Renfrewshire Valuation Joint Board

INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) Acceptable Use Policy V. 2

Title	ICT Acceptable Use Policy
Author	Kate Crawford Depute Assessor & ERO
Approved By	Management Team
Date of Approval	June 2014
Reviewer	Assistant Assessor
Review Date	2-Yearly

Review History

Review No.	Details	Release Date
1.1	Depute Assessor	June 2015
1.2	Reviewed as a result of reviewing policy IG6 Records management as IG6 references SP1.02 – David Findlay	January 2018
2	Assistant Assessor and Data Protection Officer	September 2024

1. Policy objectives:

The aim of this policy is to define clear rules for the use of the ICT system and other information assets within Renfrewshire Valuation Joint Board hereinafter referred to as the "Board".

This Policy further supports the Information Security Policy which aims to protect information assets and systems owned and used by the Board from threats, whether internal or external.

In order to ensure that the Board can have confidence in its information, and that will be available when it is needed, information and the ICT systems used for processing must be used, managed and secured appropriately.

This Policy supports the Board's Code of Conduct, the overriding principles of which apply at all times.

2. Applicability:

This policy is applicable to all Board employees, contractors and relevant third parties.

3. Scope:

The ICT systems and information within scope of this policy are to be taken to include but are not limited to files, documents, diagrams, contracts, schedules, plans, directories, contact lists which are exchanged directly or as the content of or attachment to e-mails together with content passed within instant messaging. The requirements of this policy are to be met irrespective of the media used for the exchange i.e. both hardcopy and softcopy.

4. Definitions

- **IT system** – includes all servers and clients, network infrastructure, system and application software, data, and other computer subsystems and components which are owned or used by the Board, or which are under the Board's responsibility. The use of an IT system also includes the use of all internal or external services, such as Internet access, e-mail, etc.
- **Information asset** – in the context of this Policy, the term 'information asset' is applied to information systems and other information/equipment including paper documents, mobile phones, portable devices such as laptops, tablets, data storage media, etc.
- **Internet** - Refers to the use of any resources from the World Wide Web, whether browsed or downloaded.
- **E-mail -** Refers to all use of e-mails whether internal or external and where permitted for business purposes, social media sites.

5. Principles

a. Responsibility for assets

Each information asset has an owner designated in the Board's Asset Inventory. The asset owner is responsible for the confidentiality, integrity and availability of information of the asset in question.

b. Acceptable use

The Board's ICT systems and information exist to support and enable our business activities. The Board trust our employees to be fair and sensible when using its ICT systems and information. The following guidance is provided to remove any potential ambiguity as to the Board's expectations in this area. If employees are uncertain as to any aspect of this, they should consult their manager or a member of the IT Team.

6. Data Security

6.1 Data Security

- Users must not send, upload, remove on portable media or otherwise transfer to a non-Board system any information that they should reasonably regard as being confidential to the Board.
- Users must keep passwords confidential and not allow others to access their accounts. Users must ensure all passwords comply with the Board's password policy.
- Users who are supplied with computer equipment by the Board are responsible for the safety and care of that equipment, and the security of software and data stored it and on other Board systems that they can access using it.
- Because information on portable devices, such as laptops, tablets and smartphones, is especially vulnerable, special care should be exercised with these devices both on-site and when out of the office environment. Users will be held responsible for the consequences of theft of or disclosure of information on portable devices entrusted to their care if they have not taken reasonable precautions to secure it.
- All workstations (desktops and laptops) should be secured with a lock-on-idle function after a maximum of 15 minutes of inactivity. In addition, the screen and keyboard should be manually locked by the responsible user whenever leaving the machine unattended.
- Users who have been charged with the management of those systems are responsible for ensuring that they are always properly protected against known threats and vulnerabilities, as far as is reasonably practicable and compatible with the designated purpose of those systems.
- Users must always guard against the risk of malware (e.g., viruses, spyware, Trojan horses, rootkits, worms, backdoors) being imported into Board systems by whatever means and must report any actual or suspected malware infection immediately via the security incident procedure.

6.2 Internet & E-mail

Use of the Internet and e-mail is to provided for business purposes.

Any reasonable, limited, personal use of the Board ICT services, and equipment must comply with the Code of Conduct. Reasonable personal use of such services and equipment:

- Should not interfere with the performance of your duties.
- Should not take priority over your work responsibilities.
- Should be lawful and in accordance with this ICT Acceptable Use Policy, the Information Security Policy and all other advice and guidelines circulated by the Board.

For the purposes of information security specifically, the following prohibitions are in place:

- Forwarding of e-mails to or from personal e-mail accounts is prohibited.
- The use of personal e-mails for sharing of RVJB data is prohibited.
- Using RVJB email addresses to subscribe to mailing lists, provision as contact details, or otherwise create accounts for purposes other than those that are work-related is prohibited.

When using e-mail as a means of communication, it should be kept in mind that:

- e-mails are potentially subject to disclosure under the Freedom of Information (Scotland) Act 2002 or Data Protection Act 2018, including all expressions of fact, intent and opinion.
- e-mails may be produced in court in the same manner as any other document

- A standard footer must be applied to all external e-mail messages, limiting liability and including an appropriate disclaimer.
- The content of e-mail messages and Internet sites browsed or downloaded must not contain anything that could be construed as aggressive, racist, sexist, in poor taste, unsubstantiated opinion, commercially or personally defamatory or otherwise potentially offensive.
- All users must ensure compliance with all relevant legislation.
- All users must maintain awareness of the risks presented by using the Internet.
- All Internet and e-mail traffic, including attachments and usage of the facilities may be monitored in accordance with current legislation and with respect to personal privacy and any action deemed appropriate taken.
- Inappropriate use of the Internet, or e-mail services may result in the initiation of disciplinary action against all individuals involved. Malicious use of the Internet or e-mail services will result in the initiation of disciplinary action against all individuals involved.

6.3 Backups

- ICT system users must ensure that data they wish to be backed up is stored only on network drives which incorporate this functionality.

6.4 Antivirus protection

- Antivirus software is installed on each computer with activated automatic updates. All users must not attempt to remove, suspend or otherwise tamper with this software.

6.5 Authorisations for information use

- Users of information assets may only access those information assets for which they have been explicitly authorised by the asset owner.
- Users may use the information assets only for purposes for which they have been authorised, i.e. those for which they have been granted access rights.

6.6 User account responsibilities

- ICT system users must not directly or indirectly, allow another person to use their access credentials i.e. username and password.
- Any password which is suspected of having been disclosed is to be changed immediately.
- The use of group usernames is not permitted unless authorised by the IT Team.
- The owner of the user account is deemed to be its user and is held responsible for its use and all transactions performed through their user account.

6.7 Copyright

- Users must not make unauthorised copies of software owned by the organisation, except in cases permitted by law, by the owner or the Assistant Assessor.
- Users must not copy software or other original materials from other sources and are liable for all consequences that could arise under the intellectual property law.

6.8 Monitoring the use of information and communication systems

- All data which is created, stored, sent or received through the information system or other organisation's communication systems, including various applications, e-mail, Internet, etc. whether it is perceived to be personal or not, is considered to be under the ownership of the Board.
- Users agree that authorised persons from the organisation may within the bounds of relevant legislation, access all such data and that access by such persons will not be considered a violation of the users' privacy.

- The organisation may use specialised tools for the purpose of identifying and blocking forbidden methods of communication and for the filtering out of forbidden content.

6.9 Incidents

- Each employee, supplier or third person who is in contact with information and/or ICT systems belonging to the Board or its clients must report any system weakness, incident or event, as specified in the Security Incident Reporting and Management Policy.

6.10 Taking assets off-site

- Equipment, information or software, regardless of its form or storage medium, may not be taken off-site without prior written permission by the user's Line Manager or the Assistant Assessor
- As long as such assets are held outside the organisation, they are the responsibility of the person who was granted permission for their removal.

6.11 Return of assets upon termination of contract

- Upon termination of an employment contract or other contract on the basis of which various equipment, software or information in electronic or paper form is used, the user must return all such information assets to their Line Manager or the Service Co-Ordinator/Assistant Service Co-Ordinator.

6.12 Social Media & Networking

- Information published on any personal social media sites should comply with Board confidentiality and disclosure of proprietary data policies. This also applies to comments posted on other blogs, forums, and social networking sites.
- Employees should be respectful to the Board as an Employer, other employees, customers, partners, and competitors always.
- Social media activities should not interfere with work commitments.
- Your online presence reflects on the Board. Be aware that your actions captured via images, posts, or comments can reflect that of the Board.
- Do not make reference to stakeholders and partners, without their express consent. In all cases, do not publish any information regarding a stakeholder and/or partner before, during or after the engagement.
- Respect copyright laws, and reference or cite sources appropriately. Plagiarism applies online as well.
- The Board's logo is not to be used without written consent.

6.13 Clear Desk & Office Areas

- Employees, contractors and third parties operating on the Board's premises are to ensure that all documentation is removed from their desks when they are left unattended for an extended period e.g. over lunch and at the end of the working day.
- All documentation is to be locked away in secure storage when not in use.
- Office doors and windows are to be closed and where possible, locked at the end of the working day.
- Documents are to be removed from multi-functional devices (MFDs) and scanners once they have been produced.
- A check of all MFDs and scanners is to be made at start and the end of the working day to ensure that they are clear of any documents containing potentially sensitive information.

7. Unacceptable Use

It is unacceptable under any circumstances to use information assets in a manner that unnecessarily takes up capacity, weakens the performance of the ICT system or poses a security threat.

It is also specifically unacceptable to:

- Download image or video files which may cause distress, concern, embarrassment or offence to other employees, contractors, third parties or visitors.
- Engage in any business-related activities which are not directly connected with those of the Board.
- Make any attempt to circumvent or otherwise short-cut security controls.
- Install software on a Board computer or other device without prior explicit permission from the Assistant Assessor and/or IT Team.
- Download program code from external media
- Install or use peripheral devices such as modems, memory cards or other devices for storing and reading data e.g. USB flash drives without prior explicit permission by the Assistant Assessor and/or IT Team.

  Further examples of unacceptable activity on RVJB ICT services and equipment are set out at Appendix 1 to this Policy.

8. Misuse

It is the responsibility of every user to use all ICT services and equipment appropriately, legally and in accordance with this ICT AUP and the wider policies of the Board.

Furthermore, it is a criminal offence under the Computer Misuse Act 1990 to carry out the following activities:

- Unauthorised access to computer material, i.e hacking
- Unauthorised modification of computer material
- Unauthorised access to computer material with the intent to commit or facilitate the commission of further offences.

Undertake the harassment of others by electronic means.

9. Implementation & Review:

Responsibility for the implementation and two-yearly review of this policy together with the communication of any resultant amendments across the organisation and to relevant third parties is assigned to the Assistant Assessor.

APPENDIX 1 - Unacceptable activity on RVJB ICT services and equipment

It is the responsibility of every user to use ICT services and equipment appropriately, legally and in accordance with this ICT Acceptable Use Policy (ICT AUP) and the wider policies of the RVJB, including the Code of Conduct for Employees, the Information Security Policy, and Data Protection Policy.

Any breach of the ICT Acceptable Use Policy will be viewed seriously and may result in action being taken under the RVJB's Disciplinary Procedures. Certain breaches of the ICT AUP will constitute a criminal offence.

In line with the ICT AUP, users should note that the following will be a breach of the ICT AUP:

- Attempting to gain or gaining unauthorised access to any part of the RVJB network, system or ICT estate, including, servers or server rooms, hub rooms, computers, laptops, mass storage devices, printers etc. Such activity may be considered a criminal offence and gaining such access with the intention of modifying data or programs is a more serious criminal offence.

- Disclosure of your own personal log on credentials to another individual, whether an employee of the RVJB or not to enable them to gain access to the ICT Services.

- Attempting to gain or actively gaining access to inappropriate internet sites and obtaining or attempting to obtain pornographic material or material that would offend others on the basis of the 9 protected characteristics (age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion and belief, sex and sexual orientation) and material relating to illegal activities or activities otherwise prohibited.

- Attempting to or gaining access to any internet site, the content of which promotes terrorism or any other illegal activity.

- Loading any software for personal use onto the RVJB's desktop or laptop computers (including but not limited to screensavers, games, CDs from a computer magazine or shareware from the internet). IT Team will uninstall any unauthorised software they find while carrying out their regular duties.

- Installing, modifying or introducing any new or existing programs or data with the intention of causing harm to existing systems or information held on RVJB systems. (Such activity may be considered a criminal offence).

- Installing, modifying or introducing any new or existing programs without approval of the IT team.

- Subscribing to mailing lists through the internet for purposes other than those that are work-related.

- Generating messages in a way that makes them appear to have come from someone else.

- Sending emails which are abusive, offensive, libellous or a nuisance.

- Sending of emails which are of a defamatory, threatening, abusive, insulting homophobic nature, promote racial hatred or in any other way cause fear alarm or embarrassment to the recipient.

- Generating and or distributing chain email.

- Using ICT facilities for private commercial activity.

- Contravening rules for personal use of ICT facilities.
- Downloading or distributing any material which is protected by copyright without the appropriate permissions or licence. (Such activity may be considered a criminal offence).
- Using RVJB ICT services to promote political views or campaign activity.
- Indulging in any activity which may cause embarrassment to the RVJB or brings the RVJB into disrepute.
- Running a personal website from RVJB premises.
- Improper use of official templates or letterhead.
- Downloading and re-using any images, texts or materials which are copyright protected.
- Use of unlicensed computer software on RVJB ICT equipment.
- Downloading, displaying, using or sending any defamatory, discriminatory, obscene, abusive material that would otherwise be in breach of any legislation or legal obligation placed on the RVJB.
- Posting statements on any Internet website that are defamatory, misleading or false about the RVJB, its partners or any related organisation.
- Posting or disseminating the RVJB's confidential information of any sort outside the business including to personal email addresses; and
- Posting or disseminating anything electronically that would cause embarrassment to the RVJB or is politically sensitive or potentially controversial.

The above items are examples of unacceptable use, but this is not an exhaustive list. Each incident in breach of the ICT AUP will be assessed on its individual circumstances.