Drumchapel Housing Co-operative Limited

INFORMATION TECHNOLOGY CYBER SECURITY POLICY

Purpose:	To ensure that all the information systems which the Co-operative manages are protected from security threats and to mitigate risks that cannot be directly countered
Date:	26 November 2019
Review Date:	December 2019
Regulatory Standards:	Standard 2 – The RSL is open and accountable for what it does. It understands and takes account of the need and priorities of its tenants, service users and stakeholders and its primary focus is the sustainable achievement of these priorities. Standard 3 – The RSL manages its resources to ensure its financial wellbeing and economic effectiveness. Standard 5 – The RSL conducts its affairs with honesty and integrity.
Committee Approval:	28 January 2020

CONTENTS **PAGE NO.**

1. INTRODUCTION

1.1 The continued confidentiality, integrity and availability of information systems underpin the operations of Drumchapel Housing Co-operative.

1.2 A failure to secure information systems would jeopardise the ability of the Co-operative to fulfil its aims and objectives providing effective services to tenants and customers.

1.3 This Information Systems Cyber Security Policy provides the guiding principles and responsibilities of all members of staff of the Co-operative required to safeguard its information systems.

2. PRINCIPLES

2.1 This policy will be operated within the following principles:

- Be clear and understood by all employees
- Be fair, equitable and non-discriminatory
- Reflect statutory requirements and best practice
- Be flexible and adaptable to changing needs
- Apply to all employees and Committee Members

3. POLICY OBJECTIVES

3.1 The objectives of the policy are to:

- Ensure that the information systems which the Co-operative manages are protected from security threats and to mitigate risks that cannot be directly countered
- Ensure that all members of staff are aware of and fully comply with the relevant legislation as described in this and other policies
- Describe the principals of security and explain how they shall be implemented in the organisation
- Introduce a consistent approach to security, ensuring that all members of staff fully understand their own responsibilities
- Create and maintain, within the Co-operative, a level of awareness of the need for Information Security as an integral part of the day to day business
- Protect information assets under the control of the organisation

4. RESPONSIBILITIES FOR INFORMATION SECURITY

4.1 Ultimate responsibility for information security rests with the Depute Director.

4.2 Employees and contractors should be aware of:

- The information cyber security policy
- Their personal responsibilities for information security

- How to access advice on information security matters

4.3 All employees shall comply with information security procedures including the maintenance of data confidentiality and data integrity. Failure to do so may result in disciplinary action.

4.4 Each member of staff shall be responsible for the operational security of the information systems they use. By accepting an account password, related information and accessing the Co-operative's Network or Internet system, an employee agrees to adhere to the Co-operative's policies regarding their use.

5. E-MAIL PROCEDURES

5.1 The Co-operative's e-mail system is designed to improve service to our customers, enhance internal communications and reduce paperwork. Employees using the Co-operative's e-mail system must adhere to the following policies and procedures:

- The Co-operative's e-mail system, network (including wireless) and Internet access are intended for business-use only. Employees may access e-mail and the Internet for personal use only during non-working hours and strictly in compliance with the terms of this policy.

- All information, created, sent or received via the Co-operative's e-mail system, network or Internet including all e-mail messages and electronic files, is the property of Drumchapel Housing Co-operative. Employees should have no expectation of privacy regarding this information. The Co-operative reserves the right to access, read, review, monitor, copy all messages and files on its computer system at any time and without notice. When deemed necessary, the Co-operative reserves the right to disclose text or images to law enforcement agencies or other third parties without the employee's consent.

- Use extreme caution to ensure that the correct e-mail address is used for the intended recipient(s)

- Any message or file sent via e-mail must have the employee's name attached

- Personal e-mail accounts are not permitted unless expressly authorised in advance by the Depute Director

- Alternate Internet Service Provider connections to the Co-operative's internal network are not permitted unless expressly

authorised by the Co-operative and properly protected by a firewall or other appropriate security device(s) and/or software

- Employees must provide the System Administrator with all passwords

- Only authorised staff members are permitted to access another person's e-mail without consent

- Employees should exercise sound judgement when distributing messages. Tenant-related messages should be carefully guarded and protected. Employees must also abide by copyright laws, ethics rules and other applicable laws

- E-mail messages must contain professional and appropriate language at all times. Employees must not send abusive, harassing, intimidating, threatening and discriminatory or otherwise offensive messages via e-mail. Sending these types of e-mails may result in disciplinary action up to and including termination of employment.

- Employees should archive messages to prevent them from being automatically deleted. All messages archived in the Co-operative's computer system shall be deemed Co-operative property, as is all information on the Co-operative's systems.

- Misuse and/or abuse of electronic access, including but not limited to, personal use during working hours, copying or downloading copyrighted materials, visiting pornographic sites or sending abusive e-mail messages may result in disciplinary action, up to and including termination of employment.

- Use of the Network and the Internet is a privilege, not a right. Use of the Network and Internet access extends throughout an employee's term of employment, providing the employee does not violate the Co-operative's policies regarding this.

6. CONTENT AND COMMUNICATIONS

6.1 The Co-operative, at its sole discretion, will determine what materials, files, information, software, communications and other content and/or activity will be permitted or prohibited.

7. PRIVACY

7.1 Network and Internet access is provided as a business tool for the Co-operative. The Co-operative reserves the right to monitor, inspect, copy, review and store at

any time, without prior notice, any and all usage of the Network and the Internet, as well as any and all materials, files, information, software, communications and other content transmitted, received or stored in connection with this usage. All such information, content and files are the property of the Co-operative. An employee should have no expectation of privacy regarding them. The Network Administrator may review files and intercept communications for any reason, including but not limited to maintaining system integrity and ensuring employees are using the system consistently with this Policy and prevent misuse or overuse.

8. DOWNLOADED FILES

8.1 Files should not be downloaded from the Internet without the prior authorisation of the Depute Director. Employees should note that information obtained from the Internet is not always reliable and should be verified for accuracy before use.

9. CONFIDENTIAL INFORMATION

9.1 Employees may have access to confidential information about the Co-operative, other employees, tenants and Committee Members.

9.2 With the approval of the Depute Director, employees may use e-mail to communicate confidential information internally to those with a need to know. Such e-mails must be marked 'Confidential'.

10. PROHIBITED ACTIVITIES

10.1 Employees are prohibited from using the Co-operative's e-mail system, network or Internet access for the following activities:

- Downloading software without the prior written approval of the Depute Director
- Printing or distributing copyrighted materials. This includes, but is not limited to, software, articles and graphics protected by copyright.
- Using software that is not licensed by the manufacturer or approved by the Co-operative.
- Sending, printing, or otherwise disseminating the Co-operative's data or any other information deemed confidential by the Co-operative to unauthorised persons.
- Operating a business, soliciting money for personal gain or otherwise engaging in commercial activity outside the scope of employment
- Making offensive or harassing statements based on race, colour, religion, origin, disability, age, sex or sexual orientation.
- Sending or forwarding messages containing defamatory, obscene, offensive, or harassing statements.

- Sending or forwarding a message that discloses personal information without Co-operative authorisation.
- Attempting to access or visit sites featuring pornography, terrorism, espionage, theft or drugs.
- Using another employee's password or impersonating another person while communicating or accessing the Network or Internet.
- Introducing a virus, harmful component, corrupted data or the malicious tampering with any of the Co-operative's computer systems

11. SOFTWARE

11.1 Software piracy is both a crime and a breach of the Co-operative's policy. Employees should use software strictly in accordance with its license agreement. Unless otherwise provided in the license, the duplication of copyrighted software (except for backup and archival purposes by designated employees) is a breach of copyright law. To ensure compliance with software license agreements, employees must adhere to the following:

- Employees must use software in accordance with the manufacturer's license agreements. Employees should not make additional copies of software. The only exception would be a single copy, as authorised by the Depute Director, for backup or archival purposes.
- The Co-operative does not permit the unauthorised duplication of software. Employees illegally reproducing software may be subject to disciplinary action.
- Any employee who knowingly makes, acquires or uses unauthorised copies of computer software licensed to the Co-operative or who places or uses unauthorised software on the Co-operative's premises or equipment shall be subject to disciplinary action, up to and including termination of employment.
- Employees are not permitted to install their personal software onto the Co-operative's computer system. Employees are not permitted to copy software from the Co-operative's computer system for installation on home or other computers without prior authorisation.
- In cases of homeworking, the Co-operative will purchase an additional copy or license. Any employee issued with an additional copy of software for home use acknowledges that such additional copies or licenses purchased for home use are the property of the Co-operative.
- Employees are not permitted to give software to tenants, contractors and other persons not employed by the Co-operative.

- Employees who suspect or become aware of software misuse are required to notify the Depute Director immediately.
- The Co-operative shall use software countermeasures and procedures to protect the organisation against the threat of malicious software. Users breaching this requirement may be subject to disciplinary action.

12. SOCIAL MEDIA

12.1 Employees should be aware that the Co-operative may observe content and information made available by employees through social media. Employees should use their best judgement in posting material that is neither inappropriate nor harmful to the Co-operative, its employees or customers.

12.2 Employees are not permitted to publish, post or release any information that is considered confidential or not public.

12.3 Social media networks, blogs and other types of online content sometimes generate press and media attention or legal questions. Employees should refer these enquiries directly to the Depute Director.

12.4 Employees should receive permission before referring to or posting images of current or former employees, tenants or contractors. Additionally, employees should get appropriate permission to use a third party's copyrights, copyrighted material, trademarks or other intellectual property.

12.5 Any 'after-hours' online activity that breaches the Co-operative's Code of Conduct or any other policy may lead to disciplinary action.

12.6 If employees publish content 'after-hours' that involves work or subjects associated with the Co-operative, a disclaimer should be used, such as *"The postings on this site are my own and does not necessarily represent the Co-operative's position or opinion".*

12.7 Employees should regularly check the privacy settings on their social networking profiles, as these can change.

12.8 If an employee is representing the Co-operative online by Blogging and Tweeting, appropriate rules e.g. relevant legislation on copyright and public interest disclosure should be adhered to in relation to what information they may disclose and the range of opinions they may express.

13. USER MEDIA

13.1 Removable media of all types that contain software or data from external sources, or that have been used on external equipment, require the approval of the Depute Director before they may be used on any Co-operative system. Such media must also be fully virus checked before being used on the organisation's equipment. Users breaching this requirement may be subject to disciplinary action.

14. MONITORING SYSTEM ACCESS AND USE

14.1 An audit trail of system access and data use by staff shall be maintained and reviewed on a regular basis.

14.2 Backups are run daily and monitored by Nevcom/Brightridge. Any problems or issues are notified immediately to the Co-operative along with our IT support consultant.

14.3 Access to databases are secured by logon security and file/folder access security.

14.4 In addition, the third party suppliers have additional logon security to access the databases through their software.

14.5 Security event logs can be monitored and reported as required.

15. MOBILE/SMART PHONE, TELEPHONE, AUDIO AND ELECTRONIC EQUIPMENT

15.1 Employees should not however use work time for personal purposes, on their own mobile phones to receive or make texts or calls. Any such communication should be made during authorised breaks.

15.2 Notwithstanding the above, the Co-operative accepts that there may be the need for some personal consultations and appointments to be made or received during the working day where it is not practical for them to be made at other times.

15.3 The use of audio devices, music players, games players or other electronic devices not authorised for use by the Co-operative is strictly forbidden.

16. CONTROLS

16.1 The Administrator shall be responsible for the information security of each IT asset (hardware, software, application or data).

16.2 Only authorised staff who have a justified and approved business need shall be given access to restricted areas containing information systems or stored data.

16.3 Access to computer facilities shall be restricted to authorised users who have a business requirement to use the facilities.

16.4 Access to data and system utilities shall be managed and restricted to the IT Administrator.

16.5 Locally stored backups are on a secure network storage drive in the Co-operative's server room. These stored files will be additionally password protected.

17. BUSINESS CONTINUITY AND DISASTER RECOVERY PLANS

17.1 The Co-operative shall ensure that business impact assessment, business continuity and disaster recovery plans are produced for all mission critical information, applications, systems and networks.

17.2 Cloud backups [through the Shadow Protect system] will be sent, fully encrypted to secure cloud storage where they will be available for business continuity in the event of fire, theft etc.

18. MALWARE AND TECHNICAL INTRUSIONS

18.1 The Sophos suite of applications will include web filtering, monitoring and reporting as well as real time malware and antivirus protection to protect the Co-operative.

19. INFORMATION SECURITY AWARENESS TRAINING

19.1 Information security awareness training shall be included in the staff induction process.

19.2 An ongoing awareness programme shall be established and maintained in order to ensure that staff awareness is refreshed and updated as necessary.

19. REVIEW

19.1 The effectiveness of this policy will be monitored on an ongoing basis and will be reviewed as appropriate, or according to statute and no later than 3 years from the date of implementation.

Lack of review will not cause the policy to lapse.

This policy is non contractual, and the Co-operative reserves the right to alter or withdraw it at any time.

20. GDPR Privacy Statement

20.1 The Co-operative will gather and use certain information about individuals in accordance with GDPR. Staff members have a responsibility to ensure compliance with the terms of the privacy policy and to collect, handle and store personal information in accordance with relevant legislation. The Fair Processing Notice (FPN) details how personal data is held and processed with third parties in accordance with relevant policies and procedures.