comply with the Association's Data Protection and Privacy Policies and be securely password protected or encrypted.

5.1.7 Staff are not permitted to enable automatic forwarding of e-mail messages to another location out with the Association (e.g. Hotmail, Gmail etc.) without prior connect from their Section Manager.

5.1.8 Staff must ensure that an "out of office reply" is enabled if they are to be out of the office on annual leave or other planned absence. This should include dates of absence and alternative contact details in the event of an e-mail requiring urgent attention.

5.1.9 Staff should be aware that their e-mail may need to be accessed if they are absent from work, particularly if the absence is unexpected. Approval for access must be given by the Chair Person, Director or Finance & Corporate Services Manager before access of this nature is allowed.

5.1.10 All e-mail messages originating from the Association must include the Association's agreed e-mail signature, including address, registration numbers and disclaimer.

5.1.11 Personal e-mail websites (webmail) which may include Hotmail, yahoo, Gmail, excitemail and home accounts such as BTConnect, Sky, and Virgin must not be accessed via the Association's systems.

5.1.12 E-mail messages are more permanent and accessible than most people realise. E-mails should be treated in the same way as written material in that they may be accessible even when apparently deleted. The way in which the information in the Association's computer systems is archived or backed up means that even after a message has been deleted it can still be accessed. Therefore, all e-mail messages should be regarded as permanent documents.

5.2 Internet Usage

5.2.1 Access to the Internet is provided for business purposes. Limited personal use is permitted and is to be restricted to lunch breaks and periods out with working time, this is a privilege not a right.

5.2.2 Staff should not make inappropriate use of their access to the Internet for any purpose that may be detrimental to the Association's interests. This includes, but is not limited to, accessing pornographic, illegal or other improper material.

5.2.3 Staff should not access or subscribe to chat rooms, social networking sites, dating agencies, peer to peer file sharing services, messaging services or other on-line free, or subscription Internet sites unless they pertain to work duties, which in these cases should be approved by the Section Manager.

5.2.4 Programs and files, including items such as screensavers, emoticons and Google Earth, must not be downloaded from the Internet without authorisation from the Finance & Corporate Services Manager or the IT Service Provider.

5.2.5 The Association retains the right to monitor Internet usage by staff. This right is exercised through the IT Service Providers or Sectional Managers, Director or Chair Person.

5.2.6 It is a condition of employment that all staff consent to the examination of the use and content of their Internet activity as required.

5.2.7 Abuse of Internet access may result in disciplinary action with the outcome being the removal of the privilege of access from an individual's workstation or formal disciplinary action and, in situations of serious or gross misconduct, dismissal.

5.3 Wireless Access Policy

5.3.1 The Association provides Wireless Network facilities throughout its offices and Community Centre to compliment the hardwired structured cabling.

5.3.2 The Associations provides a Public and Private wireless network.

5.3.3 The Public Wireless network is available for use by individuals using their own personal ICT equipment and provides internet access only.

5.3.4 Individuals connecting to, or attempting to connect, personally-owned equipment to the Association wireless network do so at their own risk, The Association does not accept any responsibility for any loss or damage that may occur through the use of its Wireless Network facilities.

5.3.5 Due to the nature of wireless technology the Association cannot guarantee the security or privacy of any data transmitted over the wireless networks.

5.4 Telephone Policy

5.4.1 The Association provides telephony services for use by staff in support of its business activities. A limited level of personal use is also permitted as long as this does not conflict with normal work routines. However, users should note that personal use is a privilege not a right, and is dependent upon facilities not being abused or overused. Staff should also note that the use of the Association's telephone systems for personal commercial activity is not permitted under any circumstances.

5.4.2 The Associations reserves the right to monitor volume, duration and destination of all incoming and outgoing calls in support of the business interests of the Association and to investigate complaints.

5.4.3 Staff should be aware that there may be a requirement to check an individual's voicemail messages if they are absent, particularly if the absence is unexpected. Approval for access to an individual's voicemail must be given by the Chair Person, Director or Finance & Corporate Services Manager before this takes place.

6. Contravention of the ICT Policy

6.1 Staff should be aware of their responsibilities under the Data Protection Act, GDPR, Computer Misuse Act, Electronic Communications Act and the Copyright Design and Patents Act and other legislation as relevant. The Finance & Corporate Services Manager /IT Service Provider will provide guidance where required.

6.2 Contravention of the Association's ICT Policy or any act of deliberate sabotage to the Association's computer systems, information or data may be considered a disciplinary offence.

7. Auditing, Reporting & Review

7.1 Auditing

The Association with the support of our IT Service Provider monitor compliance with the ICT Policy. The Finance & Corporate Services Manager will meet regularly with the IT Service Provider to discuss all aspects of the ICT Policy, as well as progress with the ICT Strategy.

7.2 Committee

The Finance & Corporate Services Manager will report to the Audit and Performance Sub-Committee on current issues or developments with the ICT Policy or Strategy.

7.3 Staff

ICT needs and issues should be raised at Team Meetings, full staff meetings or directly with the Section Managers. All staff have a responsibility to report any known or suspected breach of the ICT Policy to their Section Manager or Director.

8. Agreement to Terms of Policy

8.1 All Staff are asked to sign to confirm that they have read, understood and will comply with the provisions of the Association's ICT Policy and any subsequent updates as approved and issued by the Association.

Signed:	
Name:	
Date:	