Paisley
Housing Association

FINANCE
Information Security
Issued: March 2022
Review Date: March 2027

Policy on :	**Information Security**

Compliant with Charter :	**N/A**
Compliant with New Regulatory Framework:	**Regulatory Standards of Governance and Financial Management** **No 3: The RSL manages its resources to ensure its financial well-being and economic effectiveness.** **No 4: The governing body bases its decisions on good quality information and advice and identifies and mitigates risks to the organisation's purpose.**
Compliant with Tenant Participation Strategy:	**N/A**
Compliant with Equal Opportunities :	**YES**
Compliant with Business Plan :	**YES**

Date of Approval : **Date for review :**	**March 2022** **March 2027**

Responsible Officer :	**Head of Finance & IT Lorna Colville**

INFORMATION SECURITY

1 INTRODUCTION

The aim of this policy is to ensure business continuity and to minimise business damage to Paisley Housing Association & Paisley South Property Services by preventing and minimising the impact of security incidents.

The Policy applies to all Board Members (of PHA & PSPS) and Employees and covers the areas of:

- Computer Misuse
- Data Protection
- Use of Software
- Virus & Spam Protection
- Email
- Internet
- Backup and Disaster Plans
- Password Security
- Remote Access
- Physical Security
- Disposal of equipment.

2 POLICY OBJECTIVES

The objectives of the policy are to:

- Provide a comprehensive statement of Paisley HA's Policy on Information Security.
- Ensure that employees and Board Members are aware of the policy, the associated legal requirements and their rights and responsibilities.
- Protect equipment and data belonging to Paisley Housing Association.
- Ensure access to appropriate training in line with Paisley HA's staff training and continuing development policy
- Raise awareness of the need for Information Security throughout the organisation.
- Regularly review and update this policy.

The absence of a review will not cause this policy to lapse.

3 LEGAL ISSUES

There are eight areas of law, which are important in Information Security:

- Copyright, Designs and Patents Act 1988
- Computer Misuse Act 1990
- The Human Right Act 1998
- The Regulations of Investigatory Powers Act 2000
- Telecommunications Regulations 2000
- The Freedom of Information (Scotland) Act 2002 ("FOI") and the Environmental Information (Scotland) Regulations 2004 ("EIR")
- Serious Crime Act 2015
- General Data Protection Regulation 2018

Any breach of security caused by recklessly or deliberately failing to comply with the Information Security Policy could result in disciplinary action and possible prosecution.

All Staff are required to read the information security policy. Staff who require further guidance on any area of the policy should contact the ICT team.

4 COMPUTER MISUSE

The Computer Misuse Act 1990 (as Updated by the Serious Crime Act 2015 Act) covers the following criminal offences:

- Unauthorised Access to Computer Material: Obtaining Unauthorised access to computer material for example, by using another person's ID and password to log onto a computer and access data.
- Unauthorised Access with Intent to commit or facilitate further offenses: Obtaining such access in order to commit or facilitate the commission of another offence, such as theft of funds or data.
- Unauthorised Acts with Intent to Impair: Obtaining such access in order to intentionally or recklessly impair the operation of any computer, a program or the reliability of data held on a computer; prevent or hinder access to any program or such data.
- Unauthorised acts causing, or creating risk of, serious damage: Where Unauthorised acts are carried out on a computer resulting in serious damage to the economy, the environment, to national security or human welfare, or which create a significant risk of such damage even whilst physically outside the UK.
- Making, supplying or obtaining articles for use in any of the above offences

The legislation was introduced to deal with the issue of computer hacking.

All I.T. facilities at Paisley Housing Association are provided for the purpose of carrying out the business of the Association and employees may only access applications where authorised. Under no circumstances must the Association equipment be used for private commercial purposes.

In order to prevent computer misuse, the Association will

- Regulate the access of users to ICT systems, e.g. access to nominal and purchase ledgers will be limited to those staff who will use the ledgers as part of their daily work.
- Where possible, ensure that users use their own unique user ID and password. See Appendix 1 Password Procedure
- Have in place a Communication Policy to set out guidelines on use of emails, the internet and social media.

If the Association suspects there has been a breach of Computer Security under the Computer Misuse Act 1990 or Serious Crime Act 2015, it will automatically involve the Police.

5 DATA PROTECTION

GENERAL DATA PROTECTION REGULATION (GDPR) covers:

- Electronic information stored, processed or transmitted on any of the association's information systems. Includes, Server's, PC's, Laptops, Tablets, Mobile Phones, Portable Storage Devices (USB).
- Information stored within the association's paper filing/storage systems or office environment.
- Information shared with external agencies/partners.

The Association has a separate GDPR (PPKD GOV 30) which should be adhered to.

Paisley Housing Association will seek to ensure compliance with the Act by ensuring:

- Registration with the Information Commissioner's Office
- Data is processed lawfully, fairly and in a transparent manner in relation to individuals.
- Data is collected for specified, explicit and legitimate purposes.
- Data is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Data is accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Data is kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

- Data is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. Including email encryption where possible.

6 USE OF SOFTWARE

Paisley Housing Association uses software in all aspects of its business to support the work done by its employees.

No staff may install software for the Association's use without the express permission of the IT department. The IT Officer is responsible for maintaining a record system of purchase agreements and licences. All hardware purchases are recorded in the Association's asset register.

The IT Officer will coordinate installation of all software on the Association's network.

7 VIRUS & SPAM PROTECTION

The Association has installed virus protection software on its network and work laptops to protect the Association's assets.

The Association has installed spam filtering software to prevent certain emails being delivered and filter some others for review.

8 Email

Inappropriate use of Email may lead to criminal prosecution, disciplinary action, transfer of viruses or damage to the Association's assets.

Through the Communication Policy, the Association will ensure that E-mail is correctly used and that staff understand their responsibilities concerning E-mail. It will advise individuals of the consequences of inappropriate use of electronic communication.

External E-mails will have the appropriate signature and disclaimer included in the message.

The Association uses software that

- Highlight emails from external sources
- Quarantines emails that are flagged in accordance with the Association's security criteria. Staff self-manage release or blocking of such emails.

When replying to emails (both internal and external), in particular, regarding requests for payment, staff should check to ensure the email originated for a legitimate source as well as considering appropriateness of the request.

9 INTERNET

Paisley Housing Association provides access to the Internet to make information available in support of the Association's business.

Staff are permitted access to the internet during the working day for business use relating to the carrying out of official duties and tasks. Staff may have access to the internet for personal use, provided this is in their own time within the guidelines set out in the Communication Policy.

Use of the Internet will be automatically logged by the Association's firewall software for the purpose of complying with Paisley Housing Association's policies and procedures,

The Association has blacklisted a number of internet sites, such as gambling and pornographic sites via its IT security software, which prevents access to certain sites.

If any abuses are discovered in relation to the use of the Internet, access will be removed immediately, and disciplinary action or criminal prosecution may result.

Paisley Housing Association and its subsidiary has its own website (as part of the Scottish Housing Connections Group) and the Line Managers are responsible for the monitoring and updating of information contained in the web site, to ensure published data and links on the site are relevant and up to date,

10 MONITORING EMPLOYEE COMMUNICATIONS

Under the regulation of Investigatory Powers Act 2000 and Telecommunications Regulations 2000, employers have the right to monitor employee communications in the following circumstances:

- To establish the existence of facts relevant to the employer's business, e.g. if deals are concluded by telephone.
- To ensure there is compliance with regulatory practices, e.g. in financial services.
- To ascertain or demonstrate standards to be achieved, e.g. to assess the quality of service.
- To prevent or detect crime.
- To investigate or detect unauthorised use of the system, e.g. use of systems for private purposes where this is not allowed or to investigate complaints about explicit e-mails, etc.
- To check for effective operation of the system, e.g. to check for viruses.
- To check if communications are relevant to the business, e.g. checking Email and voicemail during staff absences.

Paisley Housing Association will not routinely check the communications of its staff members except in the following circumstances.

- To prevent or detect crime.
- To investigate or detect unauthorised use of communications systems.
- To check the effective operation of the system, i.e. virus checks.
- To check communications during absences from work to ensure the effective delivery of service.

11 BACK-UP AND DISASTER RECOVERY

The Association has in place a Disaster Recovery Policy (PPKD FIN33) which sets out back-ups will be taken and stored and how data will be restored. It is the responsibility of the IT officer to ensure regular back-ups are taken. In addition the policy includes contingency plans in case of the loss of the Association's main file storage.

For ongoing maintenance of the system, the Association will have a maintenance contract with various hardware and software contractors who will also access the Associations network for maintenance purposes.

12 PASSWORD SECURITY

Appendix 1 sets out the Password Procedure in more detail**,** in particular the criteria staff should use when setting password.

Passwords set by staff, should, where possible follow the Password Policy. In particular, for key applicable software/ IT functionality.

The Association has moved to Microsoft 365 for email and Exchange services. These are online services and the Association has therefore adopted Multi Factor Authentication which provides added security to users of these online accounts.

13 REMOTE ACCESS

Remote access includes situations such as employees working away from the Association's offices using computers to connected directly to the Association's network.

The Association has the facility for staff to access office systems remotely. The responsibility of securely implementing this rests with the Head of Finance & IT. However, staff are personally responsible for the security and privacy of organisational and personal data from third parties, in particular, when working remotely. Access to the network is controlled by the use of a VPN and Firewall

The details in this policy apply equally to staff working from a remote access facility as to those working from Association premises.

14 PHYSICAL SECURITY

The Association has invested substantial sums in Information Technology and threats to the physical security of the equipment could seriously impact on the Association's ability to deliver services to the public.

The physical servers are stored in a well ventilated, locked area and access be restricted to ICT staff.

The Association carries insurance relating to its office equipment and disruption to work. It also has an ICT Disaster Recovery Policy which includes a Plan to be implemented in emergency

situations.

Staff however are responsible for ensuring that the IT equipment provided to them is:

- Safely secured when not in use.
- Is used in a safe manner
- Is not accessible to unauthorised users.

15 DISPOSAL OF PCs AND SOFTWARE

It is the responsibility of the IT Officer for the safe disposal of PCs and software, ensuring that data is successfully wiped from any data-carrying device prior to disposal, gifting or sale.

IT equipment that is deemed no longer fit for purpose by the Association & have had all data removed, may be sold to staff, but it is their responsibility to ensure that they obtain licensed software to use with them.

Where possible, IT equipment no longer required by the Association and not resold will be passed to a charitable IT recycling business for reuse.

All servers will be destroyed and a Certificate of Destruction will be obtained.

Where recycling is not possible the IT Officer will ensure all hard disks and software will be securely destroyed.

16 REPORTING SECURITY INCIDENTS

An information security incident is an event which causes loss or damage to the Association's data and assets, e.g. sabotage, virus infection, fraud, theft, misuse of personal data and accessing illegal or inappropriate material on the Internet.

Such incidents should be immediately reported to the IT Officer for investigation and action as required appropriate.

Such incidents could lead to breach of legislation, financial loss, disruption to service and loss of customer confidence.

Any serious cyber breaches should be reported to the Information Commissioners Office.

The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority (ICO). This must be done within 72 hours of becoming aware of the breach, where feasible. Examples include, the loss of a USB stick, data being destroyed or sent to the wrong address, the theft of a laptop or hacking.

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay.

The Association must also keep a record of any personal data breaches, regardless of whether we are required to notify third parties.

In addition, any attempted security breaches experienced the association should be reported to the Cyber Crime Unit of the National Crime Agency.

17 TRAINING

The Association places high priority on training staff. Implementation of this policy is no exception. High priority will be given to staff & board training and development in relation to use of software, email, social media and the internet, in particular as part of the staff & board appraisal processes.

18 REVIEW

This Procedure will be formally reviewed by the Board every 5 years and within the period by the Head of Finance & IT where updated are required.

Appendix 1 : PHA Password Procedure

GENERAL

Users are expected to follow these rules and recommendations create secure passwords and maintain password confidentiality.

The following should be adopted where possible and specifically will be adopted for key software / IT functionality

Applicable Software/IT Functionality

These are:

- Active Directory access/remote desktop access.
- Office 365 access
- Specific third party software where confidentiality and appropriate access if very important.

Where possible other password should also follow these principles as much as is practical taking into account the limitation of the individual software, portal etc. and the sensitivity of the data held.

Passwords must not be recorded

Users must never retain written down password anywhere nor save them for automatic access. This includes saving credentials for account login (e.g. Remote Desktop Connection “Allow me to save credentials” tick box). Password can however be securely stored as advised by IT.

Passwords must not be shared

Passwords are confidential; users must not share their passwords with others.

Complexity requirements

Password complexity requirements will be enforced on Key applicable software/IT functionality. Complexity requirements force users to have strong passwords.

Minimum password length

Minimum password length must be enforced; this must be set to 12 characters.

Passphrases

The use of passphrases (a sequence of words used instead of a password) are encouraged. Due to their length, passphrases are more secure than passwords.

Use numbers and special characters

Users must include a mix of Capital Letters, Lower Case Letters, Numbers and Special characters (&*@?) in their passwords.

Avoid names and dates

Users must not use easily guessable passwords, such as:

- Personal details such as name, birthday, place of origin
- Local names such as place names or business names

Avoid Generic Words

Users must avoid using generic word such ass Password as they are easy to guess.

Avoid simple sequences

Users must avoid including sequences, such as 123 or abc.

Avoid keyboard sequences

Users must avoid including sequences of characters that are in close proximity on the keyboard, such as qwerty or zxcvb.

Life span of Password

Where the password can follow the above complexity criteria, the password do not require to be refreshed.

Where due to other restrictions this is not possible, Users should be required to reset their password every 180 days, or as dictated by the third party software.

Password history

Password history must be enforced; a minimum of 3 passwords must be remembered. Where applicable, this prevents users from reusing an old (remembered) password.

Avoid repetitive or incremental changes

When changing passwords, users should avoid reusing old password with small or incremental changes (e.g. the password WHAT GOES UP 12 should not be replaced with WHAT GOES UP 13 or WHAT GOES UP NEW). When the password is changed, a completely new password should be created. This is most applicable when accessing sensitive and critical business data.

Capitals and number placement

Users must avoid capitalising only the first character and adding a number to the end of their password. Instead, capital letters and numbers should be placed less predictably within the password, rather than simply at the beginning and end.

Check passwords

Users are should check the strength of their passwords:

https://www.my1login.com/resources/password-strength-test/

Compromised Passwords

If a user believes their password has been compromised, they must change it, and inform the IT Officer immediately.

Staff Member leaves PHA

If a user leaves PHA or software access for any other reason should be removed, the IT Officer should be advised immediately by the Head of Department. The IT Officer with liaise with the relevant Head of Dept to have the staff member's Active Directory and Office 365 password expired/revised, as appropriate in the circumstances.

Similarly, these passwords can be amended by the IT Office if access is required due to any other absence.