IT Policy Manual

Prepared By	IT
Policy Created	IT Policy Manual
Effective Date	June 2020
Review Date	June 2021*
Posted on Website	No

*As IT changes are significant within CVHA currently these policies will be reviewed annually until strategy delivered

If you need this publication in larger print, audio form, Braille, or in another language, please contact our office and we will try to help you.

Contents

CLYDE VALLEY GROUP

PROVIDING HOMES | SHAPING COMMUNITIES

IT Security Policy
Policy Number IT1

1. Introduction and Objectives

1.1 Clyde Valley Housing Association (CVHA) regards the integrity of the computer systems as an important contribution to the efficient and effective provision of its services. Measures are in place to ensure that CVHA's systems remain secure against any unauthorised intrusion.

1.2 This policy defines a framework by which Clyde Valley Housing Association's (CVHA) computer systems, assets, infrastructure and computing environment will be protected from threats whether internal, external, deliberate or accidental.

2. General Security, Responsibilities and Training

2.1 All central computer systems, environments and information contained within them will be protected against unauthorised access.

2.2 All use of CVHA's IT facilities will comply with the IT Acceptable Use Policy.

2.3 Information kept within these systems will be managed securely, to comply with relevant data protection laws and to ensure that such assets will be managed in a professional, safe and dependable manner.

2.4 All staff are required to familiarise themselves with this IT Security Policy, to adhere to it and comply with its requirements. Failure to do so may result in disciplinary action.

2.5 All new users will receive the necessary instruction on the ICT Acceptable Usage at Induction. Any breach of this policy may be regarded as a serious matter, which could result in disciplinary action.

2.5 Initial training for new users on the various IT systems will be carried out by the IT Officer. In the absence of the IT Officer this will be carried out by the ICT Manager.

2.5 Managers are responsible for ensuring the competency of any temporary, freelance or consultancy staff, before they are allowed to access CVHA systems.

2.5 Managers have a responsibility for ensuring the implementation of, adherence to and compliance with this policy throughout their areas of functional responsibility.

2.6 The integrity of all central computer systems, the confidentiality of any information contained within or accessible on or via these systems is the responsibility of the ICT Manager.

2.7 All breaches of security will be reported to and initially investigated by the ICT Manager.

2.9 All users have a responsibility to report promptly to the ICT Manager any incidents which may have an IT security implication for the organisation.

3. The Computing Environment

3.1 The computing environment is defined as all central computing resources and network infrastructure managed and overseen by the ICT Manager and all computing devices that can physically or wirelessly connect to it, All are covered by this policy, including computing hardware and software, any CVHA related data residing on these machines or accessible from these machines within the network environment and any media such as CD-ROMs, DVD-ROMs, portable storage devices and backup tapes.

3.3 All temporary and permanent connections via the network, the Wireless network, the Virtual Private Network (VPN) are similarly subject to the conditions of this policy.

3.4 Computing resources not owned by CVHA may be connected to its network. However, all such resources must first be authorised by the ICT Manager.

3.5 CVHA reserves the right to monitor, log, collect and analyze the content of all transmissions on networks maintained by CVHA at any time deemed necessary for performance, fault diagnostic and IT Acceptable Use Policy compliance purposes.

4 Physical Security

4.1 The Server Room houses the physical servers, telephone systems, network and external communication with protected power arrangements in a climate controlled environment.

4.2 The room will remain locked at all times, with access only granted by the Finance and Corporate Services Director, ICT Manager or IT Officer.

4.3 Any unattended portable equipment should be physically secure, for example locked in a cupboard or a desk drawer. When being transported in a vehicle they should be hidden from view. Staff should not store sensitive information on portable equipment whenever possible.

4.5 Staff who store confidential information on CVHA owned portable equipment must ensure that they advise the IT Department of such data to ensure that is thoroughly and securely cleansed from that equipment.

5. Data Security

5.1 CVHA attaches great importance to the secure management of the data it holds and generates.

5.2 CVHA holds a variety of sensitive data including personal information about its customers. Staff have been given access to this information, and are reminded of their responsibilities under data protection and GDPR law and must adhere to the Data Protection and Information Sharing Policy.

5.3 CVHA provides a secure remote access solution for staff to access IT systems remotely via Citrix Netscaler.

5.4 Any copying of sensitive data and information onto any form of portable media transport device or mechanism (Memory Stick, CD, DVD, External Hard Drive, PDA, portable music player, Laptop, etc.) or its transportation beyond the office environment should be authorised by a Line Manager in the first instance.

5.5 Staff must not store any CVHA data within any personal cloud based storage they access. All CVHA data containing any personal data must be used at all times within the Citrix Operating Environment.

5.6 Confidential or sensitive information being transported out with the office must be password protected. Staff must ensure that they are aware how to password protect information. If they are unsure training can be provided by either the ICT Manager or the IT Officer.

6. Firewall and External Connections

6.1 CVHA has a firewall, which sits between its internal network and the Internet, providing security at the perimeter. This is a managed service and automatic updates are performed on a nightly basis to ensure the systems are up-to-date.

6.2 External connections may be required which bypass the firewall for BACS or Telebanking. The ICT Manager will consider the security implications as these connections could provide a point of unauthorised access. The ICT Manager will determine the appropriate configuration in relation to the network.

7. Cyber Crime and Penetration Testing

7.1 Cyber crime is on the increase and all of CVHA staff have a responsibility to ensure computer security is not compromised.

7.2 Staff should be familiar with the ICT Acceptable usage policy and will be required to sign off annually that they are familiar with and adhere to the contents of the policy.

7.3 The main threat to the security of CVHAs network is Ransomware, Hacking and Distributed Denial of Service Attacks (DDOS).

7.4 Hacking is the primary method for infiltrating networks. Hacking is when a 3rd party will try to gain unauthorised access to CVHA's computers systems and gain administrative control.

7.5 A successful hacking will compromise data stored on the network which includes person details of CVHA customers, staff, strategic plans or other sensitive data. This data can then be sold to fraudsters.

7.6 To identify any weakness in its outside internet facing perimeter, it will be the responsibility of the ICT Manager to arrange and co-ordinate an annual Penetration Test.

7.7 This will be penetration test will carried out by an independent 3rd party provider. This provider will be a member of CREST and will be changed for each testing.

7.7 Reports of the penetration test will be presented to the Audit and Risk Committee by the ICT Manager.

7.8 Ransomware is when data is encrypted by malicious software. The attackers then demand money to release a key to decrypt the data back to a readable format.

7.9 To minimise the risk of ransomware email scanning and antivirus software is utilised. Staff however should not install any unknown software to pc/laptops or click on any suspicious links in emails. If there is any doubt staff should speak to a member of the IT team.

7.9 Cyber crime is a risk to CVHA and as such is included on the Strategic Risk Register.

8. Loss or Theft of Confidential Information

8.1 All incidences of loss or theft of confidential information should be reported so that they may be investigated. A data or IT security incident relating to breaches of security and/or confidentiality could range from computer users sharing passwords to the loss or theft of confidential information either inside or outside CVHA.

8.2 A security incident is any event that has resulted or could result in:

- The disclosure of confidential information to any unauthorised person.
- The integrity of the system or data being put at risk.
- The availability of the system or information being put at risk.

8.3 Adverse impact, e.g.:-

- Negative impact on the reputation of the organisation.
- Threat to personal safety or privacy.
- Legal obligation or penalty.
- Financial loss or disruption of activities.

8.4 All incidents must be reported to your immediate line manager and to the Finance and Corporate Services Director and relevant Director. IT Security incidents should be reported to the ICT Manager using the IT Security Form in Appendix A. These reports should include:

- Details of the incident.
- Date of discovery of the incident.
- Place of the incident.
- Who discovered the incident?
- Category/classification of the incident.
- Action already taken if risk to organisation.
- Any action taken by the person discovering the incident at the time of discovery, e.g. report to police.

8.5 In the case of a serious IT security breach, the ICT Manager will instigate an investigation into the incident and will decide with the Finance and Corporate Services Director whether it needs to be reported to any regulatory bodies or other third parties, e.g. insurers or Regulator. The ICT Manager will retain a central register of all such IT incidents.

8.6 The following is a list of examples of breaches of security and breaches of confidentiality. It is neither exclusive nor exhaustive and should be used as a guide only. If there is any doubt as to what constitutes an incident, it is better to inform your line manager who will then decide whether a report should be made.

8.7 Examples of breach of security:-

- Loss of computer equipment due to crime.
- Loss of portable media devices, e.g. – memory sticks etc.
- Accessing any part of a database using someone else's password.
- Finding doors and/or windows broken and/or forced entry gained to a secure room/building in which computer equipment exists.

8.8 Examples of a breach of confidentiality:-

- Finding confidential/personal information either in hard copy or on a portable media device outside CVHA offices.
- Finding any records about a staff member, customer, or applicant in any location outside CVHA premises.
- Passing information to unauthorised people either verbally, written or electronically.

9. Passwords

9.1 Computer and network systems access is only via individual user accounts with a confidential personal password. Users will not disclose their password to anyone.

9.2 Passwords are required to be changed every 60 days. This password must be complex (letters, numbers, upper and lower case and special characters) and a minimum length of 5 characters.

9.3 Users cannot use any of their 3 previous passwords for their new password.

9.4 Lock out of the system will occur after 5 failed login attempts. The ICT Manager or IT Officer will be required to reactivate the User account.

9.5 Capita Open Housing and Open Accounts password are required to be changed every 90 days. This password must also be complex and a minimum of 5 characters.

9.6 User accounts will be disabled from both Open Housing and Open Accounts after 3 failed login attempts. The ICT Manager or IT Officer will be required to reactivate the User account.

10. Email

10.1 Email is not a completely secure medium. Users should be conscious of this and consider how emails might be used by others. Remember that emails can easily be taken out of context, which once an email is sent no one can control what the recipients might do with it.

10.2 Users should not necessarily trust what they receive in an email - in particular, users must never respond to an email request to give a username or password.

10.3 If an unsolicited email is received from an unknown source with attachments or links do not open or click on links. Notify the ICT Manager or IT Officer who will determine if the validity of the email.

11. Social Networks

11.1 CVHA respects staff members' rights to a private life and that includes joining any social sites they wish. However, information posted on such sites is classed as public and not private. Staff are therefore not allowed to disclose confidential information relating CVHA, its customers, partners, suppliers, board members, employees, etc.; on any social networking sites.

11.2 It is also prohibited to post any comments on people and events connected with CVHA, or make any remarks which could potentially bring CVHA into disrepute. Any such actions could result in disciplinary action, including dismissal.

11.3 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 staff from listing **CVHA** as their employer however we do advise against it.
- Staff should be aware of the language and content of their posts – in particular where employees have an association with their employer e.g. listing their employer or linked with colleagues.

12. File Storage

12.1 All users have access to the centrally managed file storage.

12.2 For the vast majority of applications the security of files stored centrally is appropriate. In particular this means they will be backed up.

12.3 For users who are provided with PCs, files should not be stored on local drives as these will not be backed up and data could be lost.

13. Anti-Virus Security

13.1 CVHA subscribes to 2 unique anti-virus providers. Emails are virus scanned by anti-virus software within the firewall and each PC and Server has anti-virus installed.

13.2 Updates are checked for on a daily basis, and applied when available.

13.3 Full system scans are undertaken once per week.

14. Disposal of IT Equipment

14.1 CVHA will ensure safe disposal of redundant IT equipment under the EU Directive on Waste Electronic and Electrical Equipment (WEEE).

14.2 All information will be completely removed from the system disks or other storage media prior to the equipment is disposed of.

15. System Maintenance

15.1 System back-ups will be carried out in line with CVHA's back up procedures.

15.2 The ICT Manager will ensure that appropriate maintenance contracts and system

15.3 Support arrangements are in place to provide the advice, back up and repair services necessary and to minimise any disruption to the day-to-day work of CVHA through the non-availability of CVHA's systems.

16 Our policies relating to the following are also relevant to this document and must be complied with at all times:

- Access to Information
- Data Retention
- Data Protection and Information Sharing
- Freedom of Information
- IT Acceptable Use Policy

CLYDE VALLEY GROUP

PROVIDING HOMES | SHAPING COMMUNITIES

Clyde Valley Group
IT Security Incident Form

Name:	
Date:	
Details of Incident:	
Date of Discovery:	
Who discovered the Incident:	
Category / Classification of Incident:	
Any Action Taken:	
Signed:	

To be completed by ICT Manager

Details of Incident	
Cause of Incident	
Remedial Action Taken (if any)	
Long term implications	
Date Completed:	
Signed	

IT Acceptable Usage Policy
Policy Number IT2

1. Introduction

1.1 The Clyde Valley Group (CVG) aims to help staff make best use of the various means of communications available to them in the interests of best value and delivering quality services to its customers.

1.2 CVG recognises the benefits of electronic communication making it easier for information to be distributed both internally and externally. The CVG is committed to reviewing and updating its systems and processes in line with changing technology and expectations from service users.

1.3 The CVG is also aware of the potential risks to the Group through computer misuse, which can lead to *inefficiencies, damage to data and reputation as well as legal implications.*

2. Legislation

2.1 This policy takes into account and incorporates the principles detailed with the following legislation and codes of practice.

- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Data Protection Act 2018
- The General Data Protection Regulation (EU) 2016/679 (the **"GDPR"**);
- The Privacy and Electronic Communications (EC Directive) Regulations 2003
- Human Rights Act 1998
- Electronic Communications Act 2000
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988
- Protection from Harassment Act 1997
- Defamation Act 1996
- Equality Act
- Criminal Justice and Public Order Act 1994
- Telecommunications Act 1984 (Section 43)
- Protection of Children Act 1978 (Section 1)
- Obscene Publications Act 1959
- Information Commissioner's Code of Practice on the Employee/Employer Relationship

3. Scope of the Policy

3.1 This policy relates to the use of the CVG telephone systems, including main landlines, mobiles, fax, personal computers (PC), including desktops and laptops and tablets, Wyse terminals, email and the Internet. All of these systems will be, hereafter, referred to as ICT systems. This policy applies to all employees and Board members of the CVG, and to all other persons who are granted access to CVG ICT systems. It also applies to CVG employees who have access to CVG ICT systems remotely.

4. Policy Objectives

4.1 This policy has been devised in order to enable both the CVG and its employees to gain the maximum benefit from its ICT Systems.

4.2 The Policy aims to: -

- Establish the parameters of acceptable usage;
- Safeguard confidential and sensitive information;
- Specify maintenance and monitoring arrangements;
- Raise awareness of copyright and contract issues;
- Prohibit access to inappropriate websites;
- Prohibit employees from distributing offensive material electronically;
- Protect the CVG and it employees form potential legal liabilities; and
- Encourage best practice.

5. File Locations

5.1 All electronic data stored by CVG is to be held on centralised servers. No data shall be stored locally to PCs, laptops or tablets. Data requiring access by other CVG employees will be stored under the relevant folder structure on the Group's mapped G drive. This will ensure that data can be accessed in the absence of the relevant personnel. In addition this also ensures that all data is included within the backup process minimising the risk of data loss to the CVG.

Any information CVG users may have that require a level of confidentiality e.g. Appraisal forms can be stored under the employees mapped H drive. No personal information e.g. family photos, personal letters may be stored on any of the Groups network. In addition copyrighted material that is not associated with the CVG, e.g. music or films are not to be stored on the network.

5.2 All incoming paper files should be scanned into the relative folder within the Document Management system. Paper copies should not be kept unless the law requires them to do so or they are required to be given to someone external to the CVG.

6. Security

6.1 All employees should act in accordance with the IT Security Policy, which is available within the CVG Intranet or Company Policy folder.

6.2 Employees must not move or disconnect their PC or Wyse terminals. This can cause harm to the both the equipment and the employee. IT equipment can be heavy and can result in injury if not handled properly.

6.3 Employees are accountable for the use of the PC/Wyse terminal provided to them by the CVG. Employees must not leave any PC or terminal logged on in their name and unattended. When away from the keyboard staff should log out of the system completely or lock access to the PC/terminal using the Ctrl, Alt and Del key combination will remove access for others.

6.4 Where multiple users share PCs/terminals employees must protect the confidentiality of messages and information sent to them. In order to protect this information, employees must log off when they have finished using a shared PC.

6.5 Confidential or sensitive information e.g. confidential personal details, grievance, disciplinary or harassment information should not be transferred by email.

6.6 At all times employees should act in such a manner as to protect the confidentiality of the information that is being processed, in accordance with the Data Protection Act 2018 and the General Data Protection Regulation (EU) 2016/679 (the **"GDPR"**) and, at all times, in accordance with the CVG Data Protection Registration. Details are available from the Finance and Corporate Services Director.

6.7 All PCs, terminals, monitors and printers should be switched off at night when leaving the office or disconnecting from your remote workstation.

6.8 Employees may not install any software onto any PCs. Should any individual require access to specific software then Line Managers should liaise with the ICT Manager.

6.9 Individual and personal screen savers should not be set on PC's. All machines will have a CVG house style screen saver loaded and this should remain at all times.

7. Email

7.1 Email provides a speedy, convenient and efficient means of communication. Email should not be used where there is a need for a two-way discussion or where differences of option need to be resolved or where a formal written communication is appropriate e.g. confirming contractual or legal matters. Sensitive personal data should not be sent via email.

7.2 No one, unless it is an emergency or an agreed communication should send an All Staff e-mail. All information should be posted on the CVG Intranet.

7.3 Email communication should be treated with the same degree of care and professionalism as a letter sent on CVG headed paper. Emails should adhere to the e-mail etiquette at Appendix One. It should be typed in CVG house style, a copy of which is available at G:\House Style Templates and Procedures\Clyde Valley Housing Association\Email Signature.docx

7.4 All external emails have a disclaimer attached automatically. Care should be taken to avoid entering into binding contractual relations inadvertently, making negligent statements or breaching confidentiality obligations. Employees must ensure they do not breach copyright or incur expense to the Association when copying, downloading or sending material to 3rd parties.

7.5 When going on leave or if you are going to be out of the office for a full day or more, you should ensure that you turn on your Out of Office Officer. The message should read and be formatted as follows:

I am currently on annual leave/out of the office, and will return to work on XX XX XX.

If you require urgent assistance please telephone 01698 268855, otherwise I will respond to your enquiry on my return.

Please note that your e-mail has not been forwarded to any other member of staff.

Regards,
Insert Name
Clyde Valley Housing Association

7.6 Prohibited Use of Email

The following is a list of prohibitions in relation to the use of e-mail:

- All attachments received from 3rd parties must be treated with caution and if employees are in doubt as to its content clarification should be sought from the ICT Manager or the IT Officer.

- Emails must not be used as a means to harass or intimidate other employees of the CVG or individuals external to the CVG.

- Employees must not criticise other individuals or other organisations through emails. All emails are traceable to their source.

- Confidential information regarding the CVG must not be transmitted via email.

- Emails must not be used to pass on sexually explicit, sexist, racist, or bigoted material. If such material is received please notify the ICT Manager or their Line Manager.

- Employees must not send emails that a defamatory to an individual's sexuality, disability, race, age, colour or creed, in line with the Association's Equalities Policy.

- Employees must not send any emails with non-business related attachments. These attachments use system resources and may contain viruses harmful to the organisation.

- Employees must not use their CVG email address when signing up for non-business related services. These email address can and will be passed onto other organisations and will increase the level of spam coming into the organisation.

- Email must not be used for unsolicited (spam) messaging or chain emails. If a message is received containing a message warning of a virus, do not send it on. Forward a copy on to either the ICT Manager or the IT Officer, and then delete the email.

7.7 Emails to and from CVG will be monitored on a quarterly basis by the ICT Manager, for both content and nature. Violations of the acceptable usage policy could result in disciplinary action being taken, including dismissal.

8. Internet

8.1 The Internet is largely unregulated, therefore care should be taken when access information for the Internet. Information obtained from it may not necessarily be accurate, up to date or reliable.

8.1 All employees are granted access to the Internet. The Internet may be used for the following purposes.

- To seek information on matters relevant to the employee's job
- For the purpose of job related education

8.3 CVG recognises the value of the Internet as a source of information. Due to the size and resources available it is easy to spend large amounts of time searching for information. In the case of technical difficulties, assistance should be sought from the IT Officer or the ICT Manager.

8.4 Employees may access the Internet for personal use but **only** during personal time e.g. lunch breaks, or before or after work time.

8.5 Prohibited Use of the Internet

Employees of the CVG must **not** at any time, use the Internet for the following purposes:

- The creation or transmission of defamatory material, whether on any of the CVG websites or an external website.
- Disseminate any material that may bring the CVG name or the name of any of its employees into disrepute.
- View or download pornography, illegal material or material deemed offensive by the CVG.
- Carry out freelance work unrelated to the CVG's business, gamble, play online games, contribute to internet newsgroups or conduct political activities.
- Use the Microsoft/Google Messaging Service.
- Enter into contractual agreements with any outside parties unless expressly authorised to do so by CVG.
- Buy or sell goods unless authorised to do so by the CVG.
- Intentionally access or transmit computer viruses or similar.
- To break or attempt to break through security controls.
- To intercept Internet traffic (such as email) which is not intended for them.
- Download screensavers or wallpapers.
- Download any programs.

- Access personal web based email accounts except during personal time e.g. lunch breaks, or before or after work time.

8.6 The law of copyright also applies to electronic documentation on the Internet. Information on the Internet may be subject to copyright restrictions. Employees should not therefore download copy or distribute software, files, graphic images, music, documents, messages and other materials in contravention of copyright law and applicable licenses. If in doubt advice should be sought from the ICT Manager.

8.7 Employee internet usage will be monitored on a quarterly basis by the ICT Manager, for content, timing and nature. Violations of the acceptable usage policy could result in disciplinary action being taken, including dismissal.

9 Social networks

9.1 CVG respects your right to a private life and that includes joining any social sites you wish. However, information posted on such sites is classed as public and not private. You are therefore not allowed to disclose confidential information relating CVG, its customers, partners, suppliers, board members, employees, etc.; on any social networking sites.

9.2 It is also prohibited to post any comments on people and events connected to CVG, or make any remarks which could potentially bring CVG into disrepute. Any such actions could result in disciplinary action, including dismissal.

9.3 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 ***CVG*** as their employer however we do advise against it.
- employees should be aware of the language and content of their posts – in particular where employees have an association with their employer e.g. listing their employer or linked with colleagues.

10. Telephones

Landlines

10.1 Employees are expected to use the telephones for the duties they are required to undertake. However the CVG recognises that it is necessary and reasonable for employees to use the telephone for personal calls on occasions such as emergencies.

10.2 Employees are expected to be responsible in exercising this privilege. It may be withdrawn at any time if employees are found to be abusing it. Personal calls should be restricted to personal time as far as possible, and must not interfere with employees' work or the work of others.

10.3 Employees must not be rude, defamatory, intimidate or verbally abuse either another employee of the CVG or anyone external to the CVG.

10.4 If an employee is subjected to verbal abuse from an external customer the call should be dealt with in line with the Compliments, Comments and Complaints Policy and their Line Manger should be notified.

10.5 If an employee is subject to verbal abuse from another CVG employee this call should be dealt with in line with the Dignity at Work Policy, and their Line Manager should be notified.

10.6 External calls to be answered with the following message – "Good morning/afternoon, the Clyde Valley Group".

10.7 Calls to be answered within 3 rings, but preferably 2. If an incoming call is to a 'group' a staff member within that group should pick up this call. The call should not be allowed to ring from one phone to another, this can be done by using *31.

10.8 If you hear a phone ringing, even if it is not in your department, answer the call, take/pass on a message if you are unable to assist the caller.

10.9 Direct dial numbers to be given to customers and publicised where possible.

Mobiles

10.10 In line with the Mobile Phone Policy employees are not permitted to use mobile telephones (including via hands free kits) or any other communication devices whilst driving. Employees should ensure that the vehicle is parked in a safe location and the engine is switched off, before making or receiving mobile phone calls.

10.11 Where an employee has the use of a Company mobile, personal calls can be made in emergencies as long as they are few in number and are kept short and to the point.

10.12 Employees who have mobile telephones may have them switched on and on the silent setting, subject to the following conditions:

- Call made or received during work time should be on occasions such as emergencies.
- On no account should a mobile be answered whilst on a call to a customer.
- Employees are strongly discouraged from entering into "texting" conversations.

10.13 Employees who have been issued with company mobile should set up a personalised greeting for the mobile voicemail. Any staff member who is unsure on how to set this up should seek advice from the IT Officer.

11. Voicemail/F6 messages

11.1 All CVG employees have access to their own individual voicemail account. The greeting on this voicemail account should be personalised by the employee and will be standard across the CVG. The standard greeting templates are detailed below.

11.1 Voice-mails should be checked regularly and calls returned to customers the same day, where possible, or by next working day.

11.2 Staff should arrange to check colleague's voicemails whilst they are on holiday.

11.3 F6 Messages should state an estimated return time to your desk (i.e. not "will be back - 5 mins, but "back at 10.15 am).

11.4 F6 message must match message on your voicemail if you are out of the office or at a meeting.

11.5 F6 must NOT be put on when you are in the office and working at your desk.

11.6 If you are not coming back to the office voice mails should be checked remotely. This is accessed by dialling your DDI number. When your voicemail starts enter *7 on the keypad, then listen to the instructions. This will advise you to enter your extension number followed by the password. This password will be your extension number with a zero added e.g. ext. 260 password will be 2600.

12 DND

12.1 When an employee is away from their desk for any great length of time, e.g. out of the office, attending an internal meeting, dealing with a customer/visitor in the office or on holiday, the Do Not Disturb facility should be enabled. This ensures that any incoming calls are transferred directly to voicemail. Employees must switch this facility off when they return to their desks. The Do Not Disturb must be switched off when you have clocked in and are at your desk.

12.2 If you are away from your desk for a few minutes i.e. at copier, getting cup of tea then your DND should not be put on and another member of your team should pick up any calls.

12.3 It may helpful to leave Phone Manager open on your desktop as a reminder to deactivate DND when back in office.

12.4 Where functions have a lone worker they must notify Corporate Services when they are unavailable.

12.5 There should always be at least 1 team member available to take calls (unless prior authorisation has been sought).

13 Message Templates

13.1 General

Hello you are through to XXXX voicemail. I am unable to take your call right now, but please leave your name, number and a brief message and I will call you back as soon as possible."

13.2 Out of Office for Most of Day

Hello, you have reached the voicemail of XX at the Clyde Valley Group. I am out of the office for most of the day, however will pick up my messages after 4.00 pm. Please leave a message after the tone.

13.3 Holiday

Hello, you have reached the voicemail of XX at the Clyde Valley Group. I am on leave and will return to the office on XX. Please leave a message after the tone and I will contact you on my return, or alternatively press 0 to speak to one of my colleagues.

14. Viruses

14.1 In order to minimise the risk of viruses entering CVG's computer system, employees are expressly forbidden to load unauthorised software onto the system or download software from the Internet.

14.2 Files or other material should not be loaded from a CD/DVD or USB stick, which has been brought into CVG from an external source unless this has first been virus checked with CVG approved virus-checking software.

14.3 Care should be exercised when opening unsolicited or unrecognised emails, as attachments may contain a virus. If there is any doubt whatsoever about the security of an incoming email attachment, do not open the email or its attachments and contact the ICT Manager or IT Officer for assistance.

14.4 Further information is contained within the IT Security Policy.

15. Monitoring

15.1 CVG will quarterly monitor the use of telephones, email and Internet access. The ICT systems are CVG property and it will be assumed that telephone calls made and received, email messages sent and received and Internet sites accessed will be regarded as relating to business purposes.

15.2 Monitoring will apply to all employees, and such other persons who are granted access to equipment and software in the ownership and/or custody of CVG. The overall purpose of monitoring is to ensure the efficient running of CVG's business and to prevent abuse of CVG's ICT systems. Specific reasons for monitoring include: -

- To protect CVG against incurring unwarranted legal liabilities.
- To make sure employees are not using CVG's computer facilities for purposes that are expressly prohibited.
- To check emails and email attachments for offensive material for the protection of all employees.
- To detect excessive personal use of CVG's ICT systems.
- To provide a record of transactions that may form part of unauthorised contractual agreements.

- To allow access to telephone and email messages relevant to the business of CVG whilst an employee is absent from work, for example on extended holiday or on long-term sick leave.

- To guard against computer viruses software has been installed onto all CVG's computer systems to check for viruses and to block access to known Internet sites containing offensive material such as pornographic and obscene items. All monitoring will conform to the relevant legislative provisions and will be undertaken by the ICT Manager, as appropriate. Where there is evidence of any misuse, the information will be notified to the appropriate Director who will investigate the matter further and determine the appropriate level of action.

15.3 Where misuse is alleged and subsequently confirmed, records of such misuse may be used in any subsequent disciplinary proceedings. Violations of the acceptable usage policy could result in disciplinary action being taken, including dismissal.

16. Violations of the Policy

16.1 CVG's telephones, computers including laptops; email and Internet facilities are provided for business purposes, other than in the limited personal use described previously. Access to these facilities must be authorised by the relevant Line Manager. Where it is established that an employee is misusing the facilities, such misuse may lead to the restriction or the withdrawal of any or all of the facilities. Misuse may also be a disciplinary offence and any violation of the policy may result in disciplinary action in terms as specified in CVG's Disciplinary Procedure up to and including dismissal. Violations could also amount to criminal offences and lead to prosecution.

16.2 All employees will be required to sign up the CVG's IT Acceptable Usage Policy on an annual basis to ensure they understand and accept the policy and its contents.

16.3 Violations of the IT Acceptable Usage Policy could result in disciplinary action being taken, including dismissal.

17. Responsibilities

ICT Manager

17.1 The ICT Manager will be responsible for ensuring:

- appropriate arrangements regarding authorised access, within the organisation, to telephones, including mobiles, computer facilities, email and the Internet;

- availability of access and support where needed and authorised is provided;

- the infrastructure for internal and external email use, access to the intranet, Internet and to the CVG's computer resources and telephone systems are maintained; and

- E-mail and Internet user identification and authorisation is managed.

Line Managers

17.2 All line managers have a responsibility to ensure that: -

- All staff within their teams are aware of and follow the terms of the Policy for use of the CVG's ICT systems;

- User requests for access and/or resources are properly authorised;

- Where employees are absent or long-term sick leave or on extended annual leave, arrangements are made to access employees' email and voicemail to deal with business in their absence.

Employees

17.3 Employees have the responsibility to: -

- Familiarise themselves with the terms of the Policy;

- Adhere to the terms of the Policy;

- Adhere to the associated guidance issued by the ICT Manager for use of email, Internet and telephone systems;

- Manage the security of their own desktop computer and other equipment and look after the CVG's computer resources for which they have responsibility; and

- Undertake training in relation to the use of CVG's ICT systems.

18 Information

18.1 In order to abide by this Policy, it is essential that employees are given sufficient information and training to ensure that email and Internet facilities as well as CVG's telephones and computer resources are used effectively and for valid purposes which are in line with the terms of this Policy and any relevant CVG policy or procedures. Accordingly, the level of support provided to employees to enable them to meet the standards required will include: -

- Providing a copy of the policy to all users and having this outlined annual to Departmental meetings by the IT Team;

- Ensuring new staff are provided with the necessary information as part of their work place induction;

- Ensuring all users are adequately trained before access to e-mail and Internet facilities is provided; and

- Ensuring all staff continues to receive appropriate training in the use of ICT systems as these systems are introduced and developed.

19 Our policies relating to the following are also relevant to this document and must be complied with at all times:

- Access to Information
- Data Retention

- Data Protection and Information Sharing
- Freedom of Information
- IT Security Policy

CLYDE VALLEY
HOUSING ASSOCIATION
PROVIDING HOMES | SHAPING COMMUNITIES

Declaration

I confirm that I have read, understood and accept the Clyde Valley Group's Acceptable Usage Policy.

I understand that violation of the acceptable usage policy could result in disciplinary action being taken, including dismissal.

Name	
Signature	
Date	

Email Rules and Etiquette

1. Keep email communication brief and to the point.

2. Do not send email messages in haste without carefully considering the facts and consequences of a message.

3. Consideration must always be given to attaching the appropriate level of importance to messages before their dispatch.

4. Do not send sensitive personal data via email without additional security measures being in place.

5. While ensuring that communication is of the highest level, i.e. by checking spelling and grammar, also avoid using jargon and try to use "plain English". Always adhere to the Associations House Style procedure.

6. On all occasions of planned leave you should ensure that your out of office reply is switched on, with the appropriate message as detailed at Paragraph 7.4 of the Acceptable Usage Policy.

7. Never assume that simply because you have sent a message it has been read. When it is important to know that the message has been read, set the read notification option.

8. One of the principal benefits of email is speed of communication. For that reason you should always strive to respond timeously to email messages and requests for information.

9. AVOID WRITING IN CAPITAL LETTERS, AS THIS IS THE EQUIVALENT OF SHOUTING!!!!

10. E-mail records take up a significant amount of data storage space on our server, therefore you should regularly delete all email messages that are not required. Important messages/documentation that requires to be retained should be moved and filed in an appropriate place.

11. Never disclose your email address to unknown individuals/organisations or leave it on open websites.

12. Give out your email address accurately and only to reputable individuals or organisations.

13. Check email regularly, at least twice a day, ignoring a mail message is confusing and discourteous to the sender.

14. Wherever possible avoid sending excessively large Emails or attachments of 10MB or greater. This is not an economic or sensible way to handle large documents and can effectively degrade the system.

15. Do not use the system to send illegal material (e.g. unlicensed software), forward chain letters, harass or threaten anyone or send abusive, unsolicited, frivolous or inappropriate messages. Apart from being discourteous or offensive you may also be breaking the law or violating CVG's Equalities or Dignity at Work Policies.

16. Do not send All Staff emails – use the intranet.

17. Consider who you are sending and copying your e-mails to. Assume that if you send it to someone that you expect that person to action it.

15 Our policies relating to the following are also relevant to this document and must be complied with at all times:

- Access to Information
- Data Retention
- Data Protection and Information Sharing
- Freedom of Information