Ferguslie Park Housing Association

ICT Policy

Date Approved by the Management Board	22 May 2019	
	Signed:	Chairperson
Date of Next Review	May 2021	

Contents

1. INTRODUCTION

1.1 Ferguslie Park Housing Association Ltd (the Association) like any modern day organisation is information systems. In order to help maintain equipment, systems and data in a controlled and secure environment, there are a number of requirements which must be observed by all staff.

1.2 This document outlines the Association's security policy relating to the use of ICT equipment, networks and all related devices and software and is intended to:

a) Protect the organisation's information assets, hardware and software against unauthorised access, loss, theft, virus infection or hacking;

b) Protect the organisation from prosecution against the use of unlicensed or illicit software;

c) Ensure that controls exist regarding the purchase and disposal of hardware and software;

d) Ensure that all installations or amendments are carried out by authorised ICT support personnel; and

e) Protect authorised users from unintentional abuse of facilities by providing a formal document with which they should comply.

1.3 extremely dependent on the integrity, confidentiality, availability and accuracy of its data and This policy applies to all authorised users of the Association's ICT service, and is intended to highlight responsibilities in ensuring the security of its data and systems.

1.3. No unauthorised person, whether in the employee of the Association or not, shall be granted access to the organisation's ICT service.

2. CONSEQUENCES OF NON COMPLIANCE

2.1. Non-compliance with this policy is likely to compromise the integrity of data and information systems which would have a significant impact in the ability of the Association to perform its daily duties and may be subject to disciplinary action.

3. LINKS WITH OTHER POLICIES, PROCEDURES AND STRATEGIES

3.1. This policy references the Association's Privacy Policy and Equality and Diversity Policy.

4. EQUALITY IMPLICATIONS

4.1. The Association is committed to giving an equal service to all. Any action taken under this policy will comply with current equalities legislation.

4.2. Association staff will operate within the Equality and Diversity Policy and will seek to address any specific needs which may arise in respect of ethnic minorities, people with disabilities, and the elderly or vulnerable residents.

4.3. The Association will in all reasonable circumstances make information available in a variety of information formats, including: large print; audio tape; and community languages.

5. POLICY MONITORING

5.1. This policy will be monitored on a regular basis by the responsible officer to ensure it remains fit for purpose and reflects the practices of the Association and any changes in legislation. The policy will be formally reviewed and, if needed, updated every two years.

6. ACCESSIBILITY

6.1. A copy of this policy will be made readily available to all stakeholders:

a) Via email once per year

b) On the shared drive

c) On request from the Finance Department

7. SENIOR MANAGERS' RESPONSIBILITIES

7.1. Senior Managers are responsible for ensuring the proper use of the organisation's information assets and equipment, and for also enabling staff to receive appropriate and relevant training in order that:

a) Computer programs and data developed or purchased for the Association are used solely for carrying out its lawful activities. Unauthorised access to, copying, alteration, destruction or interference with computer programs or data is expressly forbidden;

b) Computer hardware and software is only to be used for purposes directly concerned with the organisation's activities and must not be taken off site without prior authorisation. Authorisation for home use to undertake official duties must be strictly controlled and be given only in circumstances which reflect the duties and responsibilities of the individual officer concerned;

c) Procedures designed for the security of data, programs or equipment must be followed;

d) Offices which house computer equipment must be adequately protected, and staff must play their part in following and monitoring the security procedures;

e) Computer hardware and software must be obtained in accordance with the organisation's Financial Regulations and must be assembled and tested by authorised personnel before use;

f) Disposal of ICT equipment must be carried out by ICT support staff with regard to the Waste Electrical & Electronic Equipment (WEEE) Directive;

g) Waste computer-printed output must be disposed of with due regard to its sensitivity. Confidential output must be shredded and/or destroyed by other appropriate, authorised means; and

h) All ICT equipment must be adequately insured.

8. EQUIPMENT & STORAGE

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

8.2. All software purchased by the Association will be appropriately licensed and purchased from reputable re-sellers.

8.3. The Finance and Corporate Services Manager will keep an inventory of all ICT equipment and software. The inventory will include details of the make, model, specification, serial number, location, warranty and intended use. In respect of software, details of licence numbers and expiry dates will also be held.

8.4. All equipment will be labelled and audited periodically. These labels must not be removed.

8.5. Where possible, equipment should only be placed in areas which are not accessible by members of the public unless suitable arrangements have been made. In offices that are more accessible to the public, windows and blinds should be shut outside office hours and screens positioned so that the screen contents cannot be viewed.

8.6. All mobile or portable devices owned by the Association will be deployed with additional security and controls to avoid obvious risks to the data. These services must not be disabled or altered in any way.

8.7. Any device not owned by Association may be used in relation to Association duties, but must be authorised in advance by the Chief Executive.

8.8. Laptops and other portable mobile devices should be locked away when not in use and must not be left unattended in vehicles or public places. When being transported outside the office, such equipment must be transported as part of hand luggage at all times. Data which is to be held on laptops or other portable devices should be risk assessed and appropriate security measures employed.

8.9. All servers will be located in a lockable cabinet. The Finance and Corporate Service Manager and Chief Executive will be responsible for access to the server environment when needed.

8.10. All ICT equipment will be inspected on a regular basis to ensure that it is operational and does not present an obvious hazard. Portable Appliance Testing will be completed in accordance with statutory regulations.

8.11. Where any ICT equipment is found to be unsafe or inappropriate for its designated use it will be removed from its location, and if appropriate replaced.

8.12. Only equipment and software approved for use by the Association is to be used to access ICT services. Any ICT equipment not supplied by the Association must not be connected in any way to the organisation's ICT infrastructure unless approved in advance by the Chief Executive.

8.13. All equipment that does not require being operational out with working hours is to be switched off when not in use, particularly at the end of each working day or when the device is not used for a significant period of time.

8.14. Non employees of the Association are not permitted to use any of the organisation's ICT equipment unless authorised. Where authorised, they will be given temporary access to complete the tasks required assuming suitable advance notice is given.

8.15. Users accessing the Association's systems remotely from their own equipment are responsible for ensuring that they have up to date anti-virus protection on personal equipment.

8.16. Users of removable storage media such as usb memory sticks, must appreciate the high security risk they represent and must limit usage to those times when no other method of storage or transportation of data is available.

8.17. Staff using removable storage media to transfer data must ensure that:

a) It is the most appropriate transfer method;

b) They are able to demonstrate that the security of the media and the integrity of the data are maintained;

c) It does not contravene any legislation, policies or good practice requirements; and

d) Suitable encryption technologies are employed.

9. DATA ACCESS

9.1. All staff will be given access to the data files that they need to complete their duties. It is the responsibility of all staff to ensure that they only access data relevant to their needs.

9.2. All users will access data by using a unique user account name and password. These account names and passwords are unique to individuals and all passwords must remain confidential. Under no circumstances must employees share their password with any other employee or third party.

9.3. The Association's network support providers will be responsible for ensuring that all users have an appropriate user account name and password which will be subject to a regular audit.

9.4. Passwords will be a minimum of five characters in length and must include upper case, lower case and at least one numerical character. Good practice for selecting a password would be:

a) Be as long as possible;

b) Include mixed-case letters;

c) Include at least one digit;

d) Include special characters such as punctuation marks, if possible; and

e) Not be based on any personal information (e.g. birthday).

9.5. All accounts will be forced to change their password every 42 days.

9.6. Any loss of access device, breaches or attempted breaches of security must be reported to the Chief Executive by the registered user of the device.

9.7. Industry standard routines will be implemented to ensure security of the organisation's data from external sources.

9.8. Users accessing data via the Internet must ensure compliance with the Internet and E-mail usage section of this policy.

9.9. Confidential or sensitive information should not be supplied to anyone outside of the Association without good reason and approval of the Chief Executive. Any such information removed from the office for any reason, regardless of format or electronic medium, must be properly returned as soon as possible. Responsibility for information away from the office rests with the employee using the information.

9.10. All employees will be required to read and accept the content of this policy prior to being given access to systems and data.

9.11. The Association's support providers must be notified of all new employees, terminations and situations where system access will be affected with a change of post. Necessary steps will then be taken to remove or amend the employee's rights to relevant systems.

9.12. Unattended ICT equipment should be locked to prevent unauthorised access when away from the desk. When leaving the building you must log out of the device, or at the end of the working day, switch the device off.

10. DATA SECURITY

10.1. Any information held within any ICT system or stored on a device owned by the Association is deemed to be the property of the Association.

10.2. All data should be stored on the appropriate network servers. Responsibility for ensuring the safety and integrity of this data rests with the IT support providers. Where data is stored locally (which should only be when a valid business case exists), responsibility for ensuring the safety and integrity of the data rests entirely with the user.

10.3. All data will be secured in accordance with the Association's Backup and Disaster Recovery strategies.

10.4. Under no circumstances should any software be installed by any person other than authorised personnel. Any need for additional software must be requested through the Chief Executive

or Finance and Corporate Services Manager for consideration and if approved, will be recorded, tested and installed in accordance with best practice.

10.5. No copies of data, or software, should be made unless specifically authorised by the Chief Executive and must always be in accordance with the backup / disaster recovery strategies.

10.6. No details of how the ICT systems operate are to be given to non-employees of the Association without the approval of the Chief Executive.

10.7. All data processed and stored within the organisation's ICT system may be subject to scrutiny for its intended use, and content, as required.

10.8. Good housekeeping procedures should be utilised whenever possible, for example, control over email retention, managing the number and relevance of stored documents, etc.

10.9. Any subject access request which requires the disclosure of information held within the ICT systems, may only be authorised by the Chair of the Board or the Director. This request must be made in writing.

11. EMAIL & INTERNET USE

11.1. The primary purpose of E-mail and Internet access is to encourage greater business efficiency and to enhance knowledge, learning and communication opportunities for the organisation as a whole and its people as individuals.

11.2. E-mail is provided primarily for business use. Although email facilities can be used for personal reasons, such use should be kept to a minimum and any such use is subject to the detail within this policy.

11.3. ASSOCIATION provides E-mail to support its main business activities. Accordingly, all email on the organisation's ICT systems remains the property of the Association. The organisation reserves the right to access and interrogate any email or account in use by an individual.

11.4. An individual must not attempt to gain access to systems for which they are not authorised or to access another person's e-mail, regardless of whether those e-mails contain personal information.

11.5. Only properly licensed software purchased by Ferguslie Park Housing Association will be used to access E-mail and the Internet.

11.6. Employees should limit access to personal E-mail addresses (e.g. Hotmail accounts) via the organisation's systems to minimise risk of virus attack.

11.7. All relevant UK, European and International laws in place govern all usage of E-mail and Internet at the time of usage.

11.8. Staff who have access to an E-mail account should use the following general guidelines when using E-mail either externally or internally:

a) Check E-mail regularly, at least twice each day when in the office;

b) Treat external E-mail in the same way as normal written correspondence;

c) Confidential information should not be transmitted externally by E-mail unless absolutely necessary and appropriate encryption methods are used. The recipient of such an email must be made aware of the fact that information supplied is confidential;

d) Avoid sending excessively large E-mails or attachments wherever possible. Where large attachments are unavoidable, such files should be compressed using the appropriate compression software; and

e) All E-mail messages should contain the name of the officer, current job title and contact number.

11.9. To minimise the risk of litigation against the Association, the following rider will be automatically placed in the signature block of all outgoing E-mails:

"This message may contain confidential information intended only for the addressee named above. If you are not the intended recipient of this message, you are hereby notified that any further use of this message is prohibited and you are requested to notify Ferguslie Park Housing Association Ltd immediately. Any views expressed in this message are those of the individual sender and may not necessarily reflect the views of Ferguslie Park Housing Association Ltd.

Ferguslie Park Housing Association Limited is a Registered Scottish Charity – No SC0034893

11.10. The following will be considered improper use of the E-mail system. This list is not exhaustive:

a) Sending potentially defamatory E-mail messages that criticise other individuals or organisations;

b) Sending inappropriate messages including those that are sexually harassing or offensive to others on the grounds of age, physical ability, race, religion or gender irrespective of the legality of material in the country of origin;

c) Forging messages, deleting, copying or modifying the electronic messages of others;

d) Forwarding chain letters or sending unsolicited mail which would interfere with proper mail delivery;

e) Using the E-mail system for commercial or private business purposes; and

f) Sending or receiving illegal material, which may constitute a criminal offence.

11.11. Access to the Internet should, in the main, be limited to those pages that are relevant to a person's job. While limited private use is permitted, excessive use may lead to this privilege being withdrawn.

11.12. In the event that an individual accidentally finds themselves in an inappropriate website, this must be reported to a line manager immediately.

11.13. Staff should take care not to infringe copyright when downloading material or forwarding it to others. If unclear as to whether material is subject to copyright, permission should be sought from the site author/owner before downloading.

11.14. Staff should not access or subscribe to any site or service which could present a risk to the integrity of the ICT infrastructure or its data.

11.15. Improper use or abuse of internet access or email services could result in disciplinary action.

12. MOBILE PHONES

12.1. Where a mobile phone has been issued to enable an officer to undertake their daily duties, personal call usage will be permitted, but should be kept to a minimum. Excessive use, unless agreed by a line manager, may lead to disciplinary action.

12.2. Smartphones should be considered to be mobile computers and, as such, will be subject to the same conditions as any other device as outlined in this policy.

13. DATA PROTECTION

13.1. The Association complies fully with the provisions of the Data Protection Act 1998 and intends to comply with any additions/replacements to this Act and other relevant legislation including GDPR.

13.2. All employees and users of data, whether from manual records or from ICT systems, will adhere to the provisions of the legislation.

13.3. Personal data relating to customers, clients or employees of the Association should not be transferred to systems or equipment that does not belong to the organisation without the express written consent of either of the nominated data protection officers or the Chief Executive. Where data is transmitted at regular intervals, and there is no change to the data template, the initial consent will indicate and allow for the repeat transmissions. However, if the data template requires amendment, a new consent will be required.

13.4. All personal data relating to customers, clients or employees will be kept up to date at all times and be relevant for the purpose obtained. Any personal data which is no longer relevant should be permanently destroyed in line with the organisations Privacy Policy.

13.5. No external person is to be given access to any personal data without proper authority.

13.6. Full details of the Association's guidance on privacy can be found in its Privacy Policy.

14. COMPUTER VIRUSES

14.1. No programs or files should be loaded onto any device except by authorised ICT support personnel.

14.2. It is recognised however that, on occasion, files will need to be transferred to storage media and where relevant, these should be virus checked first.

14.3. Anti-virus software is installed on all workstations, portable devices and servers throughout the organisation.

14.4. All files introduced to the organisation's system are automatically scanned and any infected files are quarantined until investigated further.

14.5. A full scan of all local hard drives on all workstations and servers is scheduled weekly. Any workstation not switched on at the time of the scan will be scanned on the next occasion that the workstation is switched on.

14.6. Anti-virus software updates are received automatically and will be applied automatically.

14.7. Any users suspecting a virus infection on their workstation must report the situation immediately to the Chief Executive and must not continue to use the workstation until the issue has been resolved.

14.8. Any concerns about software or emails on any machine should be reported to the Chief Executive.

14.9. Under no circumstances should any attempt be made to disable the anti-virus software on any hardware.

15. EXTERNAL ACCESS TO THE NETWORK

15.1. External access to the Association's ICT service will be monitored by the IT support providers and authorisation to such access must be given by the Chief Executive prior to the granting of access.

16. AUTHORISED FILES AND PROGRAMS

16.1. In order to ensure that all software programs and files in use throughout the organisation are legitimate and non-malicious, no software should be installed on any device except by authorised ICT personnel.

16.2. The copying of software is strictly controlled under the software licensing agreement and by the Computer Misuse Act 1990. Under no circumstances should software be copied except by ICT personnel who will undertake this function to ensure licence agreements are adhered to and necessary security copies of the product exist.

17. PERSONAL USE

17.1. Personal use of the organisation's equipment for non-work related activities, exclusive of Internet access, is not permitted unless sanctioned by the Chief Executive.

17.2. Personal use of the organisation's Internet facility is permitted subject to the following rules:

a) Personal Internet usage is in an employee's own time (e.g. lunch break);

b) An individual may not access or subscribe to any non-job related Internet service using corporate credentials; and

c) An individual may not use the organisation's systems to transfer, store or download information or files for personal use.

17.3. In the event of non-compliance with the ICT policies in effect, or if personal use is deemed to exceed an acceptable level of use, disciplinary action may be instigated.

18. INCIDENT REPORTING

18.1. All users are required to report any and all information system security breaches, or ICT incidents, as soon as possible to a line manager and the Director.

18.2. Examples of ICT Security breaches include:

a) Breaches of physical security e.g. unauthorised persons accessing a secure area;

b) Access control violations e.g. person attempting or gaining access to systems or facilities to which they should not have access;

c) Non-adherence to ICT Security Policy or associated policies and guidelines;

d) IT equipment theft or loss;

e) Loss of information assets e.g. maliciously deleted data;

f) Disclosure of sensitive data e.g. loss of removable media; and

g) Virus infection.

19. DISCIPLINARY ACTION

19.1. Misuse of computer hardware and software is considered a very serious matter. Disciplinary action will, when appropriate, be taken against employees who contravene this policy and could, in certain circumstances, include dismissal. Furthermore, misuse of computer programs or data, including unauthorised access to data, could lead to prosecution under the Computer Misuse Act 1990 or the Data Protection Act 1998.

20. GENERAL

20.1. All identity cards, keys, manuals and equipment must be returned to the Chief Executive or Finance and Corporate Services Manager upon termination of employment with the Association.

20.2. When staff change post within the organisation, a review should be undertaken by the line manager to establish if items of equipment, identity cards, etc. need to be returned and to discern if access rights need to be amended.

20.3. Periodic checks may be made by Internal Audit personnel to ensure compliance with these rules.

20.4. The requirements contained in this policy statement are of a general nature covering all computer equipment; there may be additional requirements designed for specific locations, data or applications.

20.5. Any questions regarding computer security in general should be addressed to the Chief Executive.