TOLLCROSS
housing association

ICT Acceptable Usage Policy

Prepared By	**Clive Douglas, Chief Executive**
Policy Created	/
Date of Last Review	/
Date of Current Review	June 2013
Date of Next Review	June 2016
Reviewed By	Board

CORPORATE FIT	
Internal Management Plan	✓
Risk Register	✓
Business Plan	✓
Regulatory Standards	✓
Equalities Strategy	✓
Legislation	✓

On request, the Association can provide translations of all our documents, policies and procedures in various languages and other formats such as computer disc, tape, large print, Braille etc. and these can be obtained by contacting the Association’s offices.

Tollcross Housing Association
ICT Acceptable Usage Policy

1. Introduction

1.1 Tollcross Housing Association (THA) 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 THA recognises the benefits of electronic communication making it easier for information to be distributed both internally and externally. THA is committed to reviewing and updating its systems and processes in line with changing technology and expectations from service users.

1.3 THA is also aware of the potential risks to THA 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 1998
- 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
- Disability Discrimination Act 1995
- Race Relations Act 1976 and Race Relations (Amendment) Act 2000
- Sex Discrimination Act 1975
- 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 THA 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 THA, and to all other persons who are granted access to THA ICT systems. It also applies to THA employees who have access to THA ICT systems remotely.

4. Policy Objectives

4.1 This policy has been devised in order to enable both the THA 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 THA and it employees from potential legal liabilities; and
- Encourage best practice.

5. File Locations

5.1 All electronic data stored by THA is to be held on centralised servers. No data shall be stored locally to PCs, laptops or tablets. Data requiring access by other THA employees will be stored under the relevant folder structure on THA'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 THA.

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

6. Security

6.1 All employees should act in accordance with the IT Security Policy, which is available within the THA Intranet.

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 THA. 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 1988 and, at all times, in accordance with the THA Data Protection Registration. Details are available from the Corporate Services Manager.

6.7 All PCs, terminals, monitors and printers should be switched off at night when leaving the office.

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 THA 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 opinion 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 THA Intranet.

7.3 Email communication should be treated with the same degree of care and professionalism as a letter sent on THA headed paper.

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 Assistant. 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 0141 763 1317, 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
Tollcross 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 Assistant.

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

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

- Confidential information regarding the THA 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 are 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 THA 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 Assistant, and then delete the email.

7.7 **Emails to and from THA 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 accessing information from 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 THA 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. Excessive surfing or browsing should not therefore be undertaken. If the information being sought cannot be located within 15 minutes, and assistance is required then browsing should stop and advice sought from your Line Manager. In the case of technical difficulties, assistance should be sought from the IT Assistant 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 THA must **not** at any time, use the Internet for the following purposes:

- The creation or transmission of defamatory material, whether on any of the THA websites or an external website.

- Disseminate any material that may bring the THA name or the name of any of its employees into disrepute.

- View or download pornography, illegal material or material deemed offensive by the THA.

- Carry out freelance work unrelated to the THA’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 THA.

- Buy or sell goods unless authorised to do so by the THA.

- 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 THA 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 THA, 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 THA, or make any remarks which could potentially bring THA 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 ***THA*** 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 THA 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 THA or anyone external to the THA.

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

10.5 If an employee is subject to verbal abuse from another THA 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, Tollcross Housing Association**".

10.7 Calls to be answered within 3 rings. 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:

- Calls 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 Assistant.

11. Viruses

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

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

11.3 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 Assistant for assistance.

11.4 Further information is contained within the IT Security Policy.

12. Monitoring

12.1 THA will quarterly monitor the use of telephones, email and Internet access. The ICT systems are THA 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.

12.2 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 THA. The overall purpose of monitoring is to ensure the efficient running of THA's business and to prevent abuse of THA's ICT systems. Specific reasons for monitoring include: -

- To protect THA against incurring unwarranted legal liabilities.

- To make sure employees are not using THA'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 THA'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 THA 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 THA'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.

12.3 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.

13. Violations of the Policy

13.1 THA'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 THA's Disciplinary Procedure up to and including dismissal. Violations could also amount to criminal offences and lead to prosecution.**

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

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

14. Responsibilities

ICT Manager (currently 3rd party)

14.1 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 THA's computer resources and telephone systems are maintained; and
- E-mail and Internet user identification and authorisation is managed.

Line Managers

14.2 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 THA's ICT systems;

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

- Where employees are absent on 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

14.3 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 THA's computer resources for which they have responsibility; and

- Undertake training in relation to the use of THA’s ICT systems.

15. Information

15.1 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 THA'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 THA 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 annually 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.

16. Review

16.1 This Policy will be reviewed every three years or sooner to reflect changes in legal issues or best practice.

Appendix One

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 in 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 THA’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.