Communication Tools Policy

DATE OF REVIEW: 17.04.2019

DATE OF APPROVAL: 17.04.2019

DATE OF NEXT REVIEW: APRIL 2022

Dalmuir Park Housing Association can provide this document on request, in different languages and formats, including Braille and audio formats.

Purpose:	To establish DPHA's policy and set out our position on usage of e-mail, internet and social media.
Review Date:	3 years from review date
Guidance:	EVH Model Policy Findings from ICO advisory visits to social housing organisations Feb 2014 ACAS Social Media in the Workplace advice and guidance Code of Conduct Staff and Management Committee
Regulatory Standards:	4. The governing body bases its decisions on good quality information and advice and identifies and mitigates risks to the organisation's purpose 4.1. The governing body ensures it receives good quality information and advice from staff and, where necessary, expert independent advisers, that is timely and appropriate to its strategic role and decisions. The governing body is able to evidence any of its decisions.
Other Relevant Policies	IT Security Privacy Policy Staff and Committee Code of Conduct
Date reviewed by Policy Review Working Group (PRWG):	17 April 2019
Date approved by Management Committee (or PRWG if delegated):	17 April 2019
Amendments	*17 April 2019*
Publish on Website:	No

CONTENTS **PAGE NO.**

LIST OF APPENDICES

Dalmuir Park Housing Association can provide this document on request, in different languages and formats, including Braille and audio formats.

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

1.2 This policy sets out the standards expected of DPHA's employees, workers, committee members, stakeholders, consultants and agency staff when using communication tools whether that be in connection with DPHA's business or in the case of social media platforms, the expression of views that contradict, oppose or infringe on the purpose, ethos or principles of DPHA.

2.0 PRINCIPLES

- This policy applies to all employees, workers, committee members, stakeholders, consultants and agency staff of DPHA and refers to communication tools at DPHA

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

- Any person who uses DPHA communication tools 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

- Any user of the communication tools whose actions violate this policy or any other DPHA policy or regulation, may be subject to limitations or removal of any communication tool privileges in addition to disciplinary action in accordance with DPHA's disciplinary procedures

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

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

3.0 LEGAL AND REGULATORY REQUIREMENTS

3.1 The **Human Rights Act 1998** Article 8 gives a 'right to respect for private and family life, home and correspondence'. Employees have a reasonable expectation of privacy in the

workplace.

3.2 The **Data Protection Act 1988** and **General Data Protection Regulations** cover how information about employees and job applicants can be collected, handled and used.

3.3 The **Regulation of Investigatory Powers Act 2000** covers the extent to which organisations can use covert surveillance.

4.0 ACCESS

4.1 It is DPHA's intent as far as possible to provide basic, network-connected communication tools for the use of staff and management committee members. It is also DPHA'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.

4.2 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.

4.3 Occasional and incidental social communications using any communication tools are not disallowed by this policy and are permitted so long as this does not interfere with employees' performance of their expected duties. However, each user should comply with the relevant policies of the Association.

4.4 Use of the Internet must not be for illegal or offensive purposes. Examples include (but are not limited to) sexually explicit, pornographic, distasteful or racist material. Specifically, such material may not be archived, stored, distributed, edited or recorded using Association network or computing resources. The Association will actively log and monitor all traffic between Association personnel and the Internet. This will include details of all sites visited. Logs will be reviewed on a periodic basis, and disciplinary action may be taken against individuals who visit inappropriate sites.

4.5 As a general principle access to communication tools via DPHA's resources will not be available out with office hours except where prior permission has been sought and granted.

5.0 PROPER USE

5.1 Communication tools are very informal mediums. They are closer to speech than more formal written communications, yet there is a permanent written record. It typically lacks the care given to 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 (via social media platforms) that they might not otherwise feel comfortable communicating to others face to face.

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

- Sending e-mails or posting comments on social media platforms containing negligent misstatements or binding the organisation in other ways

- Harassment of colleagues or others (e-mail and social media networks are common in workplace harassment cases and under existing anti-discrimination legislation, an employer can be liable for acts of their employees, whether or not done with the employer's knowledge or approval)

5.3 The following is a guide on DPHA's standards and is not exhaustive:

- Confidential information should not be transmitted by communication tools 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 (e.g. the need to delete messages regularly)

- Users should use appropriate etiquette when writing using communication tools. The use of capital letters, for example, is considered the equivalent of SHOUTING

- Inappropriate messages are prohibited including those which contradict, oppose or infringe on the purpose, ethos or principles of DPHA

- If a member of staff is in receipt of such messages, they should raise any concerns with their line manager immediately

- Staff also have the right to raise a grievance should they receive offensive communication messages from a fellow employee

- If there is concern over a colleague's general conduct using communication tools this must be raised immediately with their line manager

- Users should not send potentially defamatory communication messages which criticise other individuals or organisations

- Users should not access or download inappropriate material, such as pornography, from communication tools

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

6.0 SOCIAL MEDIA FORMS

6.1 DPHA respects the right to a private life and that includes joining any social media platforms employees wish. However, information posted on such sites is classed as public and not private. Employees are therefore not allowed to disclose confidential information relating to DPHA, its customers, partners, suppliers, committee members, employees, or stakeholders on any social networking platforms. It is also prohibited to post any comments on people and events connected to DPHA or make any remarks which could potentially bring DPHA into disrepute. Any such actions could result in disciplinary action, including dismissal.

6.2 If using social media platforms employees are expected to adhere to the following;

- Keep profiles set to private and protect tweets
- Ensure all passwords are kept private
- We do not prohibit employees from listing DPHA as their employer however we do advise against it
- Employees should be aware of the language and content of their posts – where employees have an association with their employer e.g. listing their employer or linked with colleagues

7.0 POLICY BREACHES

7.1 As mentioned earlier, DPHA provides tools to support its communication, learning and service activities and associated administrative functions. Any use of these facilities that interferes with DPHA's activities and functions or does not respect the image and reputation of DPHA will be regarded as breaching this policy.

7.2 Any line manager 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 social media, should not unilaterally seek to gain access to a 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 disciplinary action using the appropriate procedures

7.3 The following are some examples of breaches of this policy and is not exhaustive:

- Concealment or misrepresentation of names or affiliations in e-mail messages
- Alteration of source or destination addresses of e-mail
- Use of communication tools for commercial or private business purposes
- Use of communication tools, in a way that unreasonably interferes with or threatens other individuals
- Use of communication tools that degrades or demeans other individuals – whether DPHA employees or others
- Any form of commercial use using communication tools is prohibited
- The purchase or sale of personal items through advertising on the internet
- The use of communication tools to harass employees, vendors, customers, and others
- The use of communication tools for political purposes
- The release of untrue, distorted, or confidential information regarding DPHA business via communication tools
- Viewing/downloading purely entertainment sites or material where there is no benefit to DPHA in terms of its learning, communication or service aims described earlier.

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

7.4.1 **Spamming**

Spam is broadly defined as unsolicited, e-mail sent to a large number of recipients, and its content is not related to the business activities of DPHA business related. DPHA's e-mail accounts are not allowed to be used for the purpose of sending SPAM messages. Not only is this a misuse of DPHA resources, but it can also result in external sites "blacklisting" DPHA, prohibiting delivery of any future e-mails to our location.

7.4.2 **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 in DPHA.

Accounts found associated with chain letters or pyramid schemes may be turned off without warning.

7.4.3 **Spoofing**

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

7.4.4 **Harassment**

Harassment (cyber bullying) via any communication tool as specified in DPHA's equality & diversity policy, as with other avenues of communication, is prohibited.

7.4.5 Phishing

Staff should take steps to avoid phishing scams and other attempts by hackers to steal passwords and other sensitive information. All Staff will receive training on how to recognise these attacks and ensure they do not open any emails or attachments which look suspicious.

8.0 PRIVACY

8.1 Authors or parties to communication messages should be the primary sources of authorisation in granting access to their information or files. Third party access to email ordinarily may only be accomplished through either the sender or the recipient(s) of that mail.

8.2 Certain staff, due to the specific responsibilities of their role, require access to individual's hardware and software within DPHA and personal files or resources contained within them.

8.3 It is important that all users are aware that there is the possibility that security levels can, and do, vary when a message is sent. This can result in messages being visible to others other than the intended recipient.

8.4 DPHA will inform all users of the backup system in use and how this affects the retrieval of any data on DPHA's systems.

8.5 DPHA will not monitor the contents of messages as a routine procedure. However, DPHA does reserve the right to inspect, copy, store, and disclose the contents of electronic messages at any time. 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. If it is necessary to obtain access the appropriate approval will be sought first.

9.0 SECURITY

9.1 Security of DPHA's information and systems including protection from viruses through communication tools is a serious concern for DPHA. As a result, all users must keep personal log-ons and passwords confidential and change passwords on a regular basis as instructed by IT Security procedures. Failure to adhere to this policy jeopardises network security, puts users at risk of potential misuse of the system by other individuals and is a disciplinary matter. Network users may be held responsible for all actions taken using their personal network access permissions.

9.2 In a further effort to ensure the security of our systems and the information on it, DPHA IT Security Policy further details the downloading, and uploading of files. Virus detection software is installed on individual workstations and the network. However, users are responsible for virus checking any downloaded files.

9.3 For additional data security cloud-based media storage will be restricted and all DPHA PC hard drives will have restricted access to add, transfer or remove data. Only certain authorised staff members will have permission to do this. Staff are therefore prohibited to add, remove or download or upload any mass data unless authorised to do so. Guidance on processing any electronic personal information can be obtained from DPHA Data Protection/Privacy Policy.

9.5 All electronic information passed to third parties should be in accordance with DPHA's Data Protection/Privacy Policy.

9.6 This policy will be updated as appropriate. If any individual requires further clarification with anything contained in this policy, they must speak to the Senior Corporate Services Officer.

10.0 GDPR

10.1 We will treat personal data in line with our obligations under the current data protection regulations and our Privacy Policy. Information regarding how data will be used and the basis for processing data is provided in our Employee Fair Processing Notice.

APPENDIX A

DECLARATION FORM - Communication Tools Policy

I confirm I have read through and fully understand the terms of Dalmuir Park Housing Association's Communication Tools Policy. I also understand that DPHA may amend this policy from time to time and that I will be issued with an amended copy.

Name: _____ **Job title:** _____

Signed: _____ **Date:** _____