PORT OF LEITH
HOUSING ASSOCIATION

INFORMATION SECURITY AND ACCEPTABLE USE POLICY 2018

Author	Neil Donald, ICT Manager
Policy Owner	Head of Organisational Development and ICT.
Reason	As part of review cycle.
Training and Awareness Methods	Briefing sessions Team meetings
Approval	Leadership Team
Review Cycle	1 years
Last reviewed	September 2018
Next Review Date	September 2019
Internal References	Disciplinary Policy Data Management Policy
Compliance with any legal and/or regulatory requirements	Data Protection Act 2018 Privacy and Electronic Communications Regulations 2003 Computer Misuse Act 1990
Equality Impact Assessment Outcome	This policy was evaluated by Ian Treger on 19 September 2018 and was assessed as LOW impact

REVISION TRACKING

Revisions are minor changes which are made between Full Reviews which might be needed because of new ideas or changes

Revision Date	Part of doc revised	Reason for revision	Approved by

1.0 DEFINITIONS, OBJECTIVES AND APPLICABILITY

1.1 Information Security is the practice of defending information from unauthorised access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

1.2 Information Security controls are designed to protect the Association and the Association's reputation through the preservation of CIA:

- **Confidentiality** - knowing that key data and information can be accessed only by those authorised to do so;
- **Integrity** - knowing that key data and information is accurate and up-to-date, and has not been deliberately or inadvertently modified from a previously approved version; and,
- **Availability** - knowing that the key data and information can always be accessed.

The Association is committed to protect its stakeholders' key data and information and to deploy controls that minimise the impact of any Security Incidents.

1.3 The Association is committed to taking all reasonable steps to ensure the objectives of the Information Security Policy are met to protect the interests of all stakeholders. A robust approach to information security is one of many approaches that support the Association's values and aims.

1.4 The Association adopts a risk-based approach to information security, with the Information Security Policy focussing on the risk mitigation and contingency risk responses.

1.5 The Policy applies to the following groups, henceforth referred to as 'subjects'

- all full-time, part-time and temporary staff employed by, or working for or on behalf of the Association;
- student placements at the Association;
- contractors and consultants working for or on behalf of the Association;
- all other individuals and bodies who have been granted access to the Association's ICT systems and/or key data and information.

The Chief Executive is ultimately responsible for ensuring that the policy is implemented and for overseeing compliance by subjects under their direction, control or supervision.

It is the personal responsibility of each person to whom the policy applies to adhere with its requirements.

2.0 GENERAL DATA PROTECTION REGULATIONS

2.1 The Association is registered with the Information Commissioner's Office. This policy is closely related to the Association's Data Management Policy.

2.3 In the event of a data breach (ie any event resulting in potential unauthorised access to information, the data loss action plan should be followed (Appendix 1).

3.0 PERSONNEL SECURITY

3.1 Controls will be deployed to reduce the risks of human error, theft, fraud, nuisance or malicious misuse of facilities.

a) Security roles and responsibilities will be included in job descriptions where appropriate. These will include any specific responsibilities for the protection of particular assets, or the execution of particular processes or activities including data protection.

b) Steps will be taken in accordance with the Recruitment Policy to minimise the likelihood of personnel (eg enhanced disclosure checks), who pose a security risk, being employed in posts involving key data and information, such as those concerned with sensitive customer, financial or personnel related data.

c) All staff are reminded of their obligation to protect confidential information in accordance with The Association's 'Openness, Confidentiality and Freedom of Information Policy'. Any information received by staff from applicants, tenants, suppliers or others is to be treated as confidential. All information held on the Association's computer systems likewise is confidential. Confidential information must not be divulged to third parties without the appropriate authority unless there is a legal obligation to do so.

d) Employees will be informed of their information security responsibilities during induction training and these will be reiterated on appropriate Association's intranet.

e) Information security awareness training and / or instruction will be made available to staff.

4.0 RESPONDING TO SECURITY INCIDENTS

4.1 Suspected security weaknesses

Those subjects using the ICT facilities must not try and prove any suspected or perceived security weakness. The exception to this rule is ICT support staff that have been granted a specific policy exemption which allows them to do so as part of their role.

4.2 Reporting security incidents

All actual and suspected security incidents are to be reported to the ICT Manager in the first instance. Should the ICT Manager not be available a member of the Leadership Team should be informed.

4.3 Network isolation and reconnection

Any computer that is perceived to be placing the integrity of the network at risk will be disconnected from the network. Subsequent reinstatement will only be permitted once the integrity of the system has been verified by a member of the ICT Team.

4.4 Security incident management

Events that are regarded as being 'security incidents' will be defined, and processes implemented to investigate, control, manage and review such events in accordance with the Incident Management Procedure, with a view to preventing recurrence.

5.0 COMPUTER SYSTEMS SECURITY

5.1 Computers are provided to users who need to use them to carry out their jobs. Access to the various computer systems are provided to users once the appropriate and necessary forms have been provided to the ICT Team.

5.2 Users are responsible for any system access via their network account. To avoid misuse, all access to the Association's network is password protected. All users should lock their workstation when leaving their desk. This is to prevent unauthorised individuals using the workstation.

5.3 Every computer has antivirus software installed. It is the computer users' responsibility to understand the operation of this software. If you require assistance with the operation of the antivirus software please contact the ICT Team.

5.4 Every PC on the network has the Windows firewall enabled, with the minimum number of 'open ports' to allow approved software applications to operate.

5.5 Access to, and use of, ICT systems will be monitored using various software technologies. It is expressly forbidden for subjects to attempt to circumvent or alter any computer security system or monitoring system.

6.0 SYSTEM ACCESS

6.1 Subjects are only authorised access to the Association's ICT facilities in accordance with specific privileges that they have been given.

6.2 Formal procedures will be implemented for granting access to both Association ICT facilities, and external services via Association systems, for all users. This will be supported by a formal review of user privileges on a regular basis to ensure that they remain appropriate.

6.3 Dormant accounts will be closed in accordance with the Account Management Policy.

7.0 PASSWORD CONTROLS

7.1 A solid password policy is one of the most important security control an organisation can employ. Since the responsibility for choosing good passwords falls on the users, a detailed and easy-to-understand policy is essential.

7.2 The following statements apply to the construction of passwords for any device within the organisation:

- Passwords should be at least eight characters
- Passwords should be comprised of a mix of letters, numbers and special characters (punctuation marks and symbols)
- Passwords should be comprised of a mix of upper and lower case characters
- Passwords should not be comprised of, or otherwise utilise, words that can be found in a dictionary
- Passwords should not be comprised of an obvious keyboard sequence (ie qwerty)
- Passwords should not include 'guessable' data such as personal information like birthdays, addresses, phone numbers, locations, etc.

7.3 Passwords should be considered confidential data and treated with the same discretion as any of the company proprietary information. The following guidelines apply to the confidentiality of company passwords:

- Subjects must not disclose their passwords to anyone
- Subjects must not share their passwords with others (co-workers, job-sharers, supervisors, family, etc.)
- Subjects must not write down their passwords and leave them unsecured
- Subjects must not check the 'save password' box when authenticating to applications
- Subjects must not use the same password for different systems and/or accounts
- Subjects must not re-use passwords
- Subjects must change any password that they believe to have been compromised.

8 FIREWALL MANAGEMENT

8.1 The Association maintains firewalls between all internal networks and the Internet. All firewall devices are securely set up, with 8+ character complex passwords. All 'default' passwords on devices are changed. Access to firewall configuration is restricted to hosts on the intranet side of the device.

8.2 Only services ('open ports') required to service the legitimate needs of the Association are enabled on the firewall (eg email transport, website access, file transfers) and where possible the source access to open ports is restricted to verifiable and known source addresses. See Appendix 3 for approved services.

9.0 SOFTWARE

9.1 It is strictly prohibited to install software on Association owned computing equipment unless specifically authorised by the ICT Manager. This includes free software downloaded from the Internet. If additional software is required please consult the ICT Manager.

10.0 SYSTEM POLICIES

10.1 Regular backups of the IT systems will be taken and data shall be stored securely off-site. The backup recovery procedures will be tested on a regular basis as determined by the ICT Manager and at least every 12 months.

10.2 Data should not be stored on a computer's 'C Drive' as it will not be included on the automatic backup. Wherever possible data should be saved back to the file server.

10.3 All server and PC systems shall be configured to receive operating system and application updates on a regular basis. Computer users should shut down their computer regularly throughout the month (at least once a week) to ensure that updates are applied.

10.4 The ICT team and the Head of Organisational Development and ICT have access to powerful user accounts for the Association's network.

11.0 PHYSICAL SECURITY

Controls will be implemented as appropriate to prevent unauthorised access to, interference with, or damage to, information assets.

11.1 The Association Server room is kept locked at all times when the room is not in use. Routine access to the server room is restricted to ICT personnel. Access to the server cabinets is restricted to the ICT team. Access is granted to the facilities team and their contractors for the purpose of inspecting and servicing the fire, smoke and air-conditioning installations. No other access is permitted unless specifically authorised by the ICT Manager or the Head of Organisational Development and ICT.

11.2 No Association equipment shall be removed from Association premises unless authorised by the ICT Manager. An asset register of IT equipment is maintained by the ICT team and it is the responsibility of the designated user(s) of equipment to report loss or theft.

11.3 Prior to the disposal of IT equipment, all data contained on hard disks shall be removed by the physical destruction of the disks.

12.0 INTERNET AND EMAIL

i The use of the Internet and electronic mail (email) is encouraged, as they are important communication and reference tools for Port of Leith Housing Association network users. However, the inappropriate use of internet or email, can cause many problems, ranging from minor distractions to legal claims against the Association.

ii Email communications and internet access facilities are provided for Port of Leith HA business. Incidental and occasional personal use of email and internet is permitted on this basis that usage does not interfere with the proper completion of staff's duties. Personal use is permitted on the condition that all the procedures and rules set out in this policy are complied with. Be aware, however, that if you choose to make use of our facilities for personal correspondence, you can expect very little privacy because the Association may need to monitor communications.

iii Internet and email access must not be used for personal monetary gain or any commercial purposes not related to Port of Leith Housing Association.

iv To the extent permitted by law, the Association reserves the right to access and disclose the contents of electronic mail without the consent of the user. The Association will do so when it believes it has a legitimate business need including, not limited to, maintaining the integrity and effective operation of the email systems, and only after explicit authorisation is obtained from the Line Manager.

v This document details standards for the secure use of Internet and email facilities for Port of Leith HA purposes.

12.1 LEGAL INFORMATION

i It should be noted that emails fall under the scope of the General Data Protection Regulations 2018 and the Privacy and Electronic Communications Regulations 2003. Under this legislation the email originator, all email recipients and any person named in

the email are entitled to view the information about them and if it is incorrect they are entitled to have it corrected.

ii Home or personal use has a 'domestic exemption' from data protection law, but Port of Leith has no such exemption even for personal emails if they originate from Port of Leith's network. It should be noted that emails constitute correspondence and have legal implications (ie the law of contract, laws of defamation and libel).

iii All users must ensure that the methods of collecting, processing and storing information obtained by either email or internet access must comply with Port of Leith's policies, the data protection act and any other relevant legislation.

iv Users of either email or the Internet are reminded that:

- Email messages are copyrighted
- Users do not have to register copyright it exists automatically
- When users post to a public list they do not lose copyright, but the message may be archived, forwarded to other lists or quoted by others
- Messages sent to a list should not be quoted out of context, changed or reworded or misattributed
- Software or files downloaded from the internet may be protected by copyright restrictions.

v Particular attention should be paid to the risks of transmitting confidential personal information and have a statement or disclaimer which sets out the intended use.

12.2 OFFENSIVE MATERIAL

i The internet and email systems must not be used to access, display, store, generate or send to others any material which may be regarded as causing offence. What is offensive material is determined by its effect on the recipient, not how it is regarded by the sender. It includes pornographic, sexist, racist and abusive material.

ii It may not always be possible to avoid receiving offensive material from others. It is also possible to enter an internet site carrying offensive material by accident (a site not blocked by the Association's firewall). Staff receiving such material or entering a site must immediately report the matter to their manager and must never download, store or pass the material on.

ii Failure to report receipt of offensive material (see 3.1) immediately will be viewed as complicity in disciplinary action.

12.3 INTERNET

When using the internet, you must also remember the following:

- The internet is provided for business and occasional personal use. Personal use of the Internet should not be included your working time calculation.
- Do not access or try to access data which you know or ought to know is confidential.
- It is easy to enter into a legally binding contract on the internet. Take great care and consider taking advice before making any commitment.

- No software may be downloaded from the internet without the express permission of the ICT Manager.

12.4 EMAIL

When using email you must remember the following:

- All emails sent from Port of Leith facilities are firstly, representing the Association, and secondly, representing the individual. You should be civil and courteous. You should not send an email which portrays the Association in an unprofessional light. The Association is liable for the opinions and communications of its staff. Any email involved in a legal dispute may have to be produced as evidence in court.
- Ensure that email content is accurate, factual and objective in relation to individuals. You should avoid subjective opinions about individuals or other organisations.
- Emails can easily be forwarded to other parties. You should assume that anyone mentioned in email could see it or hear about it; they may, under data protection law, be entitled to see it.
- The origin of emails can be easily disguised and for it to appear to come from someone else. If you suspect that you have received a 'forged' email contact the sender by telephone.
- You must not create or forward advertisements, chain letters or unsolicited emails eg spam.
- You should be cautious when opening emails and attachments from unknown sources as they may be infected with viruses.
- File all sent and received emails in a structured way to create a permanent record for ease of retrieval.
- All personal email you send should be marked as "PERSONAL" (either in the subject heading or by using the email sensitivity option), and all personal email sent or received must be filed in a separate folder marked "Personal" in your inbox should you wish to retain it after reading.

12.5 ACCESS AND DISCLOSURE

i Users of email are advised that Port of Leith's email systems should be treated like a shared filing system, with the expectation that communications sent or received on Port of Leith's business or with the use of the Association's resources may be made available for review by any authorised Manager for purposes related to the Association's business.

ii Users of the email system must not use any form of encryption to restrict or inhibit access to the contents of an email unless specifically authorised to do so.

iii Port of Leith will monitor electronic mail as a routine matter to the extent permitted by law as the Association deems necessary for the purposes of maintaining the integrity and effective operation of the email systems.

iv Port of Leith reserves the right to inspect and disclose the contents of email:

- In the course of an investigation triggered by indications of misconduct or misuse,
- As needed to protect health and safety,
- As needed to prevent interference with the Association's business requirements, or

- As needed to locate substantive information required for the Association's business that is not more readily available by some other means.

v Port of Leith will inspect and disclose the contents of email when such action is necessary to respond to legal processes and to fulfil the Association's obligations to third parties.

vi The contents of email communications, properly obtained for the Association's purposes, may be disclosed without permission of the user. The Association will attempt to refrain from disclosure of particular communications if disclosure appears likely to create professional embarrassment, unless such disclosure is required to serve a business purpose or satisfy a legal obligation.

13.0 REMOTE ACCESS

13.1 The Association permits staff to work from home or other locations. When working from home, subjects should in the first instance seek to use Association owned notebook computers, tablets or mobile phones. In instances where this is not possible, subjects must ensure that equipment meets or exceeds the Association's standards for security.

13.2 Subjects shall protect their login and password, even from family members. When using the Association's systems, subjects must adhere to all aspects of this policy.

14.0 CONTRAVENTION OF POLICY

14.1 Contravention of the Information Security Policy, whether deliberate or inadvertent, will be fully investigated by the Association. The circumstances surrounding any contravention will be taken into account and will be dealt with via the Association's disciplinary policy as outlined in the Association's Conditions of Service.

15.0 RESPONSIBILITIES

15.1 The ICT Manager is responsible for implementing and monitoring the policy all aspects of the Information Security Policy. The ICT Manager is responsible for co-ordinating a response to an information security incident (see Appendix 1: Data Loss Action Plan).

15.2 All staff must adhere to the Information Security Policy.

APPENDIX 1: DATA LOSS ACTION PLAN

1. Establish the exact nature of the data released, the amount / volume, and the timescale over which the release has occurred and if possible the recipient(s) of the data.

Action 1 completed Yes/No/Partial	**Date**	**By Whom**	**Comments**

2. Ensure immediate action is taken to prevent further compromise.

Action 2 completed Yes/No/Partial	**Date**	**By Whom**	**Comments**

3. If the compromise has been due to personal data being sent to the wrong individual(s), the first indication that that this has occurred may be through contact from recipients. It is important that staff receiving calls / enquiries from members of the public etc. are aware of the details they need to collect and record from callers and the advice / information which should be given out.

Action 3 completed Yes/No/Partial	**Date**	**By Whom**	**Comments**

4. Staff should be aware of the need to alert the nominated Data Controller and Data Protection Officer, and liaise with the Controller to ensure that the Information Commissioner is advised.

Action 4 completed Yes/No/Partial	**Date**	**By Whom**	**Comments**

5. Consider the need to liaise with the police and other statutory bodies taking into account the circumstances of the compromise and the data involved.

Action 5 completed Yes/No/Partial	**Date**	**By Whom**	**Comments**

6. Alert your Press Office in order that the incident can be appropriately handled in the media.

Action 6 completed Yes/No/Partial	**Date**	**By Whom**	**Comments**

7. The Board should be advised and submissions / briefings prepared as required. The need for urgency in addressing the issue should be recognised.

Action 7 completed Yes/No/Partial	**Date**	**By Whom**	**Comments**

8. If appropriate, liaise with the British Banking Association, APACS - the UK payments association, the Regulator, the Care Inspectorate, etc. These bodies will be able to advise you of the actions required and can be used to alert their members to the incident and to highlight the potential risk. Further, more detailed information of the data which has been compromised should be provided to these bodies as soon as practicable.

Action 8 completed Yes/No/Partial	**Date**	**By Whom**	**Comments**

9. Formally notify those individuals whose personal data has been compromised. Notification should be apologetic in tone.

Action 9 completed Yes/No/Partial	**Date**	**By Whom**	**Comments**

10. Where it is known that information has been issued incorrectly to others, recipients of the information should also be provided with instructions on what to do with the information they have received. In some instances it may be appropriate and more practical to use the same correspondence to cover both recipients of the data and those whose data has been compromised.

Action 10 completed Yes/No/Partial	**Date**	**By Whom**	**Comments**

11. An investigation and post incident review should be carried out to determine the cause of the compromise and to evaluate the adequacy and effectiveness of the response taken. Where required, control improvements should be implemented and reviews carried out periodically to ensure that controls / systems are operating effectively.

Action 11 completed Yes/No/Partial	**Date**	**By Whom**	**Comments**

12. Depending on the nature and scale of the data compromise it may be useful to establish a Compromise Management Group / Team to coordinate the response to the incident. Representatives may include management from the operational area involved, Customer Services, Personnel, IT, Press Office, and Finance Departments etc. This Group may wish to further consider the need to establish specific team(s) to deal with individuals' queries and complaints. Factors such as accommodation, telecommunications, IT and training for staff handling enquiries should be considered. The establishment of a free phone number for concerned callers may also be useful.

Action 12 completed Yes/No/Partial	**Date**	**By Whom**	**Comments**

APPENDIX 2: INFORMATION SECURITY RISK MANAGEMENT ASSESSMENT

Expectation of Risk Event (1-5)	
Score 1	1 – 20% chance of occurring
Score 2	21 – 40% chance of occurring
Score 3	41 - 60% chance of occurring
Score 4	61 - 80% chance of occurring
Score 5	81 – 99% chance of occurring

Impact of Risk Event (1-5)	
Score 1	no significant impact on service delivery
Score 2	minor impact on service delivery
Score 3	moderate impact on service delivery
Score 4	major impact on service delivery
Score 5	catastrophic impact on service delivery

Category Score: 1 – 7 = Low, 8 – 15 = Med, 16 – 25 = High

Cause of Risk Event/Hazard	**Description of Risk Event**	**What's in Jeopardy**	**Expect (1-5)**	**Impact (1-5)**	**Severity (E X I)**	**Cat (High/ Med/Low)**	**Tolerate/Contingency/ Mitigation**
Unsecure Server Equipment	Theft of Server Equipment	• Service delivery to customers • Financial Loss	1	5	5	Low	Mitigation: • Server room locked when not in use. • Building alarmed when empty. • Insurance cover on all equipment Contingency:

							• Standby Equipment at recovery site
Unsecure IT Equipment	Theft of End-User computing device (e.g. Printer, PC, Laptop, iPad)	• Loss of data • Financial Loss • Disruption to operation	2	2	4	Low	Mitigation: • Personal data not saved on PCs • Insurance cover on all equipment • Spare equipment kept in stock
Catastrophic Fire/Flood	Fire / Water damage to IT infrastructure	• Service delivery to customers • Destruction of data • Financial loss	1	5	5	Low	Mitigation: • Daily full backup of systems • Smoke alarms in office • Insurance cover on all equipment Contingency: • Standby Equipment at recovery site • Business Continuity Plan in place

Software Failure	Loss of functionality of software	• Service delivery to customers	1	5	5	Low	Mitigation: • Daily full backup of systems • Testing of all major upgrades to software. • IT change management procedure. • Support contract maintained with main software provider (Aareon)
Insecure data	Unauthorised access / dissemination / deletion of data	• Service delivery to customers • Reputational damage • Financial damage	2	5	10	Medium	Mitigation: • Firewall deployed • Patch management procedures in place • Antivirus software deployed • Password Protection • Internet content filtering Contingency: • Data loss procedure

Assessment Date: 26/09/2017

Assessor: Neil Donald, ICT Manager

APPENDIX 3: FIREWALL MANAGEMENT - OPEN SERVICES

List of Approved Open Services as at May 2018

Service	Purpose	Comments
SMTP	Inbound email	Receive connector configured only to access requests from MS Servers.
HTTP	Public facing website	
FTP	To receive files from our main contractor at TB Mackays	Access restricted to single public IP address
RDP	Remote access to terminal servers	Firewall configured to block originating IP after three invalid login attempts.
SIP	IP Telephony	SIP Signalling has access limited to Gamma servers