FINANCE
Information Security
May 2018
May 2023

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 Budget/Business Plan :	**YES**

Date of Approval : **Date for review :**	**May 18** **May 23**

Responsible Officer :	**Finance Manager, Lorna Colville**

INFORMATION SECURITY

1 INTRODUCTION

This aim of this policy is to ensure business continuity and to minimise business damage to Paisley Housing Association & Paisley 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
- Computer Security
- Data Protection
- Use of Software
- Virus Protection
- Backup and Disaster Plans
- E-Mail
- Internet
- 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 six areas of law, which are important in Information Security:

- Data Protection Act 1998
- 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
- Freedom of Information Legislation (although currently not legally obliged to comply with we do aim to implement the principles of where possible)
- Serious Crime Act 2015
- General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR)

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 introduced four criminal offences of:

- Unauthorised Access: 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: 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.
- 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.

The Serious Crime Act 2015 was introduced to amend the Computer Misuse Act so that that law enforcement agencies would have effective legal powers to deal with the threat from serious and organised crime.

There were two main changes are:

(1) The creation of a new offence

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.

(2) Implementation of the EU Directive on Attacks against Information Systems (2013/40/EU)

- Tools for the commission of an offence – Previous legislation required the prosecution to prove that the defendant was looking to supply tools for use in committing or assisting in the

commission of another offence under the 1990 Act. The 2015 Act amends this offence so it covers the situations where an individual intends to use the tool themselves to commit or assist in the commission of a separate offence under the 1990 Act.

- Extension of the extra-territorial jurisdiction of the Act - The 1990 Act required the prosecution to demonstrate a "significant link" to the UK. The 2015 Act extended the UK's extra-territorial jurisdiction to prosecute individuals for certain offences under the 1990 Act to include the defendant's nationality. This means that a UK national can now be prosecuted for an offence where the only link to the UK is their nationality, provided that the offence is also an offence in the jurisdiction where it took place.

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.
- Ensure that users use their own unique user ID and password. The password will be regularly updated every 90 days.
- Have in place a Communication Tools 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 GENERAL DATA PROTECTION REGULATION (GDPR)

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 purpose of the GDPR is to provide a set of standardised data protection laws across all the member countries.

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

In particular, 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.

6 USE OF SOFTWARE

Paisley Housing Association uses software in all aspects of its business to support the work done by its employees. In all instances, the Association is required to comply with the Copyright, Designs and Patents Act 1988 for every piece of software used and the Association will not condone the use of any software which does not have a licence.

It will be regarded as a disciplinary matter should any employee be found in possession of or using unlicensed software.

Periodic audits may be carried out to ensure that all of our software is properly licensed in accordance with this policy. Any staff member who finds they are using copied, unlicensed software must report this to their manager and stop using the software.

No staff may install software for the Association's use without the express permission of the Finance & I.T. Manager. The BID 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 BID Officer will coordinate installation of all software on the Association's network.

7 VIRUS & SPAM PROTECTION

The Association will install virus protection software on its network to protect the Association's assets.

The Association will install spam filtering software to prevent certain emails being delivered and filter some others for review. ICT staff will have access to these emails as part of their job responsibilities and will review prior to delivery to staff.

8 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 BID 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 server.

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.

9 E-MAIL

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

Through the Communication Tool Policy (HR28), 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 and potential liability for the individual and company.

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

10 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 Tools 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.

Paisley Housing Association and its subsidiaries have their own Web Site (as part of the Scottish Housing Connections Group) and the Line Managers must approve the information contained in that web site.

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.

11 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 E-Mail 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.

12 REMOTE ACCESS

Remote access includes situations such as employees working away from the Association's offices using computers, working at home, whether or not connected directly to the Association's network.

The Association has the facility to offer remote access to staff. The responsibility of implementing this rests with the Finance & IT Manager.

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

13 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.

Where possible, physical servers should be stored in a well ventilated, locked / secure 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.

The Association also takes all reasonable measures to protect the safety of staff, board members, customers, consultants and contractors.

14 DISPOSAL OF PCs AND SOFTWARE

It is the responsibility of the BID Officer for the safe dispose of PCs and software, ensuring there is no breach of copyright law and that data is successfully wiped from any data-carrying device prior to disposal, gifting or sale.

PCs that are 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, PC's no longer required by the Association 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 BID Officer will ensure all hard disks and software will be securely destroyed.

15 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 and World Wide Web.

Such incidents could lead to breach of legislation, financial loss, disruption to service and loss of customer confidence. Guidelines will be issued to staff and managers to enable such incidents to be quickly and fairly dealt with.

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.

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

16 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, E-Mail, social media and the Internet, in particular as part of the staff & board appraisal processes.