IT Security Policy

Dalmuir Park Housing Association

Your Future Our Future

Dalmuir Park Housing Association can provide this document on request, in different languages and formats, including Braille and audio formats.

Purpose:	To establish DPHA's policy and set out our position on IT security.
Guidance:	ICO - A practical guide to IT security
Policy complies with the following Regulatory Standards:	4. The governing body bases it decisions on good quality information and advice and mitigates risks to the organisation's purpose. 4.1. The governing body ensures it receives good quality information and advice from staff and, where necessary, expert independent advisers, that is timely and appropriate to its strategic role and decisions. The governing body is able to evidence any of its decisions.
Policy is linked to the following DPHA policies:	Staff and Committee Code of Conduct Communication Tools Disposal of Assets (non-housing) Homeworking Data Protection Policy Major Incidents and Business Continuity
Date policy last reviewed:	26 August 2020
Date approved by Board of Management (or PRWG if delegated):	26 November 2024
Date policy is next due to be revised:	November 2027
Equality Impact Assessment carried out for policy?	Yes
Publish on the Website	No

CONTENTS **PAGE NO.**

LIST OF APPENDICES

1.0 INTRODUCTION

1.1 The purpose of this policy is to protect the integrity of Association resources and the users against unauthorised or improper use. Information security management enables information to be shared, while ensuring the protection of information and computing assets.

1.2 The management of the Association will ensure that the appropriate infrastructure and resources are available for the implementation and ongoing review of security policies and procedures. Security procedures and systems will be closely monitored, and appropriate action will be taken in the event of any breach of security. Regular audits will be undertaken to ensure compliance with any security policies and procedures implemented. Failure to comply with this policy may result in disciplinary action being taken.

2.0 AIMS OF THE POLICY

2.1 The aims of this policy are to:

- Ensure confidentiality and protect sensitive information from unauthorised disclosure or intelligible interception
- Ensure the integrity and safeguarding the accuracy and completeness of information and computer software
- Ensuring that information and vital services are available to users when required

3.0 LEGAL AND REGULATORY REQUIREMENTS

3.1 DPHA is obliged to abide by all relevant UK and European Union legislation. This requirement devolves to the employees and agents of the Association who may be held personally responsible for any breaches. These include:

- The Data Protection Act 2018
- Copyright, Designs and Patents Act 1988
- The Computer Misuse Act 1990
- Health and Safety at Work Act 1974

4.0 GENERAL

4.1 This security policy is applicable to all existing and proposed systems and is effective from the date of issue. The employee responsible for each system must ensure that all risks are identified, and all reasonable measures taken to avoid security breaches.

4.2 The Association's policy is to ensure that IT systems, including computer systems, network components and electronic data, are adequately protected from a range of threats. The policy covers all aspects of the IT environment: systems, administration systems, environmental controls, hardware, software, data and networks. It will apply

to all stages of the system lifecycle, from feasibility to operation and is independent of whether the system is developed in-house or purchased externally. Risk analysis should be performed on a regular basis to ensure that the security measures in place continue to minimise threat, especially at times of change to the IT systems or surrounding environment. It is also the aim of this policy to ensure that all relevant legal and contractual obligations are fulfilled.

5.0 SCOPE

5.1 It is the responsibility of all personnel to ensure that the security policy is observed and the requirements of the security policy are mandatory wherever they are applicable. This policy applies to all users of the Association's IT systems, whether or not they are staff members, and irrespective of their location. Any suspected breaches of security must be notified using the notification procedure contained within this policy.

6.0 MAIN AREAS OF SECURITY

6.1 Physical Security

6.1.1 The physical siting of IT equipment needs to be planned with due regard to health and safety and security considerations. The working environment must be maintained in conditions, which continue to satisfy standards of physical security and prevent deterioration from occurring.

6.2 Physical Access

6.2.1 Sensitive IT areas must be protected by security locked doors, which require special keys or security codes to open. Only authorised personnel have access to sensitive areas. Procedures should be in place to control the access of external personnel (e.g. maintenance engineers). Any confidential material should be held in secure cabinets, even within IT secure areas, accessible only to authorised people.

6.3 IT System Access

6.3.1 The Association recognises the value of the information contained within its IT systems and will not tolerate unauthorised use. The policy applies both to employees of the Association who may use resources to which they are not entitled and to people external to the Association who may wish to gain access to our systems.

6.3.2 It is a criminal offence for an unauthorised person to attempt to access a system or information within systems or to attempt to exceed the computer facilities and privileges granted to them. The Association will assist in the prosecution of anyone committing an offence as documented within the Computer Misuse Act 1990.

6.3.3 Those who are granted access to our systems may not transfer any or all of these rights to a third party, for example by disclosing password information. Access to DPHA systems must be approved by the Finance & Corporate Services Manager and in their absence another member of Leadership Team.

6.4 **Unauthorised Software**

6.4.1 The Association is committed to the use of only authorised software within it's computer systems. No software may be loaded onto Association computers or network without the prior authorisation of the Chief Executive. It is expressly forbidden for people to load or operate software gained from the Internet, magazine gifts or other sources. The Association is also committed to using software for which it has current licences only and will not make use of more copies of a particular piece of software than it has licences.

6.4.2 Where software is developed or configured specifically for Association use, it should only contain the functionality that was specified in the requirement and must not contain functions, which have fraudulent or mischievous intent.

6.5 **Personal Computer Security**

6.5.1 It is the responsibility of each PC user to take all reasonable precautions to safeguard the security of the computer and the information contained within it. This includes protecting it from physical hazards, including spilling liquids; not allowing unauthorised users access to the machine; and only using approved software. Where information is derived from a source where there is any question of computer virus infection, the material should be subjected to a virus scan. The storage of corporate data should always be on the Association's networked drives or the Association's MS365 locations. Storage of sensitive or critical information upon a personal computer's hard disk is prohibited.

6.5.2 Special consideration should be given to the protection of portable computers, as these are more open to theft and physical damage (e.g. being dropped). Sensitive information should not be stored on the hard disk of a portable computer under any circumstances. Sensitive information should not under any circumstances be transferred to computing equipment not owned by the Association without express permission of the Chief Executive or the Finance & Corporate Services Manager. Individual users are responsible for the security of portable equipment issued to them and for the safekeeping of equipment when kept at home or in transit.

6.6 **Access Control**

6.6.1 Access control is implemented to ensure users get access only to the required components and software on their local computer. An 'Access Register' will be maintained to allow the Association's IT support provider to check access audits on a weekly basis to ensure the policies are being adhered to and unauthorised access is being logged with the appropriate action taken.

6.6.2 Other methods of control are in place, namely blocking use of all USB mass storage devices and the implementation of Data Loss Prevention policies which log, audit and block certain types of file transfer to unsolicited cloud-based locations.

6.6.3 Multi Factor Authentication is required when users are accessing the networks or any system remotely. Multi Factor Authentication is also in place within third party hosted solutions such as the housing management system.

6.7 Password Protocol

6.7.1 A password protocol is in place which forces users to change their passwords every 60 days. This enforces complex and passwords of at least 8 characters with the use of the last 5 passwords forbidden.

6.8 Networking Security

6.8.1 The Association recognises the additional security hazards posed by networked systems and wishes to reduce these threats wherever possible. The policy restricts the transfer of confidential information over unprotected communication links, whether within the Association's private network or via the public network. Sufficient safeguards should be implemented to prevent unauthorised persons from accessing our IT systems and where there is a need to interwork with the public network, 'firewalls' must be installed.

6.8.2 For networked computer systems, the integrity and security against threat shall be operated over the whole system, with a defined minimum level of security maintained across all components. This minimum level is determined by the highest level of confidentiality of the information handled by any of the systems concerned. Where data is replicated across different elements, sufficient safeguards shall be implemented to ensure that the different systems are kept in step at all times.

6.8.3 Wireless access is provided by the Association, but access is limited. There are 2 networks, one which will only allow access to the corporate network for domain joined PCs or laptops. The second “Guest” Network utilises the same internet connection but is split away from normal traffic via layer 3 firewall and is constantly monitored.

6.8.4 Authorisation to connect to DPHA equipment will only be given once the user has read and signed the disclaimer contained within DPHA’s Communications Policy. Any breech of IT DPHA security procedures will be subject to disciplinary action.

6.9 Internet Security

6.9.1 Use of the Internet is granted subject to Association rules. While the Association is committed to use of the Internet for business purposes, it must ensure that suitable controls are in place to prevent security breaches or other negative consequences. The networks used for the Internet are not secure and any communications sent by this means could be accessed or modified by unauthorised individuals. There are also threats from obtaining information from the Internet, with virus attachments being the most common. Consequently, we must adopt procedures that minimise the risk of using the Internet and follow good practice in the way individuals behave and the Internet sites that they visit. We have established our Internet access for specific business purposes and for limited personal use, where this does not interfere with or impede business operations. Where material is obtained from the Internet, users

must ensure that any copyright restrictions are obeyed and that virus protection procedures are followed. Where material we own is published, it must make specific reference to our copyright markers.

6.9.2 The Internet must never be used for the communication of confidential information, even where encryption technology is available. Moreover, the Internet should not be used as a communication medium where any commitment is made on behalf of the Association or where commitments are received (e.g. from suppliers). The content of e-mails may be used in legal actions and the same caution should be exercised as with a written medium. When sending e-mail ensure that the content does not contain any material of a defamatory nature or engage in any racial or gender-based abuse.

6.9.3 The Association's Internet facilities and computing resources must not be used knowingly to violate the laws and regulations of the United Kingdom or any other nation. Use of any Association resources for illegal activity is grounds for disciplinary action and the Association will co-operate with any legitimate law enforcement activity in this regard.

6.9.4 Provided that individuals follow these guidelines we will gain benefits from our Internet usage, without opening the Association to the threats to which we could be subjected. It is recognised that the Internet is an area, which is undergoing significant technological change, and this policy will be reviewed periodically to ensure that it continues to satisfy our needs.

6.10 **E Mail Security**

6.10.1 The Association recognises the business value of email and is committed to providing services that support its use. However, improper use of this business tool is forbidden.

6.10.2 As previously mentioned, e-mail messages may be used as part of a legal action, and the same considerations and cautions that relate to other written forms of communication should be exercised. Examples include sending confidential messages via e-mail; sending e-mail from another user's computer or in another user's name and sending abusive, obscene, sexist, racist, threatening or defamatory e-mail messages.

6.10.3 Additionally, e-mail messages, including those stated to be confidential or personal, may be disclosed in investigations by relevant authorities or regulatory bodies, and improper statements made by e-mail can give rise to personal or Association liability.

6.10.4 The Association expressly reserves the right, where it considers it appropriate, to access or disclose electronic messages or files of an employee. In doing so, the Association will follow appropriate procedures designed to assure compliance with Association policies. In considering whether to take such steps, the Association shall take into account the need to protect the Association's or it’s systems' security, fulfil Association's obligations, comply with legal processes, or protect the rights or property of the Association.

6.11 **Viruses and other Malicious Agents**

6.11.1 The Association views the threat of infection from computer viruses as extremely serious and will take steps necessary to prevent such infection.

6.11.2 Our IT service provider will ensure that appropriate software is maintained and developed as required to protect against viruses; spy-ware; ransomware; ad-ware and SPAM. This software will be updated regularly with the latest virus and spy-ware definitions. Performance will be monitored, and software will be upgraded or replaced as necessary to ensure adequate protection. We are currently protected against the above threats by Sophos Intercept X software. Alternative products may be considered as they arise.

6.11.3 However, it is also the personal responsibility of all users to ensure that they do not introduce viruses into computer systems. Material that is known or suspected to be infected must not be introduced into Association systems. Users should take care when receiving electronic information from an unknown source, including attachments within e-mail. Where there are reasons to bring information from an external source, active virus checking must be performed, in a safe or quarantined environment.

6.11.4 DPHA aims to have Cyber Essentials accreditation in place to assist in minimising the risk of malicious attack. Procedures will be implemented to ensure the accreditation is retained on an ongoing basis and this will include regular user training covering the latest threats and recommended actions.

7.0 BACKUP PROCEDURE

7.1 The Association currently utilise both on premises servers for applications and data as well as utilising some cloud-based systems. As a result, we have implemented several IT solutions to ensure the backup and disaster recovery routine is robust and fit for purpose.

7.2 Onsite Data and Systems

The Association currently run a Barracuda backup appliance. The backup appliance takes daily baily backups and snap shots of servers, and all associated on-premise data. The first copy is retained on the physical Barracuda appliance and a secondary copy of the backup is replicated offsite to Barracuda's cloud platform. The offsite copy is retained for 7 years and can be used in the event of any disasters at DPHA.

7.3 Office 365 Backup

DPHA utilise Microsoft Cloud Services such as Office 365, Teams, SharePoint, OneDrive. Although Microsoft's platforms are extremely robust and highly available, they do not cater for any form of granular data restores or long-term data retention. As such DPHA utilise a Cloud to Cloud backup solution that ensure all Email, Teams, SharePoint and OneDrive data is securely backed, retained for 7 years and is accessible in the event of a disaster with Microsoft Services.

7.4 Cloud Application Providers

Some of DPHA critical systems are delivered via hosted third-party solutions (Such as Home Master). It is the third-party organisations responsibility to ensure appropriate backup and DR polices and solutions are in place for the delivery of this system.

8.0 REMOTE ACCESS FOR IT SUPPORT PROVIDER

8.1 Authorised support engineers will have the capability to dial into the DPHA office through a secure VPN L2TP connection. The required port will be opened on the DPHA firewall to specific public IP addresses only. Users are not capable of connecting to the DPHA network without a specified IP address assigned by your broadband ISP.

9.0 REMOTE ACCESS FOR STAFF

9.1 The Association provides all staff with equipment and capabilities to access the Associations systems from home and other remote locations. DPHA will ensure appropriate firewalls and security is in place in relation to the internal network and third-party suppliers will ensure appropriate security within their data centres to ensure that all access is secure

10.0 VULNERABLE TESTING

10.1 Vulnerability testing will be carried out annually and also after any large infrastructure changes, and the report provided will give extensive details about the external security of the system.

11.0 HARDWARE DISPOSAL PROCEDURE

11.1 This is carried out by IT support provider in accordance with legislation required in Scotland and destruction certificates can be produced if required.

11.2 When disposing of hardware, account will be taken of relevant IT disposal legislation including the Data Protection Act. Our IT support provider will ensure that appropriate measures are in place to decommission machines effectively and that data is protected at all times. Primary decommissioning will be carried out before the machines leave the site. Where practical, our IT service provider will ensure that equipment is recycled in line with environmental considerations.

12.0 DISASTER RECOVERY

12.1 When the business continuity plan is activated any available windows-based device can be used (Laptop or Desktop) with a high-speed internet connection, to restore back up data.

12.2 Our IT support provider will work with the Corporate Services Officer to highlight which services, software and data are critical to ensure the most effective and productive method of restoration at the time of the issue. During this process re-

establishing initial core services will be given priority and once there has been confirmation of more permanent premises any required hardware will be installed, with a full working plan created to return to normal business as quickly as possible. For email access there should be no requirement as this is stored in a Microsoft Office 365 Cloud and only requires internet access.

13.0 CHANGE MANAGEMENT

13.1 From time to time systems require changes for planned upgrades, maintenance, or fine-tuning. Managing these changes is a critical part of providing a stable infrastructure. Any changes will be managed in a well-communicated, planned and predictable manner that minimises unplanned downtime and unforeseen system issues.

13.2 Effective change management requires planning, communication, monitoring, rollback, and follow-up procedures to reduce negative impact to the user community.

13.3 The following change management processes will be followed:

Scheduled changes and procedures shall be developed to inform users of any of upcoming application and system changes that impact system availability or operations.

- Regular planned changes shall be communicated to all users on a monthly basis.
- Unplanned changes shall be communicated immediately to all users with regular updates on progress towards resolution and continuation of service.
- Regular system and application patching schedules shall be communicated to users and performed in such a way as to minimise system downtime and user productivity.
- Changes affecting computing environmental facilities (e.g., air-conditioning, water, heat, plumbing, electricity, and alarms) shall be reported to or coordinated with other teams and users shall be notified through the Corporate Services Officer.

13.4 Any change management will be determined by the Leadership Team who shall discuss this on a monthly basis and will consider the full effect of any changes to the IT systems along with professional advice from the IT support provider. The final approval to allow or delay any changes will be with the Chief Executive.

13.5 Changes may be denied for the following reasons:

- Inadequate change planning or testing

- Lack of stakeholder acceptance (where applicable)
- System integration or inoperability concerns
- Missing or deficient roll-back plans
- Security implications and risks
- Timing of the change negatively impacting key business processes
- Timeframes do not align with resource scheduling (e.g. late-night, weekends, holidays, or during special events)

13.6 Controls and Management

13.6.1 Documented procedures and evidence of practice should be in place for this policy including logs of change events, IT change management meeting minutes, IT Inventories, IT Support provider Incident Reporting monitor.

14.0 DATA PROTECTION

14.1 We will treat personal data in line with our obligations under the current data protection regulations and our Privacy Policy. Information regarding how data will be used and the basis for processing data is provided in our Employee Fair Processing Notice.

15.0 EQUALITIES AND HUMAN RIGHTS

15.1 We are committed to promoting an environment of respect, understanding, encouraging diversity and eliminating discrimination by providing equality of opportunity for all. This is reflected in our Equality and Human Rights Policy.

16.0 DISSATISFACTION

16.1 Any employee not satisfied with the implementation of this Policy can in the first instance raise their concerns with their manager or the senior officer dealing with the situation. If the employee remains dissatisfied, they should refer to the Association's Grievance Policy and procedures.

17.0 REVIEW

17.1 This policy will be reviewed by the Board every 3-years or earlier if required.

Appendix 1

BREACH OF SECURITY NOTIFICATION PROCEDURE

In the event of a breach of IT Security the following staff members should be contacted immediately who shall contact the IT Service provider for professional advice.

Chief Executive	Anne Marie Brown	Ext 2136
Finance and Corporate Services Manager	Carla Cameron	Ext 2121
Corporate Services Officer	Kimberley Tennant	Ext 2132
Microtech Helpdesk	01563 530 480	