ARDENGLEN

ICT Policy

Policy Title:	**ICT Policy**
Risk Priority:	**Medium**
Policy Author:	**Leanne McGowan**
Date of Approval:	**1st May 2018**
Date for Next Scheduled Review:	**May 2021**
Review Body:	**Board**
Equality Impact Assessment Complete:	**No**
Policy Published on Web:	**No**
Scottish Social Housing Charter Standard	**N/A**
Scottish Housing Regulator Standard:	**5**
Scottish Housing Regulator Guidance:	**5.1, 5.2**

ICT POLICY

Ardenglen Housing Association can provide this procedure on request, in large print, in Braille, on tape or in other non-written format, and in a variety of languages.

1.0 INTRODUCTION

Ardenglen Housing Association (Ardenglen) is committed to the highest standards of openness, probity and accountability.

Regulatory Standard 5 states that an RSL must *"conduct its affairs with honesty and integrity".* To ensure this, the Association has clear policy and procedures in place which make sure the organisation acts with transparency, honesty and propriety and avoids any public perception of improper conduct.

The Association's objective is to maximise the effectiveness of the applications provided, ensure business continuity in the event of any system failures and ensure compliance with the General Data Protection Regulation (EU) 2016/679 ("the GDPR"). It is essential that controls be in place which protects Ardenglen and its staff.

As the Association also provide ICT support such as computers and broadband access to Board Members it is important to note that the Policy also relates directly to Board Members.

It is vital that you read this Policy carefully. If there is anything that you do not understand, it is your responsibility to ask for an explanation.

2.0 CORE ICT INFRASTRUCTURE

This section covers Ardenglen's generic provision of ICT. Specific applications are covered in later sections.

Managers and supervisors are responsible for ensuring that this policy is complied with.

2.1 ICT Policy

The ICT Policy has been prepared to help Ardenglen and its employees to get the most out of the ICT resources at their disposal. It offers a description of these resources and defines acceptable and unacceptable use of them. By following the guidance and instructions given, employees will be contributing to the success of the Association as well as developing their own skills and understanding.

2.1.1 ICT Infrastructure of Ardenglen:

- Ardenglen has provided an ICT infrastructure, which allows efficient information and resource sharing. This helps facilitate good working relationships with colleagues, business partners and customers, which, in turn, help the Association to reach its objectives.

- The business software packages run on a system of Network Servers and individual Personal Computers (PC). They are maintained by the appointed IT consultants.

- All data should be stored on the Network Servers. Employees are directed to the Association's data map and folder structure within the ICT procedures.

- Employees will have access to all data required to complete their daily activities.

- An industry standard local area network (LAN) is used to connect the Network Servers, PCs, telephones and shared equipment to each other.

- Each employee will have access to a PC, which will give them access to the software and data required by them.

- The Association will endeavour to upgrade or replace the PCs when required, in order to maintain acceptable performance, subject to budgetary constraints.

2.1.2 Security, Integrity & Access

The security of information is of paramount importance to Ardenglen who consider there to be four basic aspects of information security. They are: -

Physical and Network Security

The server and associated infrastructure will be located in a secure location, away from public areas and under supervision.

Access to the secure area will be restricted to the IT Consultant and designated employees only. The secure area will be kept locked at all times with the exception of routine maintenance or backup operations.

Access to the server is protected by password and restricted to the IT Consultant and designated employees only.

In consultation with the IT Consultant, the Association will ensure appropriate network security controls are in place. These will include firewall configuration, anti virus software, anti spy ware and appropriate security levels and controls for remote access facilities.

The Association's network security is further enhanced by the wifi configuration. The router supports three different configurations:

- Staff mobiles with internet only permanent connection. Password communicated by email and changed every 6 months.
- Visitor/guest with internet only time limited connection. Password communicated verbally and changed every month. Set to require re-authentication on reconnect.
- Office laptops with internet and network permanent connection. Password inserted by Finance & Business Support team and changed every 6 months.

Confidentiality

All Association information must be protected from unauthorised disclosure. This includes 'leaks' of information and unauthorised access to data and 'hacking' into systems from internal or external locations.

Integrity

Data must be protected from unauthorised modification. Only those with the appropriate authority should be able to change data. Data must also be protected from accidental alteration.

Availability

To maintain its value, Association data must be available when and where it is needed.

It is, therefore, Association policy to protect business information from all internal and external threats either deliberate or accidental.

It is equally important to maintain customer confidence by meeting all obligations under the GDPR. The purpose of the GDPR is to protect the rights of the individual about whom data is stored and processed or supplied. All customers, past, present or future, are protected by the GDPR. Ardenglen is notified as a Data Controller with the Office of the Information Commissioner.

Therefore, in order to protect its customers the Association must protect its own internal systems.

To achieve these goals: -

- All users of ICT systems will undergo basic system training before using any system. This will include logging on and off, network locations for saving files, Anti-Virus protection, security risks and precautions and location of the ICT procedures. This training will be organised by Line Managers.

- All ICT users must comply with the password policy and procedures.

- Staff will be responsible for the security of all Association information that is taken off site, e.g., on pen drives or notebook computer. Staff should not store any Association information on their own PC.

In order to facilitate recovery in the event of a failure to protect Association information: -

- Shadow copies of all data files are created daily at 7am and 12pm.

- A full system state image backup will be completed every weekend. A copy of this backup will be retained by the designated IT Consultant off site. This copy backup is rotated on monthly basis.

- All data files will be backed up on a daily basis from Monday to Friday. In order to make this effective it is vitally important that users save all Association information on a network location.

- Daily data file backups are digitally stored on a secure Network Addressable Storage device (NAS) with secure access. An external hard drive copy will be stored in a fireproof safe, the data of which should not be older than one day.

- Further copies of daily backups will be stored off-site in the Cloud. The Cloud data centre is located in the UK.

- Daily backups are automatically monitored in real time for failure using monitoring software the IT Consultants are alerted to any failures via email.

2.1.3 ICT Support

The Association will appoint an IT Consultant to provide the support service for all ICT related issues. They will be responsible for all hardware and software installation and maintenance.

2.1.4 Training

Ardenglen will generally recruit staff with the basic ICT skills necessary for the job. Additional training, including on the job training, will be provided from the training budget, which is controlled by line managers.

2.1.5 Non-Compliance

Non-compliance of the ICT Policy and Procedures will be dealt with in accordance with the conditions of service disciplinary procedures.

3.0 PASSWORDS

Passwords are an important aspect of security being protection for domain or local user accounts. A poorly chosen password may compromise the entire

network. Although the system dictates the policy all employees are responsible for adhering to the procedures to ensure their passwords are secure.

3.1 Password Policy

The objective of the Password Policy is to assist employees to select strong passwords and as a result enhance the security of the Association's network.

3.1.1 Password Requirements

The implemented password settings are:

- History setting ensuring old passwords are not reused continually
- Maximum age ensuring passwords are changed routinely
- Minimum age ensuring the password history is effective
- Minimum password length to improve security
- Minimum complexity requirements in terms of characters chosen

3.1.2 Password Privacy

Passwords are to be treated as sensitive, confidential information and should be kept private. Passwords should not be shared with anyone, written down, stored in a file on any computer/network or talked about in front of others.

3.1.3 Monitoring and Review

The password policy requires no user intervention to administer and monitor. To ensure adequate security and appropriateness the policy will be reviewed on an annual basis.

4.0 ELECTRONIC MAIL

Electronic Mail (E-Mail) is facilitated by Outlook and enables users to organise themselves and communicate with others.

4.1 E-Mail Policy

The objective of the E-Mail Policy is to help the Association and staff to achieve the maximum benefit, at the lowest risk, from its use.

Managers and supervisors are responsible for ensuring that this policy is complied with.

4.1.1 Purpose of E-Mail

Ardenglen has provided E-Mail to facilitate communication among its employees and external business partners. The E-Mail system is the property of the Association and is intended for business and other Association sanctioned use only.

4.1.2 Guidance of Legal Issues

E-Mail users should be aware of the following:

- External E-Mails are Association records.
- E-Mails have the same legal status as other mailed documents.
- Courts can order that E-Mail messages are made available.
- Refer to existing guidelines on safeguarding confidential or competitive information.
- Any information held on individuals, including that in the E-Mail system might be subject to compliance with the GDPR.
- If in doubt ask the Business Support Team for guidance.

4.1.3 Privacy

In order to protect the Association from legal, regulatory or other repercussions Ardenglen may monitor the content of incoming and outgoing E-Mail messages.

4.1.4 Information Confidentiality

E-Mail is an inherently insecure system (a bit like sending information on a postcard). Content can be easily copied and forwarded. Secure email should be used to send sensitive or confidential information.

4.1.5 Drafting of E-Mail

It is Ardenglen's policy to ensure a consistent standard of E-Mail messages emanating from the Association. To that end, users should:

- Draft E-Mails carefully, taking into account discrimination, harassment, and Association representation and defamation issues.
- All employees should use suitable E-Mail etiquette at all times. Detailed in the ICT procedures.

- External E-Mails should have the confidentiality clause appended. See the Business Support Officer for instruction to have it automatically added to your outgoing E-Mail messages.

The confidentiality Clause is:

This communication contains information that is confidential and may also be privileged. It is for the exclusive use of the addressee. If you have received this communication in error, please contact us immediately and also delete the communication from your computer. Please check attachments for viruses: whilst precautions have been made to prevent transmission of viruses, we are not responsible for any damage caused as a result of contagion. This communication is provided for information purposes only and does not form any part of a contract or agreement. The views expressed in this communication are not necessarily those held by this organisation. Ardenglen Housing Association is a recognised Scottish Charity No SCO032542

- All E-Mails will automatically detail the name, designation and direct phone number of the staff member issuing the email.

4.1.6 Virus Threat

E-Mails offer a path for viruses to contaminate the Association's systems. The E-Mail system has Anti-Virus protection but users are reminded of the danger. See Section 2.1.2 above. For example users should not open Zip Files or other potentially suspicious elements without consultation with the IT consultant.

4.1.7 Storage

Outlook facilitates the sending and receiving of E-Mails and will archive to the mailstore all E-Mails over 3 months old. Mailstore is used for archiving, mail management, retention and retrieval. Mailstore journals every incoming and outgoing email.

4.1.8 Retention Policy

Retention and deletion of E-Mail is managed by mailstore with reference to data storage levels, archival records, contractual evidence and legal requirements. The Association adopts the National Housing Federation's document retention schedule and this can be found online at www.housing.org.uk/resource-library/browse/document-retention-for-housing-associations

4.1.9 Explicit Material

Ardenglen expressly prohibits the use of Association systems to carry explicit material. In particular:

- The distribution of chain letters, inappropriate humour, explicit language, offensive images or any other message, which breaches the Association's harassment policy or creates an intimidating or hostile work environment is not permitted.

- Both Association and employees must accept the risk that inbound E-Mail messages may contain explicit or offensive material that is beyond the control of the Association. If any such material is received then the employee should contact the Business Support Officer for advice on what action to take.

5.0 THE INTERNET

Use of the internet by employees is permitted and encouraged where such use supports the goals and objectives of the Association.

5.1 Internet Policy

The Internet has been recognised as an important source of business information for the Association, the Policy for its use is:

- Managers and supervisors are responsible for ensuring that this policy is complied with.

- Access to the Internet for personal use is confined to outside of normal working hours. Personal use must still comply with this policy.

- The Association has the right to monitor Internet activity and to block offensive, illegal and non-business related sites.

The following use of the Internet is prohibited:

- Unethical or illegal activities.

- Copying copyrighted material without explicit permission, unless covered or permitted under an agreement or other such licence.

- Introducing any form of malicious software onto the network.

- Misuse of any information obtained from the Internet.

Ardenglen Housing Association has a website at present (ardenglen.org.uk). The site provides information to visitors on services provided by the Association, as well as areas specifically for the tenants and board members. The Association is continually investigating ways of improving the services that it can offer through the site. The Internet Policy will be amended appropriately if and when this happens.

5.2 Social Networking

Social networking refers to a broad class of web sites and services that allow people to connect with friends, family and colleagues online, as well as meet and share information with people with similar interest or hobbies

Ardenglen operates a Facebook account which should be governed by the same principles that regulate the use of email and the internet.

Staff members must be aware that they may be subject to disciplinary measures for inappropriate use, even when using their own personal Social Networking accounts.

The following principles apply to Ardenglen staff using social networking sites:

- The confidentiality, privacy and dignity of Ardenglen as an organisation including its staff, tenants and contractors should be respected. This includes posting comments, pictures or any other content which refers to others without their permission.
- These sites are not acceptable platforms for discussing work related issues.
- Images of Ardenglen related activities including official functions, away days, training events or staff parties should not be posted without the permission of those pictured.
- If a member of staff identifies Ardenglen as their workplace, their line manager should be informed.
- Ardenglen staff have a duty to apply the above principles to content posted by other contributors to their pages on any web site.

6.0 TELECOMMUNICATIONS

Telecommunications is used to communicate with customers and business partners. It is, therefore, vital that reliable systems are provided and that they are used efficiently.

6.1 Telecommunication Policy

The telecommunications Policy is to provide a reliable, flexible system. Each user will be trained in the systems use and should follow the procedures laid down. In order to get the most from Telecommunications:

- Managers and supervisors are responsible for ensuring that this policy is complied with.

- Ardenglen has provided a modern telephone system with the capacity for growth to meet the Association requirements for the foreseeable future.

- Siebert Ltd provides network Service over a Session Initiation Protocol (SIP) Connection.

- A Siebert System delivers telecommunication to each desk, using the company's structured cabling system.

- The Telecommunications service is provided for all staff for business and other Association sanctioned use only. Personal use is not encouraged and is viewed as a privilege, not a right. Managers have the right to withdraw this privilege if it is abused. Excessive or inappropriate personal use will be subject to disciplinary action.

7. TRAINING

The Association through its Business Plan is committed to training and developing staff and board members to their full potential in order to deliver a high quality of service in all areas of its business.

The employee induction programme includes an overview of this policy, including responsibilities for the promotion and delivery of openness and confidentiality as relevant to their job descriptions. Board members and staff will receive updates on these issues and specific training as required.

8. EQUALITIES AND DIVERSITY

This policy will be implemented in line with our Equality and Diversity Policy and is subject to an Equality Impact Assessment to assess the likely or actual effects of the policy to our customers in respect of their disability, age, gender, race, religion/belief, sexual orientation or gender identity to ensure equal and fair access for all.

9. MONITORING AND REPORTING

The Association will use appeals, complaints, comments or suggestions from users of this policy to monitor its effectiveness. These will also be used to prompt a review of the policy where necessary.

10. REVIEW

This Policy will be approved by the Board. It will be reviewed every three years unless amendment is prompted by a change in legislation, or monitoring and reporting reveals that a change in Policy is required sooner.

11. DISTRIBUTION

This policy will be provided to every employee and board member and will be made freely available to any tenant or interested party.

12. LEGAL FRAMEWORK

- General Data Protection Regulation (EU) 2016/679

13. RELATED POLICIES

- Openness and Confidentiality Policy
- Privacy Policy
- Terms and Conditions of Employment
- Whistleblowing Policy
- Codes of Conduct

--- END OF POLICY ---