Policy: Information and Communication technology

MUIRHOUSE HOUSING ASSOCIATION

Title of Policy:	Information and Communication Technology
Date of Adoption or Last Review:	11 September 2019
Lead Officer:	Grit Nielsen, Corporate Services Team Leader
Date of Next Review:	September 2022
Regulatory Standards of Governance and Financial Management	**Standard 5** The RSL conducts its affairs with honesty and integrity.

1 Introduction

1.1 The introduction of e-mail, internet and social media platforms has greatly facilitated internal as well as external communication throughout the world. Unfortunately, these communication tools also have the potential for misuse.

1.2 This policy is a group policy and any references to Muirhouse Housing Association (“MHA”, “us”, “we”) is a reference to the group structure, including all subsidiaries.

2 Purpose

2.1 This policy sets out the MHA’s guidelines on access to and the use of the Association's computers and communication tools. It also sets out the action which will be taken when breaches of the guidelines occur.

2.2 You are only permitted to use our computer systems in accordance with our Privacy Policy, Access Control Management Policy and the following guidelines.

2.3 This policy also sets out our position on employees' use of social networking sites and blogs, whether conducted on MHA media and in work time or your own private media in your own time.

2.4 The policy aims to ensure that use of communication tools among our users is consistent with its own internal policies, all applicable legislation, and the individual user's job responsibilities.

2.5 The policy also aims to establish basic guidelines for appropriate use of the communication tools.

3 Scope

3.1 This policy applies to all employees of MHA in all locations including the Board Members, NonExecutive Directors, temporary employees and contracted staff/relevant contractors.

3.2 It also includes;

- All MHA employees whilst engaged in work for MHA at any location, on any computer or internet connection.
- Any other use by MHA employees which identifies the person as a MHA employee or which could bring MHA into disrepute on any computer or internet connection.
- Other persons working for/with MHA, persons engaged on MHA business or persons using MHA equipment and networks.
- Anyone granted access to use computer systems on the MHA IT network.

4 Definitions

4.1 The term ‘communication tools’ will be used throughout this policy to refer to email, internet and social media platforms.

5. Access

5.1 Access to MHA’s computer systems are provided in line with our “Access Control Management” Policy.

5.2 You must only log on to the MHA’s computer systems using your own password which must be kept secret. You should select a password that is not easily broken, and which meets the basic password requirements as outlined by our IT Support Provider.

5.3 It is our intent as far as possible to provide basic, network-connected communication tools for the use of staff and, when relevant, governing body members to support communication, learning and service activities. It is also our intent to provide a communications link between our own e-mail system and the mail systems that operate on other data networks.

6. Proper Use

6.1 To safeguard MHA’s computer systems from viruses, you should take care when opening documents or communications from unknown origins. Attachments may be blocked if they are deemed to be potentially harmful to our computer systems. Certain websites may be blocked for access if they are deemed potentially harmful as well.

6.2 All information, documents, and data created, saved or maintained on the Association's computer system remains at all times the property of the Association.

6.3 Where the computer systems contain an e-mail facility, you should use that e-mail system for business purposes only.

6.4 E-mails should be written in accordance with the standards of any other form of written communication and the content and language used in the message must be consistent with best practice.

6.5 All external e-mails must have the appropriate signature and Association approved disclaimers attached before they are sent.

6.6 E-mails can be the subject of legal action (for example, claims of defamation, breach of confidentiality or breach of contract) against both the employee who sent them or MHA. As e-mail messages may be disclosed to any person mentioned in them, you must always ensure that the content of your e-mails is appropriate.

6.7 Abusive, obscene, discriminatory, harassing, derogatory or defamatory e-mails must never be sent to anyone. If you do so, you may be liable to disciplinary action up to and including dismissal without notice.

6.8 If your job duties require you to speak on behalf of MHA in an online social media environment without prior training, you must agree such communication with your line manager or another senior member of staff. You may be required to have training before you are permitted to participate in social media on behalf of MHA.

6.9 Similarly, if you are asked to comment about MHA for publication anywhere, including on any social media outlet, you must not respond without prior approval from the Chief Executive.

6.10 Examples of misuse of MHA's computer system and communication tools include, but are not limited to, the following:

- accessing online chat rooms, blogs, social network sites and use of on-line auction sites
- the purchase or sale of personal items via internet sites
- sending, receiving, downloading, displaying or disseminating material that discriminates against, degrades, insults, causes offence to or harasses others
- accessing pornographic or other inappropriate or unlawful materials
- engaging in online gambling
- forwarding electronic chain letters or similar material
- downloading or disseminating copyright materials
- issuing false or defamatory statements about any person or organisation via any communication tool
- The use of communication tools for political purposes
- unauthorised sharing of confidential information about the MHA or any person or organisation connected to us, and
- loading or running unauthorised games or software

7. Private use of Communication Tools

7.1 Social networking sites and blogs offer a useful means of keeping in touch with friends and colleagues, and they can be used to exchange views and thoughts on shared interests, both personal and work-related. We do not prohibit employees from listing Muirhouse Housing Association as their employer however we do advise against it.

7.2 MHA does not object to you setting up personal accounts on social networking sites or blogs on the internet, in your own time and using your own computer systems.

7.3 You must not link your personal social networking accounts or blogs to the MHA's website. Any such links require MHA's prior consent.

7.4 You must not disclose MHA confidential information, breach copyright, defame MHA, our customers, suppliers or employees, or disclose personal data or information about any individual that could breach the Data Protection Act 2018.

7.5 Social networking site posts or blogs should not be insulting or abusive to employees, suppliers, stakeholders, Board Members or customers.

7.6 If reference is made on your personal blog to your employment or to MHA, you should state to the reader that the views that you express are your views only and that they do not reflect the views of Muirhouse Housing Association. You should include a notice such as the following:

- *'The views expressed on this website/blog are mine alone and do not reflect the views of my employer'*

7.7 You should always be conscious of the Code of Conduct and of your duty as an employee to act in good faith and in the best interests of the MHA under UK law. We will not tolerate criticisms posted in messages in the public domain or on blogs about MHA or any other person connected to us.

7.8 You must not bring MHA into disrepute through the content of your website entries or your blogs.

8. Monitoring

8.1 MHA will not monitor the use of communication tools as a routine procedure. Certain staff, due to the specific responsibilities of their role, may require access to individual's hardware and software within MHA and personal files or resources contained within them.

8.2 Whilst we do not monitor the use of communication tools as a routine procedure, MHA reserves the right to monitor, intercept and review, without further notice, employee activities using our IT resources and communications tools. We will do so only when we believe it is appropriate to prevent or correct improper use, satisfy a legal obligation, or ensure proper operation of the electronic mail facilities. If it is necessary to obtain access the appropriate approval will be sought first by an Authorised Approver, in line with our Access Control Management Policy.

8.3 Employees consent to such monitoring by your use of our computer systems and communication tools.

9 Policy Breaches

9.1 MHA provides tools to support its communication, learning and service activities and associated administrative functions. Any use of these facilities which interferes with our activities and functions or does not respect the image and reputation of MHA will be regarded as breaching this policy.

9.2 Failure to adhere to this policy jeopardises network security and puts users at risk of potential misuse of the system by other individuals. Network users may be held responsible for all actions taken using their personal network access permissions.

9.3 If Senior staff are concerned about an employee's breach of this policy, e.g. excessive use of electronic mail for personal use or spending large quantities of time on personal social media, they will:

- Review whether or not expectations and standards in this area have been well communicated and made clear to the user.
- Pursue direct communication with the user regarding the issue.
- Use appropriate procedures to take any disciplinary action.

9.4 Any evidence of misuse may result in disciplinary action up to and including dismissal without notice. If necessary, information gathered in connection with the investigation may be handed to the police.

10. Diversity and Equality

10.1 We are committed to Equality and Diversity and will not discriminate in the operation of this policy on the basis of age, sex, race, colour, ethnic or national origin, religion, marital status, family circumstances, political or sexual orientation, medical condition or disability. We aim to promote equal opportunities and comply with all current legal requirements relating to equal opportunities and the Equality Act 2010.

11 Confidentiality and Data Protection

11.1 All information provided to us by individuals will be treated in strict confidence and will only be discussed with other parties with the individual's (or their appointed representative's) prior consent. We will comply with the Data Protection Act 2018 and the General Data Protection Regulation 2016 when holding personal information in our files and on our computer systems.

12 Review

12.1 This Policy will be reviewed every three years or earlier if there are any requirements for changes.