West Granton
Housing Co-op
sustaining and championing the co-operative way

INFORMATION, COMMUNICATIONS & TECHNOLOGY POLICY

This policy was approved by the Committee of Management on 19th May 2021.
It should be reviewed again no later than 30 April 2024.

The policy has been assessed through the organisational impact assessment process.

We can, if requested, produce this document in different formats such as larger print or audio-format. We can also translate the document into various languages, as appropriate.

SCOTTISH HOUSING REGULATOR STANDARDS

STANDARD 1:
The governing body leads and directs the RSL to achieve good outcomes for its tenants and other service users.

STANDARD 2:
The RSL is open about and accountable for what it does. It understands and takes account of the needs and priorities of its tenants, service users and stakeholders. Its primary focus is the sustainable achievement of these priorities.

STANDARD 4:
The governing body bases its decisions on good quality information and advice and identifies and mitigates risks to the organisation's purpose.

STANDARD 5:
The RSL conducts its affairs with honesty and integrity.

STANDARD 6:
The governing body and senior officers have the skills and knowledge they need to be effective.

Contents

1.0 INTRODUCTION

This policy should not be confused with other policies that reference 'information' as this is a very broad term. This policy will relate to best practice for the use of information, communications and technology at West Granton Housing Co-operative. The vast majority of the policies referenced below are available via the WGHC website.

The following have been considered in relation to this policy:

- Data Protection Act 2018
- UK GDPR (General Data Protection Regulation)
- The Scottish Social Housing Charter 2017

1.1 Responsibility & Authority

WGHC policies must be approved by the Committee of Management. Minor amendments or updates to policy may be made by the CEO within the limits set out in WGHC's Governance Policy. Operational procedures, in line with policy, may be approved by the CEO.

The COO will be primarily responsible for making relevant information about the Co-operative available, via information provided on the WGHC website and/or via the Guide to Information.

The focus will be very much on providing accessible, relevant information to our members and their households. The CEO will primarily be responsible for information security and for registration under the Data Protection Act. The CEO must authorise the release of business information. The CEO or COO must authorise the release of personal data to the data subject or third parties / requester if not personal data.

1.2 Information made widely available

WGHC will strive to achieve implementation of the Office of the Scottish Information Commissioner's (OSIC) model publication framework. The Senior Management Team has responsibility for various tenant and services information and will share this with the COO who will act as the website Co-ordinator and Data Protection liaison with WGHC outsourced DPO for both FOISA requests and Subject Access Requests.

In accordance with recommended practice we will use our website as the main method of publication. However, we recognise not all our members have internet access and will continue to also use letters, leaflets, newsletters etc. to disseminate information.

On our website we will publish and keep up to date information in the following categories:

- About us – structure, governance and membership;
- Decision making – role of committee and recent committee decisions;
- Finance – income and expenditure;
- Services – what we do and how to contact us
- Who we work with – contractors
- Performance – performance information, complaints & appeals;
- Policies – key WGHC policies.

1.3 Annual Information

In accordance with our rules we will provide information to tenants prior to the Annual General Meeting including:

- Annual report;
- Annual financial statements;
- AGM agenda, minutes & reports.

We will also provide an Annual Report on the Charter (ARC) to tenants by the end of October each year. The ARC will contain a summary of how WGHC has performed in relation to key performance indicators issued by the Scottish Housing Regulator.

1.4 Periodic Information

WGHC will periodically produce leaflets and guides about housing related topics. We also receive leaflets from other agencies about housing or local issues. These will be displayed or distributed in the most appropriate ways. We shall issue information periodically about new proposals and issues of concern. The principal methods will be by email, personal letter or personal contact. Regular updates will be displayed on the WGHC website. Our quarterly newsletters are another popular way of receiving general information.

1.5 Translation

WGHC will promote the use of interpreters and/or provide assistance for those that may need it, as appropriate.

2.0 INFORMATION SECURITY - GENERAL

Information should only be accessible to those to whom it is of use in the course of their work. However, given the small number of staff and extent of generic working it is recognised that barriers to information, especially relating to tenants, is often impractical.

Both staff and committee members must not disclose any personal information about data subjects to which they have access to any other person except as permitted by this policy. This respect for confidentiality is also highlighted in other WGHC policies and in the Staff and Committee Codes of Conduct. The Committee of Management's role is strategic rather than operational. Committee will not have access to personal information about other tenants, staff and other data subjects.

Disclosure of information about individuals to Committee members will only be made when it is necessary (e.g. disciplinary hearings, membership applications). Such disclosure should be limited to the information necessary for the task in hand. In the case of appeals or complaints or disciplinary cases being heard by the Committee or a Subcommittee: where practical names and addresses and other information which would identify an individual will not be disclosed in reports. In some cases, given WGHC's relatively small stock and small number of staff, it is accepted that it may be effectively impossible not to identify an individual, especially where the individual puts their case in person. However, Committee members are at all times bound to act impartially and to disclose any personal interest.

3.0 Information Security – Computer Systems

WGHC's computers are on a network controlled by a server computer in the comms room. The server has a mapped drive "WGHC files" on which most WGHC day to day files are stored. Files are arranged in folders according to activity. There is a mixture of pro forma letter, tenant file notes, spreadsheets etc. These files are for common use. Staff should try to ensure any new file is saved in the right place and avoid filling folders with files which only they as individuals may ever use or refer to.

Files stored on the server are backed up regularly. Use "my documents" for files solely for your own use. This is to avoid clutter in WGHC files and to prevent files being accidentally altered or deleted by other staff. Each member of staff's "my documents" is mapped to a u-drive on the server. Files saved in my documents should therefore be backed up along with other files.

Organisational logos, working procedures, document layouts, legislative requirements change reasonably frequently. As such, staff should not save files to their computer desktop or to anywhere other than "my documents" on their computer as:

- These files will not be backed up
- WGHC could encounter 'version control' issues

3.1 Use of Computer systems

Staff must not use either WGHC computers, network or mobile 'phones to access pornography or to send harassing, abusive or offensive messages. Staff must not WGHC computers, network or mobile 'phones for personal commercial purposes. Staff's work email addresses must not be used to subscribe to or access any internet sites or services that are not 'housing services' related, i.e. SHR / EVH / SHN etc.

3.2 Access Control

The objective of Access Control is to assist employees in understanding the systems in place to protect the interests of all authorised users of WGHC's IT systems, as well as data provided by third parties, by creating a safe, secure, and accessible environment in which to work.

3.3 Creation of User Accounts

Once a new employee has confirmed acceptance of an offer of employment, Management will raise a request to the IT Provider to set up an email address and user account. Each user will be set up with a unique user ID and password to access to their user account. Once this is provided to the employee the employee will be asked to change their password immediately.

All new users will be given standard level access to the server. (Standard service includes MS Outlook including Office 365 email, MS Office, and Internet Access). Where the employee has no access to an existing workstation, a new computer shall be ordered and set up to the system by the IT Provider.

3.4 Removal of User Accounts

As soon as an employee leaves WGHC's employment or a Committee member leaves, access to their account shall be stopped with immediate effect. As part of the employment termination process, a request may be made by Management to revoke access levels by requesting a change to the leavers password which will prevent the leaver accessing the system. Information and emails may be retained for a period of 6 months after which the email account shall be deleted.

A request shall be made to remove the leaver from the 2-factor authentication process.
All leavers will return all property belonging to WGHC, including laptops and/or mobile 'phones.

3.5 Access for remote users

Access for remote users shall be subject to authorisation by WGHC and be provided in accordance with the Remote Access Policy and the Information Security Policy. No access to the network is permitted for personal devices.

3.6 Physical access control

Access to the Comms Rooms is restricted and can only be accessed by authorised staff who have been permitted keys. If keys are lost, this should be reported to Management as soon as possible.

3.7 Passwords

WGHC staff should select strong passwords and as a result enhance the security of the network.

3.7.1 Password Requirements

According to the National Institute of Standards and Technology, the following is recommended:

- Passwords should have a length of 8-16 characters;
- They should include non-standard characters, i.e. * / £ / $ / # etc.;
- Long passphrases are encouraged;
- Password reset is only required if the password is compromised or forgotten; and
- Multi-factor authentication is encouraged.

3.7.2 Password Privacy

Passwords are to be treated as sensitive, confidential information and should be kept private. Passwords should not be shared with anyone or talked about in front of others. Users are responsible for maintaining and ensuring the protection of their passwords.

3.8 Change Management

Changes to the IT infrastructure must only be undertaken by authorised personnel, e.g. the IT Provider. Changes to the Association's IT infrastructure and operational systems should be requested to the IT Provider, as follows:

- Raising a ticket with the IT Provider with a description of and reason for the change (e.g. increased administrative privileges).
- Formal approval process – managerial approval and authorisation prior to proceeding with changes which may have a significant impact.
- Implementation of requested change, if approved by the Provider.

Once the change has been carried out, this should be communicated to all relevant people of the changes, including:

- Advance communication/warning of changes
- Proposed schedules
- Description of reasonably anticipated outcomes provided to all relevant personnel.

All changes made, and all the steps taken in the change management process should be logged. The IT Provider should have procedures in place for aborting and rolling back if problems occur. All changes to the IT infrastructure should be assessed by the Provider for impact on the security of data and information.

3.9 Network and Systems / Data 'back up'

Computer files are backed up on a daily basis by WGHC's outsourced IT Provider and copies are stored away from the WGHC office. Back-ups are undertaken by the out-sourced IT provider to WGHC. Further, some systems are backed up automatically on a 'live' basis, MS Outlook via Office 365 etc. WGHC will use anti-virus software and other measures to try to ensure that files are not infected by viruses or similar problems and that we do not spread such problems.

4.0 WORKING FROM HOME / REMOTELY

Due to the recent Coronavirus pandemic, many people are working remotely at home instead of in their usual place of work. Data Protection law still needs to be complied with even in these unusual circumstances, including security of data and systems.
The following section covers home working generally and should be followed in all situations where staff are working from home or away from the office.

4.1 Homeworking definitions

Home Worker refers to Staff using either company provided or their own device or systems or applications, to access and store company information, at their home or remotely, typically connecting to WGHC's network via a VPN. (Provided by WGHC out-sourced IT provider).

This policy covers the use of electronic devices which could be used to access WHGC's systems and store information, alongside employees' own personal data. Such devices include, but are not limited to, smart phones, tablets, laptops and similar technologies.

4.2 Data 'ownership'

WGHC acting as the Data Controller, remains in control of the data regardless of the ownership of the device, or the location in which the data is processed. Staff are required to keep any company information and data securely and comply with Data Protection law. (Data Protection Act 2018 and/or UK GDPR) Staff are required to assist and support WGHC in carrying out its legal and operational obligations, including co-operating with the out-sourced IT provider should it be necessary to access or inspect company data stored on personal devices or equipment at their home.

4.3 Data Protection & Confidentiality

Staff must follow WGHC's policies and procedures in relation to working with personal data as if they are still based in the office. However, there are additional risks relating to working remotely. Staff should keep the following in mind:

The data protection principles still apply and need to be adhered to, i.e., Staff should only access personal data that is needed for "specified, explicit and legitimate purposes". Staff should "limit what they take home to only what is necessary" and keep it there for "no longer than is necessary". Staff must consider "appropriate security", both at home and in transit. Additionally, if required to, Staff must be able to provide WGHC with evidence they are complying with the following principles.

- Never leave a computer with personal confidential information on screen. An unauthorised person reading personal data is a data breach.
- Never leave your computer 'logged on' when unattended. Think about who may access the device when you are not around – whether deliberate or accidental.
- Ensure that rooms containing computers and other equipment, are secure when unattended, with windows closed and locked and blinds or curtains closed.
- If making a phone or online conference call remember that it is confidential and consider who is around who might overhear.
- Levels of Home Security should be at a similar level as at work.
- You should only work within WGHC's approved systems – e.g. Microsoft teams, outlook, SDM etc.
- Do not hold person identifiable information on electronic devices. If you absolutely have to download a document to your personal device, ensure it is deleted as soon as possible.
- If using your own device, check for automatic uploads to Cloud storage systems. For example, if you have subscribed to iCloud or Dropbox, you may inadvertently be uploading [name of organisation]'s documents to your personal account in these applications. You should disable these uploads whilst you are doing [name of organisation] work.
- Any paper taken from the office to work at home must be protected in transit and in your home.
- Paper files should be 'signed out' from the office and 'signed in' again when returned.
- Ensure paper is transported safely – and not left in an unattended vehicle.
- Keep paperwork secure at home and out of sight of members of your family and others
- It is imperative that paper no longer needed is shredded or returned to the office for safe disposal, on no account should files be disposed of within general waste.

5.0 EMAIL & INTERNET

Each member of staff has an email address. This is for work. It must not to be used to subscribe to or access any internet sites or services which are not directly related to WGHC work. Sending or receiving emails should also be restricted to work. The only exception which will be viewed as reasonable is sending or receiving urgent messages to or from home when telephone or text is not appropriate. This should be exceptional.

It is up to staff individually to decide how widely to publicise their individual email address. It is not expected that it will be discloses as a matter of course to any tenant, applicant, contractor etc. Equally other staff's email addresses should not be disclosed without their consent.

In leaflets, newsletters etc. WGHC's general email address mail@westgrantonhc.co.uk should generally be used. Emails to this address are delivered to a public folder named WGHC emails which can be accessed via a centralised folder in MS Outlook. Some general emails (e.g. Scottish Housing News) may be of interest and are generally left for a day or two before being deleted.)

Alternatively there are distribution groups for finance, maintenance and housing management. Emails to these addresses are distributed to all members of the group. The email addresses can be used by external agencies or individuals to access particular services.

Internally, emails to the all staff group will be distributed to all staff members. Other 'WGHC email accounts in use are:

- allstaff@westgrantonhc.co.uk
- finance@westgrantonhc.co.uk
- hm@westgrantonhc.co.uk
- mail@westgrantonhc.co.uk
- maintenance@westgrantonhc.co.uk

5.1 BYOD (Bring Your Own Device)

It is accepted that Staff may bring their own devices (mobile telephones / tablets) to work. It is permitted for Staff to access the WGHC Wi-Fi system using the password provided by their line manager. Whilst using WGHC Wi-Fi, Staff are expected to comply with all WGHC information policies as indicated within section **1.0** and sections **2.0**, **3.0**, **3.1**, **4.3** and **5.0**.
Under NO circumstances are guests, visitors, contractors, suppliers or tenants to be given access to the WGHC Wi-Fi systems, unless authorised by a member of the Senior Management Team.

5.2 Telephones

Staff may use telephones (for local calls for personal use only during lunch breaks or before or after their working day as entered on their timesheet. Outside these times they should only use telephones for personal business in the event of a very urgent matter which cannot reasonably wait. Staff must not use telephones to access chat lines, gambling lines or any line that promotes abusive or offensive messages. Staff must not use telephones for personal commercial purposes. Staff must not telephone long distance or premium rate numbers without the consent of a senior staff member.

5.3 Social Media

Staff should not post any information or comments regarding WGHC, colleagues or service users on social media. This applies at all times and in all media whether at work or in the employees own time.

WGHC reserves the right to monitor telephone, internet and email use to ensure that the facilities are not being abused. WGHC also reserves the right to withdraw access to telephones, email and internet. Abuse of the facilities could also result in disciplinary action, especially, if the reputation of the organisation is tarnished or questioned.

6.0 WGHC Policies

Reference can be made to many other WGHC policies that include details which could be construed as 'information'. These should be consulted where necessary and in addition to the detail within this policy. Most are available via the WGHC website.

WGHC have other policies that also cover the area of 'information' thus:

- Freedom of Information Policy (Non personal data information)
- Guide to Information (Generic information requests linked to FOI / FOISA)
- Data Subject Access Request Policy (Personal data information)
- Environmental Information Requests (Non personal data information)
- Allocation Policy
- Governance Policy
- Payment Card Security Procedures