ICT – Acceptable Use Policy

Date reviewed: October 2025
Next Review: October 2028

Rosehill Housing Association Limited
250 Peat Road, Glasgow, G53 6SA
Tel: 0141 881 0595, Email: admin@rosehillhousing.co.uk
www.rosehillhousing.co.uk

1. Introduction and Purpose

1.1 Internet, Electronic communications (both internal and external) and other ICT systems are vital for Rosehill's business processes. However, these can also expose us to serious risk, not least of which relates to misuse by users.

1.2 This Policy provides a framework for the use of our range of communication tools including: email, internal, social media platforms, and telephone calls. It also covers the use of any hardware (e.g. mobile devices) and software which we own and provide.

1.3 The purpose of this policy is to:

- ensure employees understand the way in which these systems should be used;
- alert employees and managers to the dangers that can arise if the technology is misused;
- advise employees that internet and email use is monitored via monitoring software and to warn employees of the consequences of misuse;
- explains what is classified as acceptable and unacceptable use of our communication tools;
- set out the rules, which must be adhered to, for appropriate use of our communication tools.

1.4 This policy should be interpreted in its widest application and includes new and emerging technologies and uses, which may not be explicitly referred to.

2. Policy Application

2.1 In addition to employees, this Policy also applies to our Committee Members and to anyone else using our communication tools such as agency staff, consultants, and contractors and so on.

2.2 Any person who uses our communication tools is bound by all of the provisions in this policy and agrees to comply with all of its terms and conditions, and with all applicable laws and regulations. All users will be required to sign the associated compliance statement, attached at Appendix 1.

3. Other Relevant Policies

3.1 This policy should be read in conjunction with Rosehill's *Privacy Policy* and *ICT and Data Security Policy*, particularly sections relating to password management, incident response, email security, and data handling.

4. Legal Framework

4.1 The following legislation is relevant to the operation of this Policy:

- Data Protection Act 2018
- Equality Act 2010
- Communications Act 2003
- Copyright, Designs and Patent Act 1988
- Compute Misuse Act 1990
- Computer Copyright Software Amendment Act 1985
- Criminal Justice and Public Order Act 1994
- Human Rights Act 1998
- Regulation of Investigatory Powers Act 2000

4.2 This list is not exhaustive and is subject to change.

Data Protection

4.3 Employees, as well as employers, have responsibilities for data protection. Line-Managers have responsibility for the type of personal information they collect and how they use it. No-one at any level should disclose personal information outside Rosehill's policies and procedures, or use information held on others for their own purposes or for any purpose other than the purpose for which the information was collected. Anyone disclosing personal information, without Rosehill's authority, may be committing a criminal offence. (See also ICT & Data Security Policy S10 & 5.11.3).

4.4 The General Data Protection Regulation covers monitoring at work. Rosehill adheres to the Information Commissioner's Code of Practice. The Code aims to strike a balance between the legitimate expectations of employees that personal information about them will be handled properly and the legitimate interests of employers in deciding how best, within the law, to run their own businesses. (See also ICT & Data Security Policy S10 & 5.11.3).

4.5 The Regulations do not prevent an employer from monitoring employees, but such monitoring must be done in a way which is consistent with the Regulations and staff should be aware of monitoring systems in place. Workers also have a right to respect for private and family life and correspondence under Article 8 of the European Convention on Human Rights. (See also ICT & Data Security Policy S10 & 5.11.3).

NB: However, all users should understand that Rosehill routinely monitors, in general, patterns of email and internet usage, uses monitoring software to record detailed use of these systems by each user. Users should note that this software records each and every site visited by all named users including the date and time. Employees should be aware that there can be no legitimate expectation of privacy when using Rosehill's email and internet facilities. Rosehill reserves the right to examine any material stored on its computer systems in circumstances

where a breach of this policy is suspected. However, we will not routinely read email, which is obviously private, unless the nature of what is being investigated requires us to. Users should also be aware that emails and their content, and internet use and logs will all be routinely stored on our Azure. Backups are held within Azure by our third-party contractors. Access to monitoring logs is restricted to the Director, Finance and IT Manager, and the IT provider. These are monitored both as a matter of routine and in specific cases where a problem relating to excessive or unauthorised use is suspected.

Legal Liability

4.6 Employees, and other users, should be aware that legal responsibility for employee emails and for internet misuse by an employee can rest with **both** Rosehill and the employee responsible. For instance, where an email contains a defamatory comment or a comment which could be considered to amount to sexual harassment then this could attract liability to both the author of the email and to Rosehill. Accordingly, employees should be aware at all times that responsibility for email and internet misuse lies wider than the individual who misuses it.

4.7 Similarly, employees and particularly the Director and Managers, should be aware Rosehill can be held vicariously liable for representations made or contractual arrangements entered into by its employees where it is reasonable for a third party to assume that the employee is acting with Rosehill's authority. Therefore, it is essential that great care is taken in relation to both external and internal emails which could be contractually binding.

5. When this Policy Applies

5.1 This policy applies in the following circumstances:

- During working hours
- At Rosehill's premises outside normal working hours
- When accessing Rosehill's systems from any location
- Whilst travelling on Rosehill's business
- When making any communication which identifies the individual with Rosehill
- Whilst using Rosehill's equipment at any location

5.2 Aspects of the policy also apply no matter where or when email or internet services, such as social media platforms, are used by Rosehill employees including outside working hours for private and personal purposes.

5.3 Any third parties such as visitors, agents or consultants using Rosehill's communication tools are subject to compliance with this policy. All applications for the use of such systems by third parties must be authorised by the Director or Finance and IT Manager.

5.4 All third parties will be required to read and understand the terms of this policy and agree to be bound by it and sign the associated form (see Appendix 2). The Customer Services Officer is responsible for issuing the form, ensuring its completion and for retaining the form.

6. When are you allowed to use Rosehill's Communication Tools for personal matters?

6.1 To ensure that there can be no misunderstanding concerning this, it has been decided that our communication tools can be used for reasonable personal use in the following circumstances:

Employees

6.2 Internet – personal use is allowed during lunch breaks only. For the avoidance of doubt, the internet cannot be accessed before you start or after you finish work; please see Section 7 for the rules for using the internet.

6.3 Email – for the avoidance of doubt the use of Rosehill's email addresses is strictly prohibited for personal use at all times; please see Section 8 for the rules for using email. (See also ICT & Data Security Policy S5.10).

6.4 Phones (work mobile and landline) – reasonable use of work mobile and or landline phones is allowed during lunchbreaks. In addition, personal calls of an urgent nature will be allowed during working hours, but it is expected that this will not be a regular occurrence. See Section 9 on the rules for using phones.

6.5 Laptops/tablets – are provided for the sole use of business purposes. See Section 10 on the rules for using laptops and tablets.

Committee Members

6.5 Tablets - All Committee Members have been issued with tablets to access the Board Portal for meeting papers and other business-related information and, Office 365 suite. The Board Portal is a web-based product tool. Personal use of the tablets (e.g. internet access) is allowed but is restricted to the Committee Member's use only i.e. no other family or household member is allowed to use it.

6.6 Email - for the avoidance of doubt the use of Rosehill's email addresses is strictly prohibited for personal use at all times; please see Section 8 for the rules for using email.

7. Rules for using Internet

7.1 Employees and other users are not permitted to surf the Internet except during their lunch break.

7.2 We consider acceptable personal use of the Internet to include activities such as personal online shopping, booking holidays and banking, accessing newspapers and so on. It does **not** include visiting online gambling sites or participating in online gaming. Employees should note that any purchases or other transactions made online whilst at work are made entirely at their own risk.

7.3 Employees and other users are also only permitted to log on to social networking and video sharing websites such as Facebook, Twitter and YouTube or use Rosehill's Communication Tools to keep a personal weblog ("blog") during their lunch break. We nevertheless reserve the right to restrict access to websites of this type at any time.

7.4 Logging on to sexually explicit websites or the downloading and/or circulation and/or storage (whether on hard drives, memory sticks, DVD and so on) of pornography or other grossly offensive, illegal or obscene material or using the Internet for gambling or illegal activities constitutes gross misconduct and could render the employee liable to summary dismissal under Rosehill's disciplinary procedure. "Rogue" websites exist that appear harmless but instead direct the user automatically to another website that may contain inappropriate material. If this occurs, you must exit the site and you must inform the Director and Finance and IT Manager immediately.

Downloading information from the Internet and file sharing

7.5 Due to ever faster computer networks, employees may be tempted to make illegal downloads of material that is subject to copyright. This includes, but is not limited to, music, film and business software. As this and any subsequent file sharing of this material constitutes an infringement of copyright, it is prohibited on Rosehill computers, laptops, mobile phones or tablets and similar devices. It is also prohibited on any devices brought to work or used by you at home whilst connected to our systems. This also applies to any download or dissemination of material made outside of normal working hours on our systems and equipment. Any breach is likely to lead to disciplinary action being taken. To ensure such downloading cannot take place, the external data extraction has been disabled on all laptops. (See also ICT & Data Security Policy S5.4 - 5.5).

7.6 Employees may need to download documents and information from the Internet in order to undertake their duties. You should only download documents and information that you are sure about, and which are required to fulfil the job duties you are undertaking. With the rapid spread of computer viruses via the Internet, care should be taken when accessing websites that you are not familiar with or when downloading documents or information. (See also ICT & Data Security Policy S5.4 - 5.5).

7.7 Our systems prevent you from downloading any programs from the Internet without the prior approval from the Finance and IT Manager or the Director. Some websites require additional add-on software to display the page

completely. These add-ons will not be downloaded by our systems. If you inadvertently download something and our system does not prevent it, you must not run anything and must immediately report this to the Finance and IT Manager or Director. (See also ICT & Data Security Policy S5.4 - 5.5).

8. Rules for using work email

8.1 As set out in paragraph 6.3 personal use of Rosehill's email addresses is strictly prohibited. This does not include, however, instances when you are communicating with other organisations you are formally involved in through your work with Rosehill; this is likely to involve only the most senior staff in the organisation. In those cases, the email should contain the line, inserted above your signature "This email is not connected to the business of Rosehill Housing Association Limited." (See also ICT & Data Security Policy S5.10).

8.2 To prevent the clogging up of inboxes, when employees need to communicate with other colleagues, where appropriate, this should be done using the posts or chat facility on Teams. Whilst "chatting" is allowed through the Teams' tools, employees must not spend excessive time chatting to colleagues in this way.

8.3 Employees are also prohibited from using e-mail or Teams posts, chats to circulate any material not related to their job. Not only does excessive time spent online lead to loss of productivity and constitute an unauthorised use of Rosehill's time, but sexist, racist or other offensive remarks, pictures or jokes sent by e-mail, Teams posts, chats, are capable of amounting to unlawful harassment and users are strictly forbidden from sending these. As "cyber bullying" is a clear risk, employees are also prohibited from using Rosehill's communication tools as a means of intimidating or bullying employees or third parties.

8.4 Employees must not use their work e-mail address to make orders for personal goods and services.

<u>Etiquette and Best Practice Guidelines for the Use of Email</u>

8.5 Email communications are often perceived as being closer to informal speech rather than formal writing. Emails can be sent quickly and often with little thought regarding their contents. What the sender may construe as acceptable could be construed as rude and abrupt by the recipient.

8.6 Therefore, the following best practice guidelines should apply when sending emails:

- Never say anything in an email that you would not say face to face. Correspondence by email should not be used as an alternative to replace communicating with another employee in person.

- The inappropriate use of upper case in email is generally interpreted as SHOUTING and should be avoided.

- Messages should be concise and to the point. Employees should not send heated messages impulsively or in anger.

- Proofread emails before sending to avoid misunderstandings.

- Check distribution lists before sending an email and target members of staff according to how important the message is to them.

- Email is not secure, therefore sensitive personal data must not be sent to anyone outside Rosehill by email with the exception of extremely limited circumstances. Please see Section 14 for more information.

Reading and storing e-mails

8.7 Employees must check their mailbox regularly during normal working hours. It is the employee's responsibility to read and action any e-mail they receive.

8.8 The e-mail system is not to be used as a storage area. Unwanted messages should be deleted completely. Important information or files should be saved into the appropriate SharePoint folder or into e-mail folders.

8.9 If employees are going to be out of the office for a day or longer and as such will be unable to check their e-mails, they should switch on their "out of office assistant" with an appropriate message. E-mails received in an employee's absence will not normally be read by other members of staff unless they have specifically requested a colleague to undertake this task. However, e-mails may need to be checked by managers for business-related reasons when the employee is absent for any reason and for any length of time. It may, therefore, be unavoidable that some personal e-mails might be read in these circumstances.

E-mail viruses and spam

8.10 All incoming and outgoing external emails are checked for computer viruses and, if a virus is found, the message will be blocked. E-mails may also be checked for other criteria, for example, having an attached image file or containing offensive or inappropriate material or including a "banned" word or from a "banned" user under the criteria in Rosehill's spam software which indicates the message is spam. Again, the e-mail will be blocked. We reserve the right to block and then read these messages to ascertain whether they are business-related.

8.11 If an employee receives an e-mail or data file that is in a format or comes from a source that is not recognised, the item is not to be opened. If there is any doubt as to the legitimacy of the email, do not click on or open any links or attachments in the email. The email should be forwarded to our IT Provider to check and when advised to do so it must be deleted from the inbox, sent and deleted folders. Employees must post a message on Teams to advise

colleagues that a suspicious email has been received and provide the subject heading and who it is from. Even if more than one employee receives the same email, each employee must forward it to our IT Provider and then follow the instructions of our IT Provider.

8.12 If an employee receives any unsolicited e-mails or spam that manages to bypass the Company's spam software, they must not respond in any way. Please forward the e-mail to our IT Provider and ask for it to be added to the banned sender's list. Some spam e-mails may offer the option to opt out of receiving them. Be aware that this is sometimes used as a way by unscrupulous spammers of validating a live e-mail address.

8.13 You must not:

- Send or receive copyright material unless you have the appropriate permissions and have paid for the material where appropriate. You must keep such permissions/proof of payment and produce them on demand by Rosehill;
- Send junk emails or unsolicited marketing material (SPAM). This includes, but is not limited to, chain letters and offers, hoax virus alerts, unsolicited mail, or communications lists;
- Send jokes which include joke animations, graphics, and sound files of any type;
- Send anything which could cause offence to, not just the recipient, but to anyone who might see what you send which includes your colleagues. This includes, but is not limited to, any material which is sexually explicit or shows people nude or semi-nude, or which is offensive or depicts explicit violence;
- Store personal emails, from others, which breach anything in this policy. Such emails must be permanently deleted immediately and the sender notified not to send such material to your work email address;
- Access any web-based email accounts where such access breaches anything contained in this policy.

NB: *The word "send" also means "forward" and "reply to," because most computers will include a copy of the original message in these circumstances.*

An employee who receives unsolicited, offensive, or sexually explicit emails should inform the Director. It will be for the Director to decide whether any further investigation or disciplinary action is appropriate.

8.14 A Rosehill auto-signature within the email client software (currently Microsoft Outlook) is set as a default but can be amended by employees as appropriate. A default company email disclaimer is also automatically added to all outgoing emails. This is a legal requirement, which acts exactly the same as a company letterhead and no attempt should be made to alter it.

9. Rules for using Office and Mobile Phones

9.1 As mentioned at 6.4 reasonable personal use of office and mobile phones are allowed; normally within lunch breaks but may be used during working hours in urgent circumstances.

9.2 When using the office or mobile phones, employees must only make personal calls to premium rate numbers if the Finance Officer has been advised in advance, and they have agreed to pay all costs incurred via salary deduction.

9.3 Work mobile phones have been allocated to all employees. All such phones are on contracts and have monthly data allowances. Employees must not use work mobile phones to:

- Access personal email accounts;
- Text personal messages;
- Access apps such as WhatsApp for non-work-related matters;

9.4 The exception to this is where an employee is required to use their phone for work purposes out with normal business hours on a regular basis. Any such employees are allowed dual use of the phone, i.e. business and personal use. However, the rules relating to personal phone calls and use of the internet during working hours and using the work email address still apply.

9.5 The vast majority of work mobile phones are only used during business hours. In such cases, employees must ensure the mobile phone is switched on when they first start working. If they are working from the office, the mobile phone must be taken with them if they do non-office-based work e.g. neighborhood walk-abouts, external inspections and home visits. Once an employee has finished working for the day the mobile phone must be switched off and locked away in a safe place e.g. desk drawer or cupboard.

9.6 If an employee is working from home, they must ensure they have their work mobile with them. It must be switched on at the start of the working day and switched off when the employee is finished.

10. Rules for using Laptops and Tablets

10.1 The personal use of laptops and tablets is not allowed.

10.2 No data relating to the business of Rosehill must be stored on the hard drive of the laptop/tablet. This includes any personal devices being used for work purposes. Company data isn't stored on the hard drive. It is all stored within SharePoint. Personal files are stored within OneDrive.

10.3 No application or programs may be installed on these devices without the prior authorisation of the Director or Finance and IT Manager.

10.4 These devices can be used whilst working at the office (both in the office and

whilst out working in the local area e.g. neighborhood, void and repair inspections).

10.5 If working from home, these devices are only to be used in the home environment and nowhere else. All employees must sign and comply with the Data Protection Statement relating to home working.

10.6 Employees are responsible for the safe keeping of these devices when using them. If an employee has sole use of a device, then they are responsible, at all times, for the safekeeping of the device.

11. Using Social Media Platforms and Video Sharing Websites

11.1 Rosehill respects the right to a private life and that includes joining any social media platforms employees wish. However, be aware that information posted on such sites is classed as public and not private.

11.2 If using social media platforms employees are expected to adhere to the following:

- keep profiles set to private and protect tweets, etc;
- ensure all passwords are kept private, and never use a work password for non-work-related activity;
- employees should be aware of the language and content of their posts and avoid posting anything they would not say publicly.

11.3 Bearing in mind that information posted on social media platforms is classed as public, therefore when logging on to and using social platforms and video sharing websites and blogs, or anything similar, at any time, including personal use outside the workplace, employees must not:

- publicly identify themselves as working for Rosehill, make reference to Rosehill or provide information from which others can ascertain the name of the organisation;
- conduct themselves in a way that is detrimental to Rosehill or brings or could bring Rosehill into disrepute;
- use their work e-mail address when registering on such sites;
- allow their interaction on these websites or blogs to damage working relationships between employees and tenants or clients of Rosehill;
- contradict or disagree with anything Rosehill does, publishes, states or represents;
- include any information about Rosehill's employees, committee members, tenants, contractors, suppliers, customers, partners, stakeholders or clients (an employee may still be liable, even if none of the aforementioned are expressly named in the websites or blogs, as long as Rosehill reasonably believes they are identifiable);
- make any derogatory, offensive, discriminatory or defamatory comments about Rosehill, its employees, committee members, tenants, contractors, suppliers, customers, partners or clients (an employee may still be liable

even if any of the aforementioned are not expressly named in the websites or blogs, as long as Rosehill reasonably believes they are identifiable);
- make any comments about Rosehill's employees that could constitute unlawful discrimination, harassment or bullying;
- disclose any commercial or confidential information belonging to Rosehill, its employees, committee members, tenants, contractors, suppliers, customers, partners, stakeholders or clients or any information which could be used by one or more of Rosehill's competitors.

11.4 In general the above rules, equally apply to Committee Members.

11.5 Employees who are discovered contravening these rules, whether inside or outside the workplace or whilst at work or not, may face serious disciplinary action under Rosehill's disciplinary procedure. Depending on the seriousness of the offence, it may amount to gross misconduct and could result in the employee's summary dismissal.

11.6 In the case of Committee Members who are in breach of the rules, we will invoke the terms of the Committee Members' Code of Conduct.

11.7 Please see Section 15, Breaches of this Policy, for further information.

12 E-mail and Internet monitoring (See also ICT & Data Security Policy S5.11.2 & 5.11.3).

12.1 Rosehill reserves the right to monitor employees' internal and external e-mails and use of the Internet, both as a matter of routine and in specific cases where a problem relating to excessive or unauthorised use is suspected. Rosehill uses software which logs all users' internet activity including specific websites visited. This happens automatically and runs in the background. The purposes for such monitoring are:

- to promote productivity and efficiency;
- to ensure the security of the system and its effective operation;
- to ensure there is no unauthorised use of Rosehill's time, e.g. that an employee has not been using email to send or receive an excessive number of personal communications;
- to ensure the smooth running of our business, if the employee is absent for any reason and communications need to be checked;
- to ensure that all employees are treated with respect and dignity at work, by discovering and eliminating any material that is capable of amounting to unlawful harassment;
- to ensure that inappropriate websites are not being accessed by employees;
- to ensure there is no breach of commercial confidentiality.

12.2 When monitoring e-mails, Rosehill will, except in exceptional circumstances, confine itself to looking at the address and header of the e-mails. However, where circumstances warrant it, Rosehill may open e-mails and access the content. In this case, Rosehill will avoid, if possible, opening e-mails clearly

marked as private or personal unless it is suspected that such marking is being used to cover unauthorised content.

12.3 Rosehill reserves the right to restrict, deny or remove e-mail or Internet access to or from any employee. The decision to do so rests with the Director whose decision is final with no right of appeal.

12.4 Incident Reporting

If any user suspects a breach of this policy, including phishing attempts, harassment, data leaks, or unauthorised access, they must report it immediately to the Finance and IT Manager, Director, or the Data Protection Officer (DPO).

Reports should include:

- A brief description of the incident
- Date and time it occurred
- Any known affected systems or individuals
- Screenshots or evidence, if available

Rosehill will follow its Incident Response Procedure as outlined in the ICT and Data Security Policy (Section 5.11.3), which includes containment, assessment, notification, recovery, and review.

All reports will be treated confidentially and investigated promptly. Staff are encouraged to report concerns without fear of reprisal.

13. Defamation

13.1 Employees must not write, send publish or copy, distribute or forward derogatory or defamatory remarks about any person or organisation either on the internet or by email. If an employee discovers potentially defamatory material, they should report it immediately. Employees must not send or forward discriminatory messages, even if it is intended as a joke, as this could be regarded as harassment.

14. Personal, Sensitive and Confidential Data (See also ICT & Data Security Policy S6 & 10.4).

14.1 Accidental breaches of confidentiality can occur by entering a wrong address or forwarding a message to inappropriate recipients on Rosehill's distribution list. It can also happen if confidential or sensitive information is sent by email without being secure. In the following pages, we set out how to share information both internally with colleagues and external parties. The following processes must be strictly adhered to.

Sharing data internally

14.2 We operate Microsoft 365 and use SharePoint for sharing files within the organisation. Therefore, any information to be shared with colleagues must be done using SharePoint. Employees must decide the level of information to be shared with colleagues. For example, it is possible to share only one file or an entire folder. It is also possible to manage the access level to a file e.g. an employee may want to share a file but does not want colleagues to be able to edit the file. In this case, it is possible to restrict access to view only.

14.3 Once an employee has selected the file/folder to share, from the more actions option (signified by three dots …) select share and then begin to type in the name of the recipient(s). A drop downlist should appear, the employee must exercise care and ensure they are selecting the correct names from the drop-down list.

14.4 It is possible to also share files by using the "posts" facility on Teams. To be able to do this, an employee must be part of an existing Teams Channel e.g. if an employee is part of the Housing Services Team and wants to share a file with all the other members of the HS Team, they can add a link to the file within the post being sent.

14.5 Employees may be part of a wider Teams Channel which includes colleagues from other departments. Files and information **should only** be shared via these wider channels if it is appropriate to send to everyone who is in that Channel.

14.6 Employees are advised that only the Director has the authority to create Teams Channels.

14.7 All Committee Members have been set up with Rosehill email addresses for business purposes only. In general, it will only be the Director and Customers Services Officer who will use these email addresses. To ensure emails are sent to the correct recipients, mailing lists should be set up for the Management Committee, the Sub-Committees and for the Chair and Vice Chair.

14.8 If emails are being sent to individual committee members, care must be taken to select the correct name from the drop-down list when typing in names. Before sending any such emails, it is important to double check the correct recipient is shown.

14.9 If any personal or sensitive data or any confidential information is to be shared, this is not to be contained within the body of the email but must be sent as an attachment. The attachment must be password protected, and the password passed to Committee Members by phone.

<u>Sharing data externally</u>

14.10 Any data that is deemed to be personal, sensitive, or generally confidential needs to be sent in a secure manner to external bodies. The following methods should be used.

- Secure Platforms/Portal

Secure platforms generally mean a managed platform that encrypts files in storage and transit. Employees should consider the following before using platforms:

1. The sender, are we expecting files from the sender?
2. The content of the files. Are they sensitive?
3. Cyber security credentials of the platform.

This should guide how well protected file sharing is required to be.

14.11 If the external body provides a secure platform or portal for sending and receiving data, then this must be used. Employees will be set up and receive log-in details for accessing such platforms/portals. Employees must ensure that log-in details are kept safe and not shared with other colleagues.

SharePoint

14.12 In the absence of a secure platform or portal, employees should share data by using SharePoint. When sending data this way, the employee should ensure the correct access level is set e.g. file is for viewing only, can view but cannot download or can edit file, etc.

14.13 Employees must obtain the authorisation of their Line Managers before using SharePoint to share data with external bodies. In the absence of Line Managers, authorisation must be sought from the Finance and IT Manager or the Director.

By Email

14.14 Sending data by email is the last resort. It should only be used if there is not a secure portal and the recipient does not have access to Microsoft 365. It is important that you check this with the external party. Before sending an email, you must first of all obtain the authorisation of your Line Manager. In the absence of Line Managers, authorisation must be sought from the Finance and IT Manager or the Director.

14.15 Any personal or sensitive data or any confidential information being sent by email must not be contained within the body of the email and must be sent as a secure attachment. The attachment must be password protected. The password must be shared with the recipient by telephone. **Under no circumstances is the password to be sent in the same email as the attachments or in a separate email.**

14.16 When creating a new email message, you can select the recipient's name by beginning to type in their name and then selecting from the drop-down list that appears. If using this option, you must be vigilant that you have selected the correct name from the drop down list, you should do this when selecting the

name at the time and then just before sending the email you must double check that the correct email address is shown.

14.17 The preferable way to select the recipient(s) is to go to an email from them in your inbox, open it and put your curser over their name; a pop-up box will appear with an envelope symbol in it. If you click on it, this will populate their email address in a new message. Whilst this is the preferable option it might not be the most feasible particularly as inboxes and other outlook folders must be cleared out on a regular basis.

14.18 You must, when sending personal or sensitive data or any confidential material by email, ensure that you mark the message as private and confidential. The attachment must also be marked confidential both in the file name and at the top of the document. (You must not forward private and confidential emails you receive to another person without obtaining the original sender's consent) If an employee discovers that there is a breach of confidentiality, they should report this to the Finance and IT Manager, or the Director immediately.

USB Ports and Unmanaged Data Sharing Websites

14.19 **For the avoidance of doubt data must not be shared (sending or receiving) through use of USB sticks or unmanaged data sharing websites such as Dropbox. To prevent this from happening, data extraction in all laptops have been disabled for such use and websites such as Dropbox have been blocked.**

15. Breaches of this Policy

15.1 Breaches will normally be dealt with by application of our disciplinary procedures, in the case of employees. In the case of Committee Members, we will invoke the terms of our code of conduct which could ultimately result in removal from the Management Committee and for anyone else we will conduct an investigation which could result in termination of contract, agency agreement or equivalent. In some cases, a breach of this policy may result in civil action being taken against the individual concerned or in criminal prosecution.

15.2 Any user of our communication tools whose actions violate this policy, or any other of our policies or regulations, may be subject to limitations imposed by us or withdrawal of any communication tool privileges. This may be in addition to disciplinary action in accordance with our disciplinary procedures and/or other procedures and policies e.g. Committee Members' Code of Conduct. Anyone who breaches this policy, who is not an employee or Committee Member of ours, will be dealt with in terms appropriate for the particular circumstances e.g. through a formal complaint to their employer.

16. Data Protection

16.1 On the 25th of May 2018 the legislation governing data protection changed with the introduction of the General Data Protection Regulation (GDPR). Following the UK's exit from the EU, and the end of the transition period which followed, the GDPR formed part of the retained EU law and became the UK GDPR which together with the Data Protection Act 2018 constitute the UK's data protection legislation.

16.2 In accordance with the UK GDPR, Rosehill Housing Association has appointed a Data Protection Officer (DPO) to oversee compliance with data protection legislation, advise on data protection obligations, and act as a point of contact for the Information Commissioner's Office (ICO). The DPO is responsible for monitoring internal compliance, providing expertise, and advising on Data Protection Impact Assessments (DPIAs).

Staff may contact the DPO Information Law Solutions Limited for guidance or to report concerns regarding data protection.

16.3 Rosehill will ensure that all third-party service providers who process personal data on its behalf (e.g., IT support, cloud services) are contractually bound to comply with UK GDPR and our internal data protection standards.

16.4 Data retention and minimisation

Rosehill will only collect and retain personal data that is necessary for its operational and legal purposes.

- Data will be retained in accordance with our Data Retention Schedule.
- Personal data will be securely deleted or anonymised when no longer required.
- Staff must avoid collecting excessive or irrelevant data and ensure that data is regularly reviewed for accuracy and relevance.
- The Corporate Services and Human Resource Manager will oversee compliance with these principles and conduct periodic audits in conjunction with our DPO.

17. Equality and Diversity

17.1 Rosehill's Equality and Human Rights policy (January 2024) outlines our commitment to zero tolerance of unfair treatment or discrimination towards any individuals or group of individuals, particularly those belonging to a protected characteristics (as defined by the Equality Act (2010). This includes ensuring everyone has equal access to information and services, by making copies of all policies available in a variety range of alternative formats (i.e. large print, translated, etc.) in response to reasonable requests.

Rosehill is aware of the potential for policies to inadvertently discriminate against individuals or group of individuals. To help address this we carry out Equality Impact Assessments (EIA) to help identify any part of a policy that may be discriminatory so this can be addressed (please see Section 9 of our Equality and Human Rights policy for more information).

As this policy applies equally to all groups, Rosehill (with committee approval) made the decision not to carry-out an Equality Impact Assessment on this policy.

18. Risk Management

18.1 In all key areas of our business we need to consider any risks which may arise. To this end we have in place a robust Risk Management Policy and from this flows our Risk Register. We have identified our Strategic risks which are regularly monitored by our Management Committee, Audit & Risk Sub-Committee, and our Management Team.

18.2 To ensure we continue to manage the associated risks with the potential misuse of our communication tools, we will periodically review this policy to ensure compliance with all legislative requirements and regulatory and best practice guidance.

18.3 As part of its risk management process, Rosehill will conduct risk assessments in its IT systems and data handling processes at least annually. This assessment will include:

- Annual Penetration Testing of network and cloud infrastructure.
- Review of access controls and permissions
- Evaluate third-party risks and software dependencies.
- Assessment of physical and remote working risks

Findings will be documented and used to update the Risk Register and inform future policy reviews.

19. Review

This policy will be reviewed at least every three years, with interim annual reviews where pace of change warrants review to ensure it continues to comply with all required legislation and best practice.

Registered Office: 250 Peat Road, Glasgow, G53 6SA
tel **0141 881 0595** • email **admin@rosehillhousing.co.uk**
www.rosehillhousing.co.uk

Registered Scottish Charity, No. SC053776. Company Registration No. SP02220R.
A registered society under the Co-operative and Community Benefit Societies Act 2014 No. 2220R(S)
and with The Scottish Housing Regulator (Number HAC174).

Appendix 1

ICT: Acceptable Use Policy – Compliance Statement

The following statement is to be used by employees and Committee Members only.

I..... (insert name) hereby acknowledge that I have received a copy of Rosehill's ICT: Acceptable Use Policy. I confirm that I have read and understood the terms, conditions and rules that apply to the Policy. I agree to be bound by all of the provisions in the policy and agree to comply with all of its terms, conditions, and rules, and with all applicable laws and regulations.

Print Name:	
Signature:	
Date:	

Appendix 2

ICT: Acceptable Use Policy – Compliance Statement and Authorisation Form

The following statement and form applies to 3rd Parties only.

Compliance Statement

I..... (insert name) hereby acknowledge that I have received a copy of Rosehill's ICT: Acceptable Use Policy. I confirm that I have read and understood the terms, conditions and rules that apply to the Policy. I agree to be bound by all of the provisions in the policy and agree to comply with all of its terms, conditions, and rules, and with all applicable laws and regulations.

Print Name:	
Signature:	
Date:	

Authorisation Form

Name		
Place of Work		
Contact no		
Email address		
Details of Access:		
Date of Access	From:	To:

Approval for Use

Approved by:	
Signature	
Date	