Internet and E Mail Policy

Yorkhill Housing Association Ltd

Internet and Email Policy

Approved by Management Committee 28th June 2021

Date for renewal 28TH June 2024

1. Introduction

1.1 The advent of electronic mail, the Internet and social media platforms has greatly facilitated internal as well as external communication throughout the world. Unfortunately however these communication tools also have the potential for misuse.

1.2 This policy formalises the Association's use of E-mail, Internet and Social Media Platforms.

1.3 While focusing on these, the principles and procedures are consistent with existing statements applying to the many other forms of communication within Yorkhill Housing Association.

1.4 Throughout this policy the term "E-mail" should be taken to include Internet and Social Media Platform usage.

2. Regulatory Standards

2.1 Regulatory Standard 4 – Governance and Financial Management.

The governing body bases its decisions on good quality information and advice and identifies and mitigates risks to the organisation's purpose.

The governing body identifies risks that might prevent it from achieving the RSL's purpose and has effective strategies and systems for risk management and mitigation, internal control and audit.

3. Principles

3.1 This policy applies to all members of the Yorkhill Housing Association and refers to all E-mail, Internet resources and social media platforms at Yorkhill Housing Association.

3.2 Individual departments and administrative units may define additional 'conditions of use' for E-mail facilities under their supervision. Any such additional conditions must be consistent with this overall policy but may include more detailed guidelines and, where necessary, appropriate additional restrictions.

3.3 Any person who uses Yorkhill Housing Association electronic communication facilities consents to all of the provisions of this policy and agrees to comply with all of its terms and conditions and with all applicable laws and regulations.

3.4 Any user of the E-mail system, whose actions violate this policy, or any other Yorkhill Housing Association policy or regulation, may be subject to limitations or elimination of electronic mail privileges as well as other disciplinary actions.

3.5 The policy aims to ensure that use of E-mail among Yorkhill Housing Association users is consistent with its own internal policies, all applicable laws, and the individual user's job responsibilities.

3.6 The policy also aims to establish basic guidelines for appropriate use of these resources. A detailed user guide is included in Appendix 1.

4. Access

4.1 It is the Yorkhill Housing Association's intent, as far as possible, to provide basic network-connected E-mail and Internet facilities for the use of staff and committee members.

4.2 It is also the Association's intent to provide a communications link between its own E-mail system and the mail systems that operate on the national and international data networks.

4.3 The primary purpose of such access is to encourage greater business efficiency and to enhance knowledge, learning and communication opportunities for the organisation as a whole and its people as individuals.

4.4 Occasional and incidental social communications using E-mail are not disallowed by this policy and are permitted so long as this does not interfere with the performance of expected duties. However, each user should comply with specific policies of their individual unit/section/department.

4.5 Any manager concerned about an employee's potential violation of the Yorkhill Housing Association's proper use principles (for example, excessive use of electronic mail for personal use or spending large quantities of time in electronic social conferencing) should not unilaterally seek to gain access to an user's electronic communications. Instead, the manager should:

- 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.

- Proceed as one would handle any personnel-related disciplinary action.

4.6 All Association users must refrain from accessing business email accounts via personal mobile devices which are not protected with the Associations security software.

5. Proper Use

5.1 E-mail is a very informal medium. It is closer to speech than a written communication, and yet there is a permanent written record. It typically lacks the care given to a written communication, and can often be stilted, abbreviated conversational language with heavy use of emoticons.

In addition, it is often the case that people 'say' things in E-mail and on-line which they might not otherwise feel comfortable communicating to others.

A combination of such informalities has the potential to create potentially dangerous situations such as:

- sending E-mail containing negligent misstatements or binding the organisation in other ways.

- using E-mail to conduct harassment on colleagues or others (E-mail seems to be a fairly common ingredient in workplace harassment cases and under existing anti-discrimination legislation, and an employer can be liable for acts of his employees, whether or not done with the employer's knowledge or approval).

5.2 The following general protocol is therefore intended to guide users on the Yorkhill Housing Association's standards in these areas:

- local rules will make clear the extent to which personal use is allowed.

- confidential information should not be transmitted by E-mail, unless it is encrypted.

- external E-mail messages should have appropriate signature files and disclaimers attached.

- users should be familiar with general housekeeping good practice (for example, the need to delete E-mail messages regularly).

- users should use appropriate etiquette when writing E-mail messages; the use of capital letters, for example, is considered to be the equivalent of shouting and could cause offence.

- User should not send one long e-mail covering multiple topics. Send several short e-mails each covering a single topic and then it is easy for people to follow. Never assume that people have read your e-mail when you next see them.

- inappropriate messages are prohibited including those which are sexually harassing or offensive to others on the grounds of age, physical ability, race, religion or gender.

- if you are the recipient of such messages you should raise your concerns with your manager immediately.

- you also have the right to raise a grievance should you receive offensive E-mail or be concerned over a colleague's general use of the Internet/E-mail resources.

- users must not send potentially defamatory E-mail messages which criticise other individuals or organisations.

- users must not access or download inappropriate material, such as pornography, from the Internet.

- users should take care not to infringe copyright when downloading material or forwarding it to others.

- users should take care to ensure that the email messages are sent to the correct recipient and must ensure that the Auto complete function is not enabled.

- chain emails are strongly discouraged and should be avoided.

- users are discouraged from using Emoji's in business emails.

6. Some Specific Examples of Improper Use

6.1 As mentioned earlier, Yorkhill Housing Association provides electronic mail facilities to support its communication, learning and service activities and associated administrative functions.

Any use of the facilities that interferes with these activities and functions or does not respect the image and reputation of the Yorkhill Housing Association is therefore improper.

In general, policies and regulations that apply to other forms of communications at the Yorkhill Housing Association also apply to electronic mail.

In addition, the following specific actions and use of electronic mail are improper:

- Concealment or misrepresentation of names or affiliations in E-mail messages.
- Alteration of source or destination addresses of E-mails.
- Use of E-mail facilities for commercial or private business purposes.
- Use of E-mail, which unreasonably interferes with or threatens other individuals.
- Use of E-mail that degrades or demeans other individuals – whether Yorkhill Housing Association employees or others.
- Commercial use - any form of commercial use of the Internet is prohibited.
- Solicitation - the purchase or sale of personal items through advertising on the Internet is prohibited.
- Harassment - the use of the Internet to harass employees, vendors, customers, and others is prohibited.
- Political - the use of the Internet for political purposes is prohibited.
- Misinformation/Confidential Information, the release of untrue, distorted, or confidential information regarding Yorkhill Housing Association business is prohibited.
- Viewing/Downloading purely entertainment sites or material where there is no benefit to Yorkhill Housing Association in terms of its learning, communication or service aims described earlier.

7. Generic Terms

7.1 Some generic terms for much of the above are as follows and are expressly prohibited under this policy:

7.1.1 Spamming

Spam is broadly defined as unsolicited E-mails sent to a large number of recipients, and its content is not Yorkhill Housing Association business related. The Association's E-mail accounts are not allowed to be used for the purpose of sending SPAM messages.

Not only is this a misuse of The Association's resources, but it can also result in external sites 'black listing' the Association, prohibiting delivery of any future E-mails to our location.

7.1.2 Chain letters and Pyramid Schemes

These E-mail messages are sent to a specific number of people, usually professing a 'get rich quick' scheme. The recipients are then asked to forward the message on to the same number of people.

These types of messages are illegal and not allowed on the Yorkhill Housing Association. Accounts found associated with chain letters or pyramid schemes may be turned off without warning.

7.1.3 Spoofing

Spoofing refers to someone sending mail that 'appears' to be from someone else. This is the same as forging someone else's identity.

7.1.4 Harassment

Harassment via E-mail, as with other avenues of communication, is prohibited.

8. Social Media Platforms

8.1 Yorkhill Housing Association respects the right to a private life and that includes joining any social media platforms such as employees wish. However, information posted on such sites is classed as public and not private.

8.2 Employees are therefore not allowed to discuss Association business or disclose any information relating to Yorkhill Housing Association, its customers, partners, suppliers, board members, employees, or stakeholders on any social networking platforms outwith the Association's official accounts.
Examples of such platforms include Facebook, Twitter, What's App,

and Snapchat.

8.3 It is also prohibited to post any comments on people and events connected to Yorkhill Housing Association, or make any remarks which could potentially bring Yorkhill Housing Association into disrepute.

8.4 Any such actions could result in disciplinary action, including dismissal.

8.5 If using social media platforms employees are required to adhere to the following;

- keep profiles set to private and protect tweets.
- ensure all passwords are kept private.
- the Association does not prohibit employees from listing Yorkhill Housing Association as their employer however doing this is not advised.

8.6 Employees should be aware of the language and content of their posts – in particular where employees have an association with their employer for example, listing their employer or linked with colleagues.

9. Privacy

9.1 Yorkhill Housing Association's view on privacy issues is best set out by the answers to the following questions that are typically most often raised in this area.

9.1.1 What is unauthorised access to information resources in this regard*?*

Generally, a good guideline to follow is that authors or parties to E-mail should be the primary sources of authorisation in granting access to their information or files. Third party access to electronic mail ordinarily may only be accomplished through either the sender or the recipient(s) of that mail.

9.1.2 Is it possible to invade the privacy of individuals, and if so is authorisation always required?

Since Yorkhill Housing Association's resources are being used to create and store files, users should understand that the Association must assign certain individuals responsibility for maintaining, repairing, and further developing those resources.

In the normal course of doing their assigned work some individuals, by virtue of their positions within the Association and their specific responsibilities, may have special access privileges to hardware and software and therefore to the content that resides in those resources.

Yorkhill Housing Association will strive to protect individual privacy by ensuring that the number of individuals with this level of access is strictly limited and that such individuals are selected for their judgment and ethics, as well as their technical expertise. Such positions, and the individuals who hold them, will be governed through defined responsibilities and procedures. (See later for 'Standards for System Administrators').

9.1.3 How possible is it that electronic mail might be inadvertently seen?

All users should be aware that E-mail may pass out of one machine environment, across a network, and into another totally different machine environment even within Yorkhill Housing Association itself. This transport becomes increasingly complicated as mail travels between offices, regions and countries.

Each time the information technology hardware, software, and service environment changes, the level of security may be affected. In addition to differing security levels in different machine environments, electronic mail may also be compromised because of an individual's own difficulty in sending a message to an intended recipient.

The sender may be uncertain about remote addressing; the message may not be deliverable, and a rejection message may be generated. If such rejections can be delivered to the original sender, ordinarily no person sees the message. If, however, the message can't be delivered to the original sender, systems can be configured to either pass the message to someone (system administrator) for assistance or to discard the rejection without the sender knowing anything about the problem.

9.1.4 Who are the 'system administrators' and what role should they play?

System Administrators are individuals who have the specific duties of enabling undeliverable mail to reach its destination, handling other delivery problems, and answering user questions about mail travel.

Users should know that mail that is deliberately sent to system administrators for advice or mail that is undeliverable will be seen by others. System Administrators should therefore observe procedures and privacy standards analogous to those used by postmasters who receive letters in a post office.

9.1.5 What material may be retrievable if required by law?

Because systems on which users carry out their communications and computing vary widely, so too do back up and save procedures.

Users need to be informed about the back-up procedures in the environment in which they are working because those procedures will ultimately determine what information has been retained in the course of backing up the system and perhaps what may be accessible by others through legal means.

For instance, within some system environments, a deleted or expired message will entirely disappear and be irretrievable after 28 days. (In some environments senders may have the facility override the automatic expiration of messages by specifying longer parameters.)

Messages that become part of a forwarding or history chain may be retrievable longer. File save procedures in each environment determine what material is saved and in what form.

While Yorkhill Housing Association E-mail administrators will not monitor the contents of mail messages as a routine procedure, the Association does reserve the right to inspect, copy, store, and disclose the contents of electronic mail messages at any time.

However, it will do so only when it believes it is appropriate to prevent or correct improper use, satisfy a legal obligation, or ensure proper operation of the electronic mail facilities.

Any E-mail administrator or postmaster who believes such actions are necessary must first obtain the approval of the Chief Executive.

10. Security

10.1 Security, including protection from viruses as well as security of Yorkhill Housing Association's information, is a concern with ~~both~~ Internet. E-mail and Social Media use.

10.2 Access to E-mail and the Internet is restricted to authorised persons. Users are responsible for the security of their own passwords, which protect against unauthorised access.

10.3 Regularly changing of E-mail and Internet passwords is recommended every 90 days.

10.4 Passwords should be over 8 characters and should contain a mix of alpha, numeric, symbols, special characters etc. Strong passwords should not contain personal names.

10.5 Users should keep personal log-ons and passwords confidential and change passwords on a regular basis as instructed by Information Services procedures.

10.6 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.

10.7 In a further effort to ensure the security of our systems and the information placed on it by users, the Yorkhill Housing Association has local rules, which govern the downloading, and uploading of files. Webroot Virus detection software is installed on individual workstations/laptops and servers.

10.8 If you do not know how to do this or don't fully understand the conventions involved here you should seek advice from your manager or system administrator?

11. Standards for System Administrators

11.1 System Administrators have specific responsibilities and access capabilities. Because of these special access capabilities they are expected to exercise special care in order to protect the privacy of the individuals whose electronic communications they handle.

11.2 System Administrators shall maintain the following standards:

- Use machine headers and machine-generated messages in order to return undeliverable mail.
- Avoid reading message content to the greatest degree possible.
- Inform users of procedures for providing service, and assiduously attempt to respect privacy. Inform users and be straightforward if something goes wrong, in order to maintain trust. Keep confidential the content of any message that was inadvertently read in the course of redirecting undeliverable mail.
- Consult with users first if it seems necessary to go beyond machine-generated explanations
- Be informed about and follow Yorkhill Housing Association policy regarding privacy in electronic communication.
- Advise all users on any restrictions on the size and type of files that may/may not be downloaded.

11.3 System administrators have a particular role in determining where on the security versus service continuum their particular mail system resides. They must inform their users of the tradeoffs between service and security that exist on their system.

11.4 System administrators will therefore need to take specific actions to ensure, to the greatest degree possible, that Yorkhill Housing Association policy is followed and that users are informed about the degree of privacy of their communications.

11.5 The following list of information items will help users be as knowledgeable as possible about the systems that they use. It will also help system administrators manage the issues of electronic mail and privacy.

System Administrators should be able to answer questions for users on the following:

- Is undeliverable mail discarded, examined for delivery clues, or automatically returned to sender?

- Is message content stripped from rejected or undeliverable mail?

- Are messages stored in clear text or encrypted while waiting to be delivered? How are they stored after delivery?

- What effect does file system backup have? Is E-mail backed up? How long are backups retained? How often are backups made?

- Where is the mail stored while waiting to be delivered and after delivery? How secure is that location?

- When I delete a message is it gone?

- Does the system make a copy of rejections? With text or without?

- If I go off site, how long is my mail held for me? Are there limits on how much mail I can receive, store, and have waiting?

- How long will my machine try to deliver outgoing mail before returning it as undeliverable?

- Is there a way my mail can be absolutely private and what rules apply to me in this regard?

- Should I send sensitive documents by E-mail?
- Can I encrypt mail?
- What kind of security features are available to me now? What is planned for the future, and when will that become available?

11.6 There are several recommended actions that a system administrator may wish to consider and/or take:

- Use encryption software packages.
- Install a filter to keep text from view of postmasters or others.
- Require postmasters and others to adjust windows on their screens in order to exclude text.
- Train and expect those with special access privileges to 'attention out' before the text of a message scrolls by.
- Set a standard of asking the user's permission prior to looking at text.
- Train and expect those with special access to use special self-restraint or to ignore the content of any private message/file.

11.7 System Administrators will not routinely examine E-mail content unless there are good reasons to suspect the system is being abused and the rules ignored.

12. Data Protection Act 2018/UK GDPR

12.1 The organisation will treat your personal data in line with its obligations under the Data Protection Act 2018/UK GDPR.

12.2 Information regarding how your data will be used and the basis for processing your data is provided in the Association's Employee Privacy Notice.

Appendix 1:

Email usage guidance incoming mail (provided by Brightridge Ltd)

Email is both an excellent communication tool and also a way that companies can inform you about their latest products and services.

However, email is frequently used to deliver unwanted material which is at best, annoying and at worst, malicious – causing considerable harm to your computer and yourself.

These include the following:

Spam (or Junk) email

- Always be vigilant when receiving or responding to emails.
- Make sure your spam filter is always switched on to minimise the risks.

Viruses & Spyware

The vast majority of email sent every day is unsolicited junk mail. Examples include:

- Advertising, for example online pharmacies, pornography, dating, gambling, get rich quick and work from home schemes, hoax virus warnings, hoax charity appeals.
- Chain emails which encourage you to forward them to multiple contacts (often to bring 'good luck').

How to spot spam

Spam emails may feature some of the following warning signs:

- You don't know the sender.
- Contains misspellings (for example 'p0rn' with a zero) designed to fool spam filters.
- Makes an offer that seems too good to be true.
- The subject line and contents do not match.

- Contains an urgent offer end date (for example “Buy now and get 50% off”).
- Contains a request to forward an email to multiple people, and may offer money for doing so.
- Contains a virus warning.
- Contains attachments, which could include .exe files.

The risks

It can contain viruses and spyware, it can be a vehicle for online fraud. Unwanted emails can contain offensive images and manual filtering and deleting is very time consuming.

Email Scams

Scams are generally delivered in the form of a spam email (but remember, not all spam emails contain scams). Scams are designed to trick you into disclosing information that will lead to defrauding you or stealing your identity.

Examples of email scams include:

- Email’s offering financial, physical or emotional benefits, which are in reality linked to a wide variety of frauds.
- These include emails posing as being from ‘trusted’ sources such as your bank, HMRC or anywhere else that you have an online account. They ask you to click on a link and then disclose personal information.

Phishing emails

Phishing is a scam where criminals typically send emails to thousands of people. These emails pretend to come from banks, credit card companies, online shops and auction sites as well as other trusted organisations.

They usually try to trick you into going to the site, for example to update your password to avoid your account being suspended.

The embedded link in the email itself goes to a website that looks exactly like the real thing but is actually a fake designed to trick victims into entering personal information.

- The email itself can also look as if it comes from a genuine source. Fake emails sometimes display some of the following characteristics, but as fraudsters become smarter and use new technology, the emails may have

none of these characteristics. They may even contain your name and address.

- The sender's email address may be different from the trusted organisation's website address.
- The email may be sent from a completely different address or a free webmail address.
- The email may not use your proper name, but a non-specific greeting such as "Dear customer."
- A sense of urgency; for example the threat that unless you act immediately your account may be closed.
- A prominent website link. These can be forged or seem very similar to the proper address, but even a single character's difference means a different website.
- A request for personal information such as username, password or bank details.
- You weren't expecting to get an email from the organisation that appears to have sent it.
- The entire text of the email may be contained within an image rather than the usual text format. The image contains an embedded link to a bogus site

Use email safely

Do not open emails which you suspect as being scams. Do not open attachments from unknown sources. Do not forward emails which you suspect as being scams.

- If in doubt, contact the person or organisation the email claims to have been sent by ... better safe than sorry.
- Do not readily click on links in emails from unknown sources. Instead, roll your mouse pointer over the link to reveal its true destination, displayed in the bottom left corner of your screen. Beware if this is different from what is displayed in the text of the link from the email.
- Do not respond to emails from unknown sources.

- Do not make purchases or charity donations in response to spam email.
- Don’t click on ‘remove’ or reply to unwanted email.
- Check junk mail folders regularly in case a legitimate email gets through by mistake.
- When sending emails to multiple recipients, list their addresses in the 'BCC' (blind copy) box instead of in the 'To' box. In this way, no recipient will see the names of the others, and if their addresses fall into the wrong hands there will be less chance of you or anybody else receiving phishing or spam emails.
- Similarly, delete all addresses of previous parties in the email string, before forwarding or replying.
- If you are suspicious of an email, you can check if it is on a list of known spam and scam emails that some internet security vendors such as McAfee and Symantec feature on their websites.