Renfrewshire Council

To: Finance, Resources & Customer Services Policy Board

On: 11 November 2020

Report by: Director of Finance & Resources

Heading: ICT Acceptable Use Policy (AUP)

1. **Summary**

1.1 Renfrewshire Council promotes a culture which recognises the importance of the safe use of ICT facilities. The current ICT AUP needs to be reviewed to reflect the current technology landscape and the Council's current use of ICT facilities. This new policy has been written not only to protect Council electronic assets, data and information but to take account of the current ICT facilities and ensure that best practice is followed. The purpose of this new policy and associated good and bad practice examples is to ensure that individuals are able to make the most of the Council's ICT facilities when carrying out their duties and are fully aware of what is acceptable and what is not acceptable behaviour when using these.

2. **Recommendation**

2.1 It is recommended that the Council approve the new ICT AUP which forms the Appendix to this report and agree that this new policy is reviewed on a two-yearly basis.

3. **Background**

3.1 We live in a world where technology has changed how we deliver services and interact with others. This is a key part of how the Council delivers services, innovates and connects to customers, service users and each other. Given the changing technology landscape, it is essential that the ICT AUP is both up to date and relevant to the Council's current ICT facilities.

3.2 This new policy covers the use of all Council ICT facilities including, but not limited to equipment such as PC's, laptops, tablets, Wi-Fi dongles and smart phones. It also includes the use of the Council's systems and applications including email, instant messaging, video conference services, Microsoft O365 and internet. This policy applies to the use of the Council's ICT facilities regardless of whether they are hosted and used on Council premises, or externally hosted online services, or if they are accessed via the work profile of a personal device such as a smart phone.

3.3 This new policy applies to:

- Council employees including teachers;
- Elected Members;
- External Partners where shared or joint services are provided using Council ICT facilities and
- Contractors, Consultants and Agency Workers i.e. personnel employed by external companies who are granted access to Council ICT facilities.

Implications of the Report

1. **Financial -** none.

2. **HR & Organisational Development -** The ICT AUP will apply to all users of Council ICT facilities and is referenced in the Statement of Particulars.

3. **Community/Council Planning -** N/A.

4. **Legal -** The ICT AUP has been drafted to ensure continued compliance with the Human Rights Act 1998,

5. **Property/Assets -** none.

6. **Information Technology -** ICT are the owners of the ICT AUP and are responsible for its implementation and ongoing reviews. The ICT AUP complies with the requirements of the Public Services Network, thereby safeguarding the position of the Council and individual users of the ICT facilities provided by the Council.

7. **Equality & Human Rights -** The Recommendations contained within this report have been assessed in relation to their impact on equalities and human rights. No negative impacts on equality groups or potential for infringement of individuals' human rights have been identified arising from the recommendations contained in the report. The ICT AUP has been drafted to ensure compliance with The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 and The Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 provide the legal framework to allow the Council to monitor communications insofar as they relate to the business of the Council without breaching the Human Rights Act 1998. If required following implementation, the actual impact of the recommendations and the mitigating actions will be reviewed and monitored, and the results of the assessment will be published on the Council's website.

8. **Health & Safety -** none.

9. **Procurement -** none.

10. **Risk -** none.

11. **Privacy Impact –** The ICT AUP has been drafted to ensure that there is no breach of privacy. The Human Rights Act 1998 obliges all public authorities to act in a manner compatible with the rights contained in the European Convention of Human Rights ("the Convention"). Article 8 of the Convention affords everyone the right to respect for private and family life including home and correspondence. This extends to privacy in the workplace. The AUP complies with both Article 8 and The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. As such, there is no infringement of privacy identified.

12. **Cosla Policy Position -** none.

13. **Climate Risk -** none.

List of Background Papers

N/A

Author: Patrick Murray, Head of ICT, 0141 618 7361

patrick.murray@renfrewshire.gov.uk

INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) ACCEPTABLE USE POLICY

1. Applicability:

1.1 We live in a world where technology has changed how we deliver services and interact with others. Technology is an everyday event for almost everyone in both our work and personal life. Renfrewshire Council is a digital council. This is a key part of how the Council delivers services, innovates and connects to customers, service users and each other.

1.2 Renfrewshire Council promotes a culture which recognises the importance of the safe use of ICT facilities. This policy has been written not only to protect Council electronic assets, data and information but to ensure that best practice is followed. The purpose of this policy and associated good and bad practice examples is to ensure that individuals are able to make the most of the Council's ICT facilities when carrying out their duties and are fully aware of what is acceptable and what is not acceptable behaviour when using these facilities. This policy outlines what is expected from the groups that this policy applies to (see paragraph 1.4) and what to do to make sure everyone is able to comply and understand their responsibilities.

1.3 This policy covers the use of all Council ICT facilities including, but not limited to equipment such as PC's, laptops, tablets, Wi-Fi dongles and smart phones. It also includes the use of the Council's systems and applications including email, instant messaging, video conference services, Microsoft O365 e.g. Sharepoint, OneNote, Yammer or Teams and the internet. This policy applies to the use of the Council's ICT facilities regardless of whether they are hosted and used on Council premises, or externally hosted online services such as Microsoft O365, Eclipse, i-Learn for example, or if they are accessed via the work profile of a personal device such as a smart phone (under any approved Bring Your Own Device program – BYOD).

1.4 This policy applies to:

- Council employees including teachers;
- Elected Members;
- External Partners where shared or joint services are provided using Council ICT facilities and
- Contractors, Consultants and Agency Workers i.e. personnel employed by external companies who are granted access to Council ICT facilities.

1.5 External Partners and Contractors must be made aware of this policy and any relevant guidelines. Appropriate Council ICT facilities access will be provided where necessary to allow work to be carried out as set down by the Council. The use of the Council ICT facilities by External Partners and Contractors for personal use including internet is not permitted for any reason. External Partners and Contractors will be made aware of and asked to agree to this by the Council prior to commencing any work on behalf of the Council which requires them to have access to, or use of, the Council ICT facilities. As part of this awareness, External Partners and Contractors will be required to sign a copy of this policy and agree to its terms.

1.6 Limited personal use of the Council's ICT facilities is permitted for Council staff, as per the terms of this policy. Staff can use the internet for personal use out with normal working hours such as lunch breaks or other unpaid breaks. Please note that personal use of the Council's email system is not permitted at any time.

1.7 Elected Members may use Council ICT facilities, except access to personal emails or personal use of the Councils email system, for incidental personal use. Council ICT facilities must not be used for party political or campaigning purposes at any time. Any misuse may be reported to the Group Leader and could also breach the Councillors' Code of Conduct. Misuse may result in withdrawal of facilities and in the case of suspected criminal activity, referral to the Police.

1.8 When using the Council's ICT facilities, individuals are reminded that the Council has several policies and procedures which detail the standards of conduct and behaviour expected. This policy should be read alongside those which include:

- The Code of Conduct for Employees;
- Disciplinary Procedures and supporting guidance;
- Grievance Procedures and supporting guidance;
- Data Protection Policy;
- Surveillance Policy and Guidelines;
- Use of Social Media Guidance;
- Code of Conduct for Officers on the Acceptable Use of Gifts and Hospitality;
- Expressing Concerns out with Line Management Policy;
- Equality and Diversity Policy;
- Any iLearn cyber security module covering safe use of the Council's ICT facilities;
- Respect at Work Policy;
- Recruitment and Selection Guidance; and
- Business World Use of Personal Devices and Email.

1.9 Technology is an important part of our working lives and is increasingly used to keep our workforce connected and to process and share information both internal and external to the Council. This sharing must be undertaken in a manner that fully protects the rights of individuals and the reputation of the Council. This policy will be reviewed as and when there are changes to legislation, best practice and guidance from specialist bodies. The Council also looks to introduce both new technologies and make changes to existing ones to improve its operation. Therefore, individuals who use Council ICT facilities should always be aware of the latest guidance around best practice and how this applies to them. Updates will be shared on the Council's intranet, by email, and other forms of communication.

1.10 The groups that this policy applies to (see paragraph 1.4) should always use Council ICT facilities responsibly and are reminded of the need to keep Council information secure and confidential. An information or cyber security breach could expose the Council to financial penalties under data protection laws and reputational damage.

1.11 The groups that this policy applies to (see paragraph 1.4) have a personal duty to only ever access the information contained on the Council's ICT network or systems for work purposes. Any misuse of data including but not limited to unauthorised access to personal information or sending offensive emails, could result in disciplinary action and/or in cases of suspected criminal activity, referral to the Police.

1.12 The Council has the right to monitor activity on the Council's ICT facilities including the use of email and the internet for legitimate business purposes to protect against misuse. Suspected misuse of ICT facilities will be investigated and may result in disciplinary action and in the case of suspected criminal activity referral to the Police. This includes any approved Bring Your Own Device solutions made available.

1.13 If the Council is legally required to provide access to information held on Council systems to an individual or organisation (e.g. in response to a Freedom of Information Request or a Subject Access Request), then the ICT service may access information of senders, recipients or those referred to. This could include but is not limited to email accounts, or personal storage on the Council network drives.

1.14 The Council may request access to a personal device that is being utilised for Bring Your Own Device purposes if the Council believes that there is a failure to comply with this policy or it is necessary to respond to requests as explained in 1.13.

1.15 This policy requires every individual to take personal responsibility for protecting data in all its forms – online and offline (as per the policies and procedures listed at 1.8) – and for the safe use of the ICT facilities provided by the Council. It also defines the standard of behaviour and ethos which should be consistent across all electronic forms of communication internally and externally.

1.16 The following sections provide some examples of appropriate and inappropriate use of ICT facilities. It is impossible to provide examples that will cover every possible scenario and should be taken as indicative of good and bad practice. For additional information or clarification, please contact:

- Carol Peters, Cyber Security Architect, carol.peters@renfrewshire.gov.uk
- Phil Feeney, Enterprise Architect, phil.feeney@renfrewshire.gov.uk
- Patrick Murray, Head of ICT, patrick.murray@renfrewshire.gov.uk

INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) ACCEPTABLE USE POLICY

2. When utilising ICT facilities, individuals must:

2.1 Irrespective of what Council communications tool you are using (e.g. email, instant messaging, social media, video conferencing, etc.) only use language which is professional, transparent, consistent and respectful regardless of race, religion or belief, disability, age, sex, gender reassignment, sexual orientation, marriage and civil partnership, pregnancy and maternity, Trade Union membership or activity. A tone of voice guide is available from the Marketing and Communications Service.

2.2 Avoid statements which might facilitate, instigate, promote or support activity associated with actions such as bullying, harassment, racism, offensive or threatening activity, illegal or defamatory actions or otherwise may bring the Council into disrepute or which may be construed as doing so. Bring Your Own Device users should take steps to keep separation between their business and personal use as far as possible.

2.3 Take care to avoid an honest mistake. You may receive dubious emails or land on websites designed to spread a computer virus. If this occurs, then please report it immediately to your line manager and the ICT Service Desk.

2.4 Be alert to possible spam which may contain a computer virus, or fraudulent attempts to provide information etc. (e.g. trying to get you to change bank account details, pay 'outstanding' invoices that do not exist, etc.).

2.5 Treat all e-mail attachments with suspicion especially if there is something unusual, e.g. you don't normally receive that type of request or information, or you do not know the person or organisation that sent the original email (i.e. the sender).

2.6 Send suspected spam, junk or fraudulent email to the corporate 'SPAM' email box so that ICT services can block this in future. (type 'spam' in the TO box of your email)

2.7 Keep passwords private and lock their network account when their ICT equipment such as PC's, laptops, tablets and smart phone are unattended.

2.8 Return Council ICT equipment such as PC's, laptops, tablets, Wi-Fi dongles and smart phones to ICT services if they are no longer being utilised so that they can either be given to another employee or can be securely destroyed. (This excludes equipment issued to staff who are on long term absence)

2.9 Be aware of your surroundings. If you are in a public place, then you are not in a trusted or secure environment and for that reason, should avoid working on, or holding discussions, about anything that is personal or sensitive as people around you may overhear conversations or read what is on your screen (shoulder surfing).

2.10 Use the internet with care. You may come across illegal material such as pornography by accident. If this occurs, do not forward or take copies of material but instead report it immediately to your line manager and the ICT Service Desk.

2.11 Protect Council ICT equipment such as PC's, laptops, tablets, Wi-Fi dongles and smart phones that have been provided to you. This includes ensuring that these are not left behind after meetings, on public transport, etc. If you lose such equipment, please report this as soon as possible.

2.12 Follow the Information Security Incident Reporting Procedure (Appendix A) if Council ICT equipment such as a PC's, laptops, tablets, Wi-Fi dongles or smart phones (including personal devices, where Bring Your Own Device has been approved) are lost or stolen, information is sent to the wrong person or information is lost or stolen.

2.13 Please contact your Line Manager and the ICT Service Desk as soon as possible if you think that you have a computer virus or believe that your network account has been used or accessed without your knowledge or permission.

2.14 Continue to work within the boundaries of Council Policies - as per 1.8 - if you are a Bring Your Own Device user.

2.15 Make sure you undertake training. Take one or more cyber security awareness and training modules applicable to your post and working practices. Modules are on the Council i-Learn section of the Intranet. At a minimum everyone must take the Induction Module (held in the Mandatory section). Thereafter, you are required to update your knowledge annually by taking one or more cyber security modules. This will benefit you in the workplace and at home.

INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) ACCEPTABLE USE POLICY

3. When utilising ICT facilities, individuals must not:

3.1 Use ICT facilities to undertake any activity that may bring the Council into disrepute, lead to someone feeling embarrassed, upset, bullied or be illegal. The type of activity includes, but is not limited to cyber bullying, grooming, stalking, making racist comments etc., and covers online services such as email, instant messaging, social media (including accessing a personal account through a work device), video conferencing etc.

3.2 Access information which is not needed for your job including, but not limited to information relating to friends, family or neighbours who are clients of the council.

3.3 Upload download or access online materials if the content is copyrighted.

3.4 Use another employee's user ID and network password to access ICT facilities, otherwise you may be accused of hacking which is a crime.

3.5 Write down network passwords, or if you feel that you must do so, then keep them in a safe and secure place so that no one else can find them. Do not store network passwords alongside Council ICT equipment such as PCs, laptops, tablets or smart phones.

3.6 Use your own personal device such as a PC, laptop, tablet or smart phone for Council business unless you are adhering to an approved Bring Your Own Device procedure, as you place the Council at significant risk of breaching statutory obligations which can result in a fine and legal action.

3.7 Use your own personal accounts such as email, social media, video conferencing etc to undertake Council business. You must never send Council information to personal accounts such as email or social media etc.

3.8 Save files to an internal disk (also referred to as a hard disk or c:\drive) because these files are not backed up and if the device such as a PC, laptop, tablet or smart phone is lost or damaged, you will lose the data. Data should be saved to the Council network and Council online storage solutions such as O365

3.9 Attempt to alter settings or upload, install or utilise software or apps on Council ICT equipment such as PC's, laptops, tablets, Wi-Fi dongles or smart phones, unless approved by ICT.

3.10 Use unencrypted external memory drives or memory sticks to store Council data.

3.11 Pass any Council ICT device such as PC's, laptops, tablets, Wi-Fi dongles or smart phones from one member of staff to another, even a family member, without consultation with ICT.

3.12 Take photographs of people especially children, without permission. Photographs are personal information and so, are subject to data protection laws. If in doubt, you should contact the Information Governance Team in Legal Services for advice or the Marketing and Communications Service.

Appendix A

Information Security Incident Reporting Procedure for All Staff

Everyone who works for the Council is responsible for the information they handle.

If you think the security of any Council information is or has been compromised, please report this immediately to:

Emma McBride, Senior Solicitor, Information Governance
0141 618 5047

If Emma is not available, please report to:

Allison Black, Data Protection Officer, 0141 618 7175
Andrew Connor, Records Manager 0141 618 5187 or
Donna Cunningham, Information Governance Officer 0141 618 7086

What is Information?

Information means data, documents and records - in both paper and electronic formats.

What is Information Security?

Information Security is not just an ICT issue – it is protecting the confidentiality, integrity and availability of information (including ICT systems) from actual or potential compromise or risk.

We do this through both technical and organisational measures designed to avoid loss of or unauthorised access to or disclosure of information.

Why is Information Security important?

The Council needs information to deliver services. The public and our partners expect the Council to handle their information sensitively and securely. Procedures must be in place to respond when any information held by the Council is lost or compromised.

Information Security is also crucial for the Council's compliance with data protection legislation.

Failure to ensure that information is secure can result in a penalty of up to 20 million Euro by the Office of the Information Commissioner and, of course, significant reputational damage.

What should be reported as an Information Security incident?

Any loss of or compromise to information should be reported as an Information Security Incident. Examples include loss of personal, sensitive personal or commercially sensitive information, in either paper format or stored on a device such as a laptop, information emailed, posted or faxed to the wrong recipient or unauthorised access to files, folders, or systems.

If in doubt, please ask!