Acceptable Use Policy

Linthouse Housing Association	
Policy Implementation Checklist:	
Policy Guardian:	Irene McFarlane
Policy Author:	Colin Jones
Policy Title:	Acceptable Use Policy
Approved by Chief Executive on:	
Approved by LHA Management Committee on:	28th March 2023
Effective from:	29th March 2023
Due for Review on:	March 2026
Policy Linkages:	All ICT related
Policy Trainer:	Colin Jones
Training Completed (date)	
Posted on Website on:	
Staff Sign off as Read and Training Completed:	
Resource Implications	N/A
For office use only	
Location of Policy	H/Policies/1. Governance_ Corporate/GC22
Location of Procedures (if appl)	N/A

Acceptable Use Policy

This Acceptable Use Policy covers the security and use of all Linthouse Housing Association information and IT equipment. It also includes the use of email, internet, voice and mobile IT equipment. This policy applies to all Linthouse Housing Association employees, contractors, committee members, and agents (hereafter referred to as 'individuals').

This policy applies to all information, in whatever form, relating to Linthouse Housing Association business activities worldwide, and to all information handled by Linthouse Housing Association relating to other organisations with whom it deals. It also covers all IT and information communications facilities operated by Linthouse Housing Association or on its behalf.

Computer Access Control – Individual's Responsibility

Access to the Linthouse Housing Association IT systems is controlled by the use of User IDs, passwords and/or tokens. All User IDs and passwords are to be uniquely assigned to named individuals and consequently, individuals are accountable for all actions on the Linthouse Housing Association IT systems.

Individuals must not:

- Allow anyone else to use their user username and password on any Linthouse Housing Association IT system.
- Leave their user accounts logged in at an unattended and unlocked computer.
- Use someone else's username and password to access Linthouse Housing Association IT systems.
- Leave their password unprotected (for example writing it down).
- Perform any unauthorised changes to Linthouse Housing Association IT systems or information.
- Attempt to access data that they are not authorised to use or access.
- Exceed the limits of their authorisation or specific business need to interrogate the system or data.
- Connect any non-Linthouse Housing Association provided device to the Linthouse Housing Association network or IT systems.
- Store Linthouse Housing Association data on any Linthouse Housing Association provided equipment.
- Give or transfer Linthouse Housing Association data or software to any person or organisation outside Linthouse Housing Association without the authority of Linthouse Housing Association.

Line managers must ensure that individuals are given clear direction on the extent and limits of their authority with regard to IT systems and data.

Internet and email Conditions of Use

Use of Linthouse Housing Association internet access and email is intended for business use. Personal use is permitted where such use does not affect the individual's business performance, is not detrimental to Linthouse Housing Association in any way, not in breach of any term and condition of employment or policy, and does not place the individual or Linthouse Housing Association in breach of statutory or other legal obligations.

All individuals are accountable for their actions on the internet and email systems.

Individuals must not:

- Use the internet or email for the purposes of harassment or abuse.
- Use profanity, obscenities, or derogatory remarks in communications.
- Access, download, send or receive any data (including images), which Linthouse Housing Association considers offensive in any way, including sexually explicit, discriminatory, defamatory or libellous material.
- Use the internet or email to make personal gains or conduct a personal business.
- Use the internet or email to gamble.
- Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam.
- Place any information on the Internet that relates to Linthouse Housing Association, alter any information about it, or express any opinion about Linthouse Housing Association, unless they are specifically authorised to do this.
- Send unprotected sensitive or confidential information externally.
- Forward Linthouse Housing Association mail to personal (non-LHA) email accounts (for example a personal Hotmail account).
- Make official commitments through the internet or email on behalf of Linthouse Housing Association unless authorised to do so.
- Download copyrighted material such as music media (MP3) files, film and video files (not an exhaustive list) without appropriate approval.
- In any way infringe any copyright, database rights, trademarks or other intellectual property.
- Download any software from the internet without prior approval of the IT Department.
- Connect Linthouse Housing Association devices to the internet using non-standard connections.

Clear Desk and Clear Screen Policy

In order to reduce the risk of unauthorised access or loss of information, Linthouse Housing Association enforces a clear desk and screen policy as follows:

- Personal or confidential business information must be protected using security features provided for example secure print on printers.
- Computers must be logged off/locked or protected with a screen locking mechanism controlled by a password when unattended.
- Care must be taken to not leave confidential material on printers or photocopiers.
- All business-related printed matter must be disposed of using confidential waste bins or shredders.

Working Off-site

It is accepted that laptops and mobile devices will be taken off-site. The following controls must be applied:

- Working away from the office must be in line with Linthouse Housing Association remote working policy.
- Equipment and documents taken off-site must not be left unattended in public places and not left in a vehicle overnight.
- Laptops must be carried as hand luggage when travelling.
- Information should be protected against loss or compromise when working remotely (for example at home or in public places). Laptop encryption must be used.
- Particular care should be taken with the use of mobile devices such as mobile phones, smartphones and tablets. They must be protected at least by a password or a PIN and, where available, encryption.

Mobile Storage Devices

Mobile devices such as memory sticks, CDs, DVDs and removable hard drives are in general terms not permitted to be used. If as a means of last resort, they may be permitted where network connectivity is unavailable or there is no other secure method of transferring data. Only Linthouse Housing Association authorised mobile storage devices with encryption enabled must be used, when transferring sensitive or confidential data.

Software

Employees must use only software that is authorised by Linthouse Housing Association on Linthouse Housing Association computers. Authorised software must be used in accordance with the software supplier's licensing agreements. All

software on Linthouse Housing Association computers must be approved and installed by the Linthouse Housing Association IT department.

Individuals must not:

- Store personal files such as music, video, photographs or games on Linthouse Housing Association IT equipment.

Viruses

The IT department has implemented centralised, automated virus detection and virus software updates within the Linthouse Housing Association. All PCs have antivirus software installed to detect and remove any virus automatically.

Individuals must not:

- Remove or disable anti-virus software.
- Attempt to remove virus-infected files or clean up an infection, other than by the use of approved Linthouse Housing Association anti-virus software and procedures.

Telephony (Voice) Equipment Conditions of Use

Use of Linthouse Housing Association voice equipment is intended for business use. Individuals must not use Linthouse Housing Association voice facilities for sending or receiving private communications on personal matters, except in exceptional circumstances. All non-urgent personal communications should be made at an individual's own expense using alternative means of communications.

Individuals must not:

- Use Linthouse Housing Association voice for conducting private business.
- Make hoax or threatening calls to internal or external destinations.
- Accept reverse charge calls from domestic or international operators, unless it is for business use.

Actions upon Termination of Contract

All Linthouse Housing Association equipment and data, for example laptops and mobile devices including telephones, smartphones, USB memory devices and CDs/DVDs, must be returned to Linthouse Housing Association at termination of contract.

All Linthouse Housing Association data or intellectual property developed or gained during the period of employment remains the property of Linthouse Housing Association and must not be retained beyond termination or reused for any other purpose.

Monitoring and Filtering

All data that is created and stored on Linthouse Housing Association computers is the property of Linthouse Housing Association and there is no official provision for individual data privacy, however wherever possible Linthouse Housing Association will avoid opening personal emails.

IT system logging will take place where appropriate, and investigations will be commenced where reasonable suspicion exists of a breach of this or any other policy. Linthouse Housing Association has the right (under certain conditions) to monitor activity on its systems, including internet and email use, in order to ensure systems security and effective operation, and to protect against misuse.

Any monitoring will be carried out in accordance with audited, controlled internal processes, the UK Data Protection Act 2018, the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice Interception of Communications) Regulations 2000.

This policy must be read in conjunction with:

- Computer Misuse Act 1990
- Data Protection Act 2018

It is your responsibility to report suspected breaches of policy without delay to your line management or the IT department.

All breaches of information security policies will be investigated. Where investigations reveal misconduct, disciplinary action may follow in line with Linthouse Housing Association disciplinary procedures.

Equalities Impact Assessment

TITLE OF POLICY:	Acceptable Use Policy
Strategic Outcome:	
What is the purpose of the proposed Policy?	To provide guidance to all staff on what is and is not a permitted use of LHA equipment and network technologies.
Protected Characteristic Groups affected by the Policy	N/A
Who is the target audience of this policy or who is intended to benefit from the proposed policy and how? (ie. employees, service users, management committee etc.)	All Staff/All Committee Members
List any existing documents, evidence, research which have been used to inform the EqIA (this must include relevant data used in this assessment)	N/A
Has any consultation involvement been undertaken with the Protected Characteristic Groups to inform this assessment? (please provide details of who and how consulted)	N/A
What is the actual likely impact?	N/A
How have you, or will you, put the Policy into practice, and who is or will be responsible for delivering it?	
How does the Policy fit into our wider or related policy initiatives?	The policy is intended to enhance our privacy policy and will form part of our overall Information Security Strategy
Do you have a set budget for this work?	N/A