Renfrewshire Council

ICT ACCEPTABLE USE POLICY

(v3.2)

August 2014

Document Control

Change Record

Version	Date	Author	Reason for Issue/ Change
1.0	04/02/2010	Fiona Davidson, ICT Manager	First draft issue for TU discussion
2.0	29/03/2010	Fiona Davidson, ICT Manager	Amendments made in line with TU's, including the EIS and also Legal services
3.0	15/04/2010	Fiona Davidson, ICT Manager	Amendment made as requested by Director of Corporate Services, and IT Manager
3.1	18/11/2013	Heather Semple, Solicitor (Information Governance)	Legal Services issue first draft for consultation.
3.2	20/12/2013	Heather Semple, Solicitor (Information Governance)	Consultee comments incorporated
3.4	27/08/2014	Heather Semple, Solicitor (Information Governance)	Draft issued to Finance & Resources Board for approval.

Document Review and Approval

Name	Action	Date	Communication
Allison Black (Legal)	Review	18/11/2013	E mail
Edith MacArthur (ICT)	Review	18/11/2013	E mail
Andrea McMahon (Internal Audit)	Review	18/11/2013	E mail
Lenore Robson (HR)	Review	18/11/2013	E mail
ISG	Review	25/11/2013	E mail
IMGG	Review	25/11/2013	E mail

Reform & Change Management Team	Review	25/11/2013	E mail
Trade Unions	Review	9/12/2013	E mail
Finance and Resource Policy Board	Request for Approval	27/08/2014	Board Report

Related Documents

Ref	Document Name/ Version	Document Location
1	Information & Communications Technologies (ICT) Acceptable Use Policy (March 2010)	Renfo
2	Guidance on Legal Issues when using ICT Facilities	Renfo
3	Guidance on Unacceptable activity when using ICT Facilities	Renfo
4	Email Good Practice Guide	Renfo

Title	**ICT Acceptable Use Policy**
Author	Heather Semple, Solicitor (Information Governance)
Issue Date	August 2014
Subject	Information Communication and Technology
Description	Renfrewshire Council's policy on the acceptable use by employees, Elected Members, Teachers, third party suppliers, partner agencies and voluntary groups, of the Council's ICT services and equipment.
Version	V3.2
Source	ICT Acceptable Use Policy, Renfrewshire Council, March 2010
Updating Frequency	2-yearly
Right	Not Protectively Marked
Category	Information Communication Technology
Identifier	

Contents

Part I: Policy Statement

This part of the Policy document defines the scope and principles of the Policy. This section also sets out the groups of personnel who are subject to the Policy.

The Council is committed to adopting a fair, transparent and consistent approach in the application of this Policy regardless of race, religion or belief, disability, age, sex, gender reassignment, sexual orientation, marriage and civil partnership, pregnancy and maternity and Trade Union membership or activity.

1. Introduction

1.1. Renfrewshire Council (the **Council**) relies extensively on effective and efficient Information and Communication Technology (**ICT**) in exactly the same way as any other public or private organisation responsible for the delivery of services. The Council recognises that ICT Facilities play an essential role in enabling greater efficiency, and can significantly improve business performance.

1.2. This ICT Acceptable Use Policy (this **Policy**) defines the acceptable use of the Council's ICT Facilities, including but not limited to electronic networks, software applications (e.g. Internet and email systems, and social media etc.) and associated equipment (including portable computing devices, mobile communication devices, printers and photo copying services, etc.) provided by the Council and external contractors for Council's business purposes. **This Policy applies to the use of all ICT Facilities regardless of whether it is used on Council premises or elsewhere.** In order to ensure the efficient and responsible use of the Council's ICT Facilities, employees and other users must read, understand and agree to this Policy and follow the Council's procedures and best practice guidelines.

1.3. Access to and use of the Council's ICT Facilities is to enable the business of the Council to be carried out effectively and efficiently. Access to and the use of the ICT Facilities can be withdrawn at any time if it is considered that ICT Facilities are being used in breach of this Policy.

1.4. The Council is obliged to ensure that appropriate operational, technical and organisational measures have been introduced to ensure Council information and its associated Infrastructure is protected against damage and risk. The Council must also ensure these measures are maintained to support the continuous service delivery within the legislative boundary and statutory duties. It is also vital that information held by the Council is not exposed to unnecessary risk. Therefore, as part of the Council's obligations in respect of both compliance with legislation and addressing potential risks, acceptance of the terms and conditions of this Policy is mandatory if access to ICT Facilities is to be permitted.

1.5. This Policy must be read in conjunction with other relevant Council policies, procedures and guidance, including but not limited to:

1.5.1. Code of Conduct for Employees;

1.5.2. Information Management Policy;

1.5.3. Information Security Policy;

1.5.4. Records Management Policy;

1.5.5. Data Protection Policy;

1.5.6. Use of Council Resources Policy

1.5.7. Guidance on the Responsible Use of Personal Data and Confidential Information;

1.5.8. Privacy Impact Assessment;

1.5.9. Guidelines on the use of Mobile Devices;

1.5.10. Guidance on Unacceptable activity when using ICT Facilities;

1.5.11. Guidance on Legal Issues when using ICT Facilities; and

1.5.12. Email Good Practice Guide.

These documents are available on the Council's intranet, Renfo.

1.6. For Council employees, failure to comply with any aspect of this Policy may be viewed as a disciplinary matter and may, therefore, be subject to the Council's Disciplinary Procedures (or the relevant disciplinary policy for Teachers where relevant).

1.7. Where any requirement of this Policy appears to have been breached, whether deliberately or accidentally, users should report the matter immediately to a Line Manager or Senior Officer and to the ICT Service Desk.

1.8. All users of the Council's ICT Facilities should read this Policy carefully in order to understand its terms. Failure to follow the terms of this Policy may result in access to the Council's ICT Facilities being restricted or withheld and may lead to disciplinary action being taken.

1.9. Any queries in respect of this Policy should be referred to a Line Manager, Senior Officer or the ICT Service Desk.

1.10. Any training seminars or update briefings from the Council in relation to the acceptable use of ICT Facilities should be attended. Similarly all materials or alerts issued in relation to acceptable use of ICT Facilities should be read.

2. Definitions

The following terms are given the following meanings throughout this Policy:

Business Use means all use which is related to Council duties and responsibilities;

ICT Facilities means all facilities, equipment, services and systems (including the Internet and intranet) which enable the function of information processing and communication by electronic means;

Personal Use means all use other than Business Use;

Senior Officer means a Council officer of management level and above; and

Working Hours means the period of time that the individual spends at paid work (this is highlighted in the individual employee's contract of employment). This does not include recognised unpaid breaks. For example, amongst Council employees common Working Hours are Monday to Thursday 0845 - 1645 and Friday 0845 – 1555 (in this example an unpaid meal break can be taken between 1200 – 1400).

3. Purpose

3.1. The purpose of this Policy is to ensure that all users of the Council's ICT Facilities are fully aware of what is acceptable and what is not acceptable behaviour when using ICT Facilities. All users must also be aware of their responsibilities when using any of the ICT Facilities. This Policy also aims to provide guidance as to what behaviour will not be permitted, under any circumstances, and the possible sanctions should there be a failure to comply with this Policy.

3.2. The following principles underpin this Policy:

3.2.1. The Council's ICT Facilities must remain secure;

3.2.2. The Council accepts its obligations to keep data secure;

3.2.3. The Council's ICT Facilities are primarily for Business Purposes and for other approved purposes set out in this Policy or as agreed with a Line Manager/ Senior Officer; and

3.2.4. Inappropriate, unlawful or unauthorised activity is not permitted.

3.3. It is also the purpose of this Policy to ensure that the Council meets its obligations in terms of various legislative and regulatory provisions including, but not limited to:

- Civic Government (Scotland) Act 1982
- The Communications Act 2003
- Computer Misuse Act 1990
- The Copyright, Designs and Patents Act 1988
- The Data Protection Act 1998
- The Digital Economy Act 2010
- Equality Act 2010
- The Freedom of Information (Scotland) Act 2002
- Human Rights Act 1998
- Obscene Publications Act 1964
- The Privacy and Electronic Communications (EC Directive) Regulations 2003

- Protection from Harassment Act 1997
- Public Services Network (PSN) Code of Connection
- Regulation of Investigatory Powers Act 2000
- Regulation of Investigatory Powers (Scotland) Act 2000
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

Users of the Council's ICT Facilities are bound by all relevant legislation. Further details are on the Council's intranet, Renfo.

4. Scope

4.1. It is the responsibility of all users of the Council's ICT Facilities to comply with this Policy and be familiar with its content.

4.2. This Policy applies to all of the following categories of personnel who have access to the Council's ICT Facilities:

4.2.1. All Council employees including but not limited to those who work full-time, part-time, job share, compressed hours, remote workers and recognised home-workers;

4.2.2. Teachers situated within the Council Headquarters and in all teaching establishments under the responsibility of the Council's Education and Leisure Services;

4.2.3. Elected Members;

4.2.4. Employees of partner agencies, whether co-located within Council premises or not;

4.2.5. Third party suppliers and contractors;

4.2.6. Employees and members of Arms Length Organisations (ALO);

4.2.7. Members of voluntary organisations; and

4.2.8. Any other party who, in providing a service to or receiving a service from the Council requires access to the Council's ICT Facilities.

4.3. Before being provided with access to Council ICT Facilities all third party suppliers and contractors and any other party who, in providing a service to or receiving a service from the Council requires access to the Council's ICT Facilities must sign the Declaration attached as Appendix 1.

<u>Employees</u>

4.4. It is the responsibility of all employees to ensure they have read, understood and observe this Policy and any other relevant associated codes of practice and guidance documents.

4.5. Employees must fully understand that all ICT Facilities are provided as business tools and that there is no individual right of privacy.

4.6. The Council's ICT Facilities may be used to allow employees to undertake activities, such as continuous professional development (CPD) during Working Hours, with prior notification and agreement from a Line Manager or Senior Officer.

Line Managers/ Senior Officers

4.7. Line Managers/Senior Officers are responsible for ensuring that employees and other users of the Council's ICT Facilities within their own service are informed of and work in a manner that is consistent with the principles outlined in this Policy.

Elected Members

4.8. Elected Members may use Council ICT Facilities while engaged on Council business for example when dealing with correspondence from constituents.

4.9. Elected members may also use Council ICT Facilities (except access to personal emails or personal use of the council's email system) for incidental Personal Use.

4.10. Elected members must not use Council ICT Facilities for party political or campaigning purposes at any time.

Teachers

4.11. Teachers are permitted to fulfil their continuous professional development (CPD) requirements during their 'non-contact time' (which is within Working Hours) with agreement from the Head Teacher.

Contractors/ External Partners

4.12. The Council's partner agencies include: Renfrewshire Leisure Limited, Renfrewshire Valuation Joint Board, Scotland Excel and the NHS organisations where shared or joint services are provided using Renfrewshire Council ICT Facilities (note this list is not exhaustive).

4.13. Contractors are personnel employed by external companies which have been awarded a contract to provide services to the Council for the duration of the contract.

4.14. Contractors/External Partners must be made aware of this Policy and any relevant associated codes of practice and guidance. Appropriate ICT access will be provided where necessary to allow work to be carried out as set down by the Council.

4.15. Use of Council ICT Facilities by contractors and employees of partner agencies for Personal Use is not permitted. Contractors/ External Partners will be made aware of this prior to commencing any work on behalf of the Council which requires them to have access to or use Council ICT Facilities.

Employees of Arms Length Organisations (ALO)

4.16. Employees of partner agencies who have access to Council ICT Facilities are not permitted to use the Council ICT Facilities for Personal Use.

4.17. Employees and Members of Arms Length Organisations are permitted to use Council ICT Facilities in accordance with the provisions of this Policy.

All other parties

4.18. All other parties who have, for business purposes, access to Council ICT Facilities will not use this access for any Personal Use under any circumstances.

4.19. Where any party is found to be acting contrary to section 4.18 above they will have their access immediately withdrawn and subject to review.

5. Unacceptable Use

5.1. Use of ICT Facilities must be reasonable and responsible.

5.2. Breach of this Policy could be considered misconduct or gross misconduct and could lead to dismissal in line with the Council's Disciplinary Procedures (or the relevant disciplinary policy for Teachers where relevant).

5.3. Some examples of unacceptable behaviour whilst using Council ICT Facilities and facilities whether for business or the limited permitted Personal Use are outlined on the Council's intranet, Renfo ("Guidance on Unacceptable activity when using Council ICT Facilities").

5.4. Where any activity is discovered and the conduct is considered to be of a criminal nature, the Council reserves the right to report the circumstances to the police for further investigation. Such activity includes, but is not limited to:

5.4.1. Use of Council ICT Facilities to operate, control or in any other way facilitate the running of a business;

5.4.2. Use of Council ICT Facilities to copy or illegally access or transfer Council data;

5.4.3. Use of Council ICT Facilities to instigate, promote or in any other way support or encourage bullying, harassment, racism, offensive or threatening activity; or

5.4.4. Use of Council ICT Facilities to gain access to any Internet based website, whether free to access or subscription based, which advertises or promotes, sells or offers for sale any service or services, content or material which is offensive, of a sexually explicit nature, depicts acts of depravity or may contain material access to or possession of which may constitute a criminal offence, under either UK or EU criminal law.

6. Use of ICT Facilities for Business Use

6.1. The purpose of the Council's ICT Facilities is to enable tasks to be carried out in relation to the provision of Council services or which support the Council's objectives and goals.

6.2. It is important to understand that the Council owns and is liable not only for the equipment, hardware and software, but also for any information including emails sent and received and all Internet/intranet pages generated or stored on the Council's ICT equipment.

6.3. Employees studying for a work related qualification with Council support may use Council ICT Facilities to prepare study material. However, this must be done in non-Working Hours unless otherwise approved by a Line Manager or Senior Officer. This should be in accordance with the 'Use of Council Resources' policy, available on the Council's intranet, Renfo.

6.4. The Council ICT Facilities (for example, the Internet) may not be used to prepare, research or produce material in connection with a private business, or any area which may be deemed as a conflict of interest, as detailed in the 'Code of Conduct for Employees' and the 'Use of Council Resources' policy. If in doubt, further clarification can be sought from ICT Services, Legal & Democratic Services or HR and Organisational Development.

6.5. Employees may be able to use the Council's ICT Facilities outwith their normal Working Hours with the prior agreement of their Line Manager or Senior Officer. Any such use should be limited and in line with this Policy, and the 'Use of the Council Resources' policy available on the Council's intranet, Renfo.

7. Use of ICT Facilities for Personal Use

This section must be read together with the overall principles of this Policy, and in particular with the following sections in Part II of this Policy: Email (section 5); the Internet Usage (section 6); Portable Electronic Devices (section 10); and Council Telephone Systems (section 11).

7.1. Limited Personal Use of Council ICT Facilities is permitted, as per the terms of this Policy. For the avoidance of doubt, Personal Use of the Council's email system is not permitted at any time (as per section 5 of this Policy).

7.2. Personal Use of the Council's ICT Facilities must be kept to a reasonable level and must not take place during the user's Working Hours unless authorised by a Line Manager or Senior Officer (or Head Teacher if the user is a Teacher within a School).

7.3. For the avoidance of doubt, users on the Flexible Working Hours Scheme (Flexi Time) must be clocked out of the flexi system when using the ICT Facilities for Personal Use.

7.4. Use of the Council's printing facilities for Personal Use is not permitted at any time, without prior permission from a Line Manager or Senior Officer. Printers can be audited to ensure that this instruction is being complied with.

7.5. Excessive use of any of the Council's ICT Facilities by Elected Members for Personal Use may result in this being raised with the relevant Group Leader and may also result in the use of those ICT Facilities being withdrawn.

7.6. The Council will not be responsible for any damage, distress or loss a user may suffer, including loss of data, or losses sustained in any on-line financial transaction while using the Council ICT Facilities.

7.7. Personal Use of Council ICT Facilities is not granted to contractors. This must be conveyed to any contractors working for the Council before they commence their work.

8. Monitoring Use of ICT Facilities

8.1. The Council has both technical and organisational controls which enable the Council to actively monitor all activity taking place.

8.2. It is the responsibility of all users to use the Council's ICT Facilities responsibly and only in connection with the role they are employed to fulfil. Where, during monitoring, it becomes apparent or it is suspected that a user has or may have undertaken activity that is outwith their remit or has carried out any unauthorised activity, this will be subject to further enquiry either internally or by external agencies, where appropriate.

8.3. ICT Services are responsible for logging use of ICT Facilities and collecting relevant information which may be used to ensure that this Policy and the relevant legislation are complied with. Internal Audit may make use of this information as part of ongoing Audit activity. The Council may also provide this information to assist Police investigations and to respond to orders of court.

8.4. In the event that the Council is legally required to provide access to information held on Council systems to an external person or body (e.g. in response to a Freedom of Information Request or a Subject Access Request), then ICT Services may access information without the permission or knowledge of users. This could include but is not limited to email accounts or personal areas on network drives.

8.5. Any monitoring process used by the Council will comply with the relevant legislation, including but not limited to the requirements of the Freedom of Information (Scotland) Act 2002, the Data Protection Act 1998 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

9. Actions in Breach of the Acceptable Use Policy

9.1. Suspected breaches of this Policy should be reported to the user's Line Manager, a Senior Officer, Group Leader (Elected Members) or service contact (partners and external organisations) for investigation.

9.2. Under the Council's Disciplinary Procedures (or the relevant disciplinary policy for Teachers where relevant), any Council employee found to be in breach of this Policy may lose access to the ICT Facilities and in addition be subject to disciplinary action, up to and including dismissal. The Council's Disciplinary Procedures are available on the Council's intranet, Renfo.

9.3. If an employee of an external partner or contractor is found to be in breach of this Policy, this should be reported to the relevant employer for the matter to be progressed through their own disciplinary procedures. Any breach in this respect could result in the termination of access to the Council's ICT Facilities or the termination of a contract, depending on the seriousness of the case.

9.4. In relation to Elected Members, a breach of this Policy may lead to the termination of access to ICT Facilities or further action if circumstances warrant it.

9.5. In extreme cases, misuse or unacceptable use of ICT Facilities could be reported to the Police for further investigation.

9.6. If users are in any doubt about what constitutes acceptable or unacceptable use clarification should be sought from their Line Manager or a Senior Officer.

10. Health, Safety and Wellbeing

All ICT equipment must be used with care. Specific guidance is available from ICT Services.

11. Impact Assessment

This Policy has been impact assessed in line with the Council's obligation to comply with the Equality Act 2010 and the Public Sector Equality Duty.

12. Monitoring & Review

This Policy will be reviewed in line with any legislative changes and examples of best practice relating to acceptable use of ICT Facilities and equipment within the workplace and to reflect organisational requirements. In any event, this Policy will be reviewed every 2 years in order to maintain accuracy and relevance.

Part II: Use of ICT Facilities

This Part of the Policy provides a list of common uses of ICT Facilities and sets out the conditions of acceptable use. Please note that this Part II is to provide understanding on the Policy Statement in Part I of this document and is not intended to be exhaustive.

1. Access to ICT Facilities

1.1. A request to gain access to Council ICT Facilities must be made to a Line Manager or Senior Officer in the first instance. Thereafter, the request for access must be made to the ICT Service Desk with evidence of authorisation from a Line Manager/ Senior Officer. Information on how to contact the ICT Service Desk can be found on the Council's intranet, Renfo.

1.2. Access to any of the Council's ICT Facilities will only be granted where there is a demonstrable business need, and access will only be to those facilities which are specifically authorised.

1.3. Access to specific electronic networks or information systems will be based upon the role being performed and permissions will be granted sufficient to enable that role to be fulfilled.

1.4. Any request for amendment to existing access rights must also be made by a Line Manager or Senior Officer. The request must state the business reason and justification for amendment of existing access rights (particularly where the amendment, if implemented, will provide access to information of a more sensitive nature than was previously accessible).

1.5. Requests for access to any information systems by a contractor or external partners must be made by a Line Manager or Senior Officer within the service they are working in. At the time of the request it must be expressly stated that the user is a contractor or an external partner (and there must be an effective contractual agreement in place).

1.6. Any attempt to gain unauthorised access to ICT Facilities or use of Council ICT Facilities to gain unauthorised access to any other information system will be a breach of this Policy and may also be a breach of legislation (including the Computer Misuse Act 1990).

1.7. A Privacy Impact Assessment should be completed if access rights to information systems (regarding personal or sensitive information) changes. Information on the Council's Privacy Impact Assessment procedure is available on Renfo.

2. Supply and Use of ICT Hardware and Software

2.1. Hardware is the physical equipment used in an ICT system. The Council will provide users with equipment to enable access to the Council's electronic networks and information systems. This will include, but is not limited to, a desktop or laptop PC, or equivalent device and associated keyboard, mouse, screen, docking station, disk

drives, printers, encrypted USB pen drives, and mobile devices such as a Blackberry or other approved hand held devices, as appropriate.

2.2. With the exception of portable devices (such as laptops / Blackberrys etc.), equipment should not be disconnected, moved or modified in any way without prior agreement from ICT Services.

2.3. ICT equipment must be disposed of safely and appropriately and should not be disposed of by a user themselves. All users must consult the ICT Service Desk in relation to disposal of ICT equipment.

2.4. Only appropriate information systems (software) required to support business functions and applications will be installed on Council hardware. All such software will be installed by ICT Services. Users must not install, move, or copy software or change any system files. The ICT Service Desk must always be contacted before hardware or software is altered, added or removed.

2.5. No Council owned software may be installed on personally owned equipment without approval from ICT Services.

2.6. All software used on Council ICT equipment must be authorised by ICT Services and acquired legally. This is an individual and Service responsibility. ICT Services will hold and maintain licences for information systems.

2.7. A standard set of productivity tools (including but not limited to Microsoft Office, Lotus Notes etc) are available, chosen to provide a balanced and up-to-date coverage of most business needs. These are continually reviewed to keep up-to-date with advances in technology.

2.8. Users should contact the ICT Service Desk if a business specific information system is needed. ICT Services will ensure that all technical considerations relating to user requirements and to underlying Council information services are addressed.

3. ICT Security

3.1. The security of the Council's ICT Facilities and equipment is essential. ICT security is the responsibility of all users.

3.2. The Council is a Data Controller under the Data Protection Act 1998. Employees should be aware of their responsibilities when processing personal and sensitive data relating to any living individual (including names, addresses and telephone numbers). More detailed advice on managing sensitive and confidential information is contained within the 'Guidance on the Responsible use of Personal Data and Confidential Information' policy which is available on the Council's intranet, Renfo.

3.3. Council owned data should not be extracted from Council's information systems and stored insecurely. Advice on transferring data to other organisations should be sought from ICT Services or the ICT Service Desk. Transfer of data onto portable equipment (such as, but not restricted to corporate USB pens, laptops or memory cards) should only be considered if electronic transfer is not possible and should always be encrypted.

3.4. Where necessary, remote access technologies are available to allow work to be carried out on Council's information systems from home or other locations – this should only be with approval from a Line Manager or Senior Officer and in connection with ICT Services.

3.5. Users should not copy or transfer Council information from or onto personal devices or personal storage.

3.6. Users must also ensure that Council information is not uploaded onto the internet unless there is a clear business reason to do so and there is express agreement from a Line Manager or Senior Officer. Advice on effective and secure transfer of Council information should be sought from the ICT Service Desk or Information Security Officer.

3.7. Users should not leave ICT equipment (including desktop computers, laptop PCs and mobile devices) unattended in such a state as to risk unauthorised access to information. If possible, devices should be locked when unattended or other appropriate security measures taken.

3.8. Users should not connect to the Council's electronic network from a device that has not been provided by the Council (e.g. a device at an Internet cafe or home PC).

3.9. ICT Services are responsible for ensuring that the Council ICT devices have:

3.9.1. an anti-malware product installed and operational and up-to-date signatures;

3.9.2. the firewall turned on; and

3.9.3. an up-to-date operation system that it is configured to automatically update.

3.10. Users should not wilfully uninstall, turn off or reconfigure operating systems on ICT devices. If Users become aware that any or all of the facilities outlined in 3.9 above become inactive, they should contact the ICT Service Desk in order for the device to be disconnected from the network with immediate effect.

3.11. Anything unusual on a device used for Council purposes should be reported to the ICT Service Desk immediately.

3.12. The Council's 'Information Security' policy (available on the Council's intranet, Renfo) provides further guidance on the importance of securing our information and ICT assets against security threats.

4. Password Management

4.1. All ICT users are issued with a unique username and initial password to access ICT Facilities. The user will, on initial log on, create their own password. Under no circumstances is the default password to be used other than to gain initial access.

4.2. Users are responsible for choosing their password with care to avoid easily guessable ones and in accordance with the Council's guidance on Password Security available on the Council's intranet, Renfo.

4.3. Users should never ask to use another person's password or user ID. If access to ICT Facilities is required, users should get authorisation from their Line Manager or Senior

Officer for their own ICT user account to be set up appropriately. If the user has forgotten their own password, the password should be reset by using the password reset tool available on the Council's intranet, Renfo, or the ICT Service Desk should be contacted to request a new one.

4.4. Users must not attempt to gain access to information for any purpose other than that related to work duties.

4.5. Usernames and passwords issued must not be disclosed to any other person, for any reason. Unauthorised use of a password to access information or an information system other than that required to carry out work duties is a serious offence and may result in disciplinary action being taken.

4.6. Any user who is found to have unauthorised access to or shared their username and password which then permits any other person access to any part of the Council's ICT Facilities may have their access rights suspended immediately, while an investigation is conducted as to what has been accessed. Depending upon the outcome of such investigation the user's access rights may be:

4.6.1. Reinstated;

4.6.2. Withdrawn entirely; or

4.6.3. Reinstated but with restrictions.

5. Email

5.1. Email is an important and significant electronic channel of communication within the Council and to communicate with external organisations. Responsible use of the email system is vital to ensure integrity of the Council's processes and procedures, as well as providing assurance to partners and stakeholders that ours and their information is being handled and managed appropriately.

5.2. Use of the Council's email system is restricted to Business Use only. **Personal Use is <u>not</u> permitted at any time.** At no time should employees, Elected Members or any other user of the Council's ICT Facilities use Council email for personal purposes.

5.3. All email activity including traffic into or out of the Council is examined by the email gateways and the content of emails may be intercepted for the purposes of monitoring or keeping records of communications on the Council system. Any email which appears to contain spam, offensive content, or content which could cause damage to Council services will be quarantined until appropriate action can be taken. Genuine business emails will be released on request.

5.4. The Council provides two different email facilities based on the level of sensitivity of information contained in their regular email communication. Those who require email for normal business reasons are provided with an email which has the following format username@renfrewshire.gov.uk. Those who require email to send and receive information of a more sensitive nature are provided with an email address which has the following format, username@renfrewshire.gcsx.gov.uk. Users should note that all secure email communications (the latter email format) may be monitored, not only by

the Council, but by the provider of the secure mail system to ensure the secure and effective operation of government systems and for other lawful purposes. This section 5 applies to the use of email irrespective of which format of email address. Please refer to the Council's Information Security Policy and Email Good Practice Guide (available on the Council's intranet, Renfo) for guidance on the use of these email facilities.

5.5. Sensitive and/ or confidential information should only be sent securely. Where users require to send confidential, sensitive or personal information via email, advice on encryption methods and software should be sought from the ICT Service Desk and the appropriate encryption technique applied.

5.6. Users with email accounts within the Government Connect Secure Extranet (GCSX) environment (i.e. username@renfrewshire.gcsx.gov.uk), may send sensitive and confidential data (this does not include data classified as "Confidential" under the Government Protective Marking Scheme) to another user within GCSX. Usually email accounts which are secure contain the terms 'gcsx' or 'gsi' within the address. Other methods for secure transfer of data may be available, for further information please contact the ICT Service Desk, Information Security Officer or refer to the Information Security Policy (available on the Council's intranet, Renfo).

5.7. The Council operates a system of email filtering, monitoring and logging. The Council reserves the right to access, record or monitor the contents of emails both sent and received via the Council email system for business purposes (including but not limited to in order to ensure that Council business and security procedures are adhered to; to prevent or detect unauthorised use of the Communications systems; to block inappropriate or malicious material sent and received by email; and to access communications where necessary in the event of a user's absence). Reports on patterns of use are routinely issued to Line Managers/ Senior Officers within each Service.

5.8. Users of Education Scotland's GLOW network must be aware that regular monitoring of this system is undertaken by the national providers, independently of the Council. Users should make their own efforts to observe and understand the terms and conditions to the use of GLOW email facilities.

5.9. Any email generated on the Council's email systems is owned by the Council. An email is classified as a Record in line with the Council's Record Management Policy. The Council may be required to provide any information held, which includes the content of emails in response to a legitimate request under the Freedom of Information (Scotland) Act 2002, a Subject Access Request under the Data Protection Act 1998 or an order of the court.

5.10. The Council's email facilities and email through GLOW should not be used to, or appear to, promote, encourage or express any personal or political views/ opinions which may bring the Council into disrepute or harm the Council's reputation or breach any of the Council's other policies. All employees must ensure that the content of their emails is business related and the language used is not discriminatory or defamatory in any way. This includes any emails relating to Trade Union activities and emails to and from Trade Union representatives and their members.

5.11. Under no circumstances should any email be generated and sent or forwarded to any person where the content of that email or any attachment thereto contains defamatory, offensive, abusive, threatening and /or bullying content or content the very nature of which may cause harm or distress. The sending of any such emails will be considered 'gross misconduct' and may result in dismissal in line with the Council's Disciplinary Procedures (or the relevant disciplinary policy for Teachers where relevant). Where the sending of such emails is considered to be criminal the appropriate authorities will be notified, which may result in criminal prosecution. All emails must reflect the high professional standards to which the Council subscribes.

5.12. Technical measures have been introduced in an attempt to block emails with such content; however it is still possible for inappropriate content to be received or indeed sent. Where an email with such content is received this should be reported to a Line Manager or Senior Officer who will take the appropriate action.

5.13. Users should not open suspicious emails. All suspicious emails should be reported to the ICT Service Desk immediately. Similarly, users should not open electronic attachments or follow electronic links if the source of such an attachment/ link is unclear. In such instances, the ICT Service Desk should be contracted for advice.

5.14. If at any time a web site which is accessed for personal reasons asks for an email address to be entered then a personal email address must be used, not a Council email address.

5.15. Users should not send Council data to or from personal email accounts. Advice on effective and secure transfer of Council information should be sought from the ICT Service Desk or Information Security Officer.

5.16. An instant messaging application, 'Sametime', forms part of the Lotus Notes email system. As with Lotus Notes this is provided for Business Use and not Personal Use. 'Sametime' is a useful informal tool for internal communication. Home Workers in particular are encouraged to use 'Sametime' for Business Use to remain in touch with office based colleagues.

6. Internet Usage

6.1. Access to the Internet can be withdrawn at any time should it be apparent that access privileges are being abused.

6.2. Use of the Internet is subject to monitoring controls and regularly reported on to senior management. Users of the Internet, from Council owned, provided or managed devices, should have no expectation that their activity on the Internet will remain private, including when accessing the Internet for Personal Use as the Council's ICT Facilities and all modes of communication are essentially business tools.

6.3. The Council operates a system of website filtering, monitoring and logging, and has blocking software in place. Certain types of site are blocked for security reasons (e.g. web mail and gambling sites) or for bandwidth reasons (e.g. streaming media sites). Access may also be blocked or restricted because of the nature of the content on the site e.g. adult pornography, gambling etc. These measures are in place to protect the individual as much as they are there to protect the corporate network. A full list of

Internet filtering categories and information on those accessible for Personal Use is available on the Council's intranet, Renfo. The fact that a particular site can be accessed does not in itself mean that access is permitted, if the site is not appropriate for a person's business needs. Exceptions are permissible in certain circumstances with authorisation from a Line Manager or Senior Officer and in liaison with ICT Services.

6.4. A record is kept of every Internet site accessed whether the attempt was successful or not. This record shows the originator's user name and PC, date, time and site address of attempted access, whether successful or not. As part of standard monitoring procedures baseline information in the logs can be examined, and any evidence of misuse investigated by a Line Manager or Senior Officer.

6.5. It is the User's responsibility to report any inadvertent access to websites which contain inappropriate material to the ICT Service Desk immediately.

6.6. Users must not attempt to use any tools (for example, Anonymous Proxy tools) to make their Internet activities untraceable.

6.7. If using the Internet for personal purposes you must comply with the terms of Part I: section 7: Use of ICT Facilities for Personal Use of this Policy.

6.8. Software must not be downloaded from the Internet by users without approval from ICT Services and a Line Manager or Senior Officer.

6.9. Users must not use their access to the Internet to carry out their own private business purposes.

6.10. Users should not use the Internet to make negative or defamatory comments about the Council, its agreed decisions or policies, or its officers or Members. Such behaviour could result in disciplinary action in line with the Council's Disciplinary Procedures (or the relevant disciplinary policy for Teachers where relevant) and potentially legal action.

6.11. Employees and users of the Council's ICT Facilities should be aware that many Internet sites keep a record of visitors to the site for marketing purposes and that this record could become public. Employees and other users will need to ensure that they do not visit any sites where such publicity could lead to embarrassment to the Council. If you believe that a colleague is misusing the system, or that your ICT Facilities have been misused, you must contact your Line Manager or Senior Officer in your employing service.

6.12. Users should contact the ICT Service Desk for advice on Internet usage and advice on safe Internet use.

7. Social Media

7.1. Social Media and Social Networking sites are a form of online communication and might include (but is not limited to) Facebook, Twitter, and YouTube. This Policy does not prohibit access to Social Media or Social Networking sites for Business Use (or Personal Use outwith Working Hours), but it should be noted that all use of Social

Media or Social Networking sites should be in accordance with this Policy and separate Council guidelines on Social Media.

7.2. For full guidance on Social Media, please refer to separate and more detailed Council Social Media guidelines which are available on the Council's intranet sites or by request from your Line Manager.

7.3. Guidelines on promotion of Council services via Social Media will be managed by Communications staff. Social Media alerts or pages should not be used for Council business without notifying Communications staff. The Communications team will keep a register of Social Media used for Council business.

7.4. The Council will monitor the use of Social Media and Social Networking sites to ensure that any use complies with this Policy and Social Media specific guidelines.

7.5. Employees and Elected Members should be aware that all communications, including via social media, is subject to control under the relevant codes of conduct and legislation (e.g. on defamation). Social Media should not be used to, or appear to, promote, encourage or express any personal or political views/ opinions which may bring the Council into disrepute or harm the Council's reputation or breach any of the Council's other policies. All officers and Elected Members must ensure that language used is not discriminatory or defamatory in any way.

7.6. Employees should be aware of their association with the Council when using Social Media or Social Networking sites, including professional networking. Employees should ensure that profiles and related content are consistent with how they wish to present themselves to colleagues and professional contacts.

7.7. Employees must not disclose personal, sensitive or confidential information gained during the course of your employment without authorisation, including via social media. Unauthorised disclosure could constitute misconduct/ gross-misconduct in accordance with the Council's Disciplinary Procedures (or the relevant disciplinary policy for Teachers where relevant).

7.8. Any conduct on Social Media or Social Networking sites which breaches Council policies or the Employee Code of Conduct such as failing to show respect at work (including bullying, harassment, victimisation and discrimination), may be subject to disciplinary action in accordance with the Council's Disciplinary Procedures (or the relevant disciplinary policy for Teachers where relevant). Please refer to the Council's Respect at Work Policy which is available on Renfo.

7.9. Using Social Media or Social Networking sites to make negative or defamatory comments about the Council, its agreed decisions or policies, or its officers or Members could also result in disciplinary action in line with the Council's Disciplinary Procedures (or the relevant disciplinary policy for Teachers where relevant) and potentially legal action.

8. Wi-Fi

8.1. Wi-Fi connection to Council-managed devices via Council owned devices is available throughout Renfrewshire House (and some other Council locations) to enable robust access to the Council's electronic network and flexible business operations.

8.2. Wi-Fi connection to internet only is also available on request to users with approval from a Line Manager or Senior Officer (and in liaison with ICT Services).

8.3. Council managed Wi-Fi access is fully managed and monitored by ICT Services.

9. Home Working/ Remote Working

When using Council ICT Facilities to work on Council business away from Council premises, the following rules apply:

9.1. All work related to the business of the Council must be protected. All data of a personal, sensitive or confidential nature should be both password protected and encrypted;

9.2. All work, in particular that where personal or sensitive information is involved, should be carried out in a position where it cannot be seen by others. Accessing Council information in public places should be avoided to reduce the risk of 'shoulder surfing'. Users should be aware of their surroundings when viewing Council information; and

9.3. All reasonable precautions should be taken to safeguard the security of any Council equipment or data regardless of the medium it is stored in to prevent it from theft, loss, destruction or harm (either accidental or malicious).

10. Portable Electronic Devices

10.1. Laptops and other forms of Portable Electronic Devices (including but not limited to mobile communication devices, Personal Digital Assistants (PDAs) and external storage devices etc) are used to help conduct the business of the Council.

10.2. Portable Electronic Devices (PEDs) are the property of Renfrewshire Council and are issued for legitimate Council business purposes only.

10.3. Permission is granted for a mobile device to be used to make a personal call or send a personal text message, providing all Personal Use is identified and paid for (where possible). It is the responsibility of Line Managers and Senior Officer to manage the Personal Use of mobile communication devices. All suspicious or unacceptable usage should be reported to the ICT Service Desk.

10.4. Mobile telephones should only be used for external communications where no fixed alternative telephone line is available or where the use of a fixed line is inappropriate.

10.5. Only Council owned and managed PEDs are permitted to connect to the Council's network, and must not be connected to third party networks or hardware which is not Council managed. This is to ensure that these devices remain free of viruses or other malicious software that may be transmitted on unknown networks. Any modifications or

upgrades to a PED should only be carried out by ICT Services, or with the permission of ICT Services.

10.6. Information collected on PEDs for Council purposes should be transferred to the Council network in a timely manner.

10.7. Using PEDs in public places should be avoided to reduce the risk of 'shoulder surfing'. Users should be aware of their surroundings when viewing Council information.

10.8. All users of PEDs and mobile communication devices are responsible for the security of the equipment itself and for the data which is stored on it. All PEDs and mobile communication devices should be stored securely and appropriate security measures should be taken to ensure that they, or data held on them, are not subject to loss, damage or unauthorised access. When PEDs and mobile communication devices are used outwith Council premises they should be kept as securely as possible and out of view. These should not be left unattended in a public place.

10.9. Users must also ensure that data stored on these devices is held as securely as possible. Data held on such devices should be password protected where possible and, where personal, sensitive or confidential information is stored, encryption should be applied. The ICT Service Desk can provide advice on appropriate encryption methods.

10.10. Any theft, loss of, damage to or unauthorised access of such equipment or data must be reported as soon as reasonably practicable to a Line Manager or Senior Officer and treated initially as an Information Security Incident.

11. Council Telephone Systems

11.1. All telephone and mobile handsets are provided for use in support of the Council's business.

11.2. Where personal calls are made provision exists for these to be recorded as such, and costs recovered. Advice should be sought from a Line Manager or Senior Officer, or ICT Services.

11.3. Employees must not try to use or let anyone else use Council-supplied telephone equipment and particularly not for:

11.3.1. Anything that is illegal;

11.3.2. Making offensive or threatening calls;

11.3.3. Making calls which can be construed to constitute harassment or disparagement of others based on their sex, race, sexual orientation, age, national origin or political beliefs;

11.3.4. Unreasonable Personal Use; or

11.3.5. Use in relation to any other business owned or operated by the employee.

11.4. Precautions should be taken to avoid revealing sensitive or confidential information to those within the immediate vicinity when discussing Council business on a telephone conversation.

11.5. Sensitive and confidential information must never be left as a message on an answer phone. Before discussing sensitive or confidential information with another person their identity and location must be confirmed.

11.6. Telephone usage is subject to routine monitoring and auditing. Content of calls will only be recorded with the explicit knowledge of the user unless this monitoring falls into the terms of the Regulation of Investigatory Powers (Scotland) Act 2000.

11.7. All outgoing telephone calls detailed on telephone bills, unexpected peaks and excessive usage may be investigated in conjunction with the relevant line manager/senior officer.

11.8. Any loss or damage to telephony equipment should be notified to both a Line Manager or Senior Officer and the ICT Service Desk as soon as reasonably practicable.

12. Voicemail

12.1 Voicemail facilities can be set up on Council managed telephone handsets to facilitate Council business. Voice messages are Council records.

12.2 Employees are responsible for maintaining the security of their voicemail. Employees must choose a secure pin code number to reduce the risk of unauthorised access. Unauthorised entry to another employee's voice mailbox is not permitted and may result in disciplinary action.

12.3 Voicemail should normally be checked on a daily basis. Voicemail messages should not be stored for longer than is necessary. Mailbox greeting messages should be kept current, accurate and relevant.

12.4 Shared voicemail accounts may be set up for certain services. It is the responsibility of the manager of any service with a shared mailbox to ensure the management and security of shared mailboxes.

12.5 In order to ensure continuity of service facilities, such as voicemail, may be required to be monitored by a line manager/senior officer or other colleagues, where an employee is absent from the workplace e.g. sickness absence, periods of annual leave etc.

Appendix 1 – Declaration

To be completed by Third Party suppliers and contractors and any other party who, in providing a service to or receiving a service from the Council requires access to the Council's ICT Facilities.

I_____, on behalf of _____ (please provide organisation name if relevant) have read and understood the terms of Renfrewshire Council's ICT Acceptable Use Policy. I agree to abide by the terms of the ICT Acceptable Use Policy.

I understand that any act by me which is considered to be against the terms of this Policy may, at the discretion of Renfrewshire Council, result in the termination of any existing agreement between the parties. I also understand that some breaches of this Policy could constitute a criminal offence.

I agree that if I inadvertently access any Internet site containing unsuitable material, I will report this matter to the ICT Service Desk immediately.

Signature.....

Date of Signature.....