To: Finance & Resources Policy Board

On: 24 August 2016

Report by: Director of Finance and Resources

Heading: Information Handling Policy

1 Summary

1.1 The Council recognises that it is sometimes necessary for Council information to be removed from the office for business purposes. The arrangements set out in this Information Handling Policy aim to ensure that the Council is complying with its obligations, as a data controller, under the Data Protection Act 1998 ("DPA"). The DPA regulates the processing of personal data and so, it is important that the Council makes proper provision for the way in which it handles personal data, including when this is removed from Council premises.

1.2 This Policy should be read alongside existing policies which promote best practice when handing information within the office, such as the Data Protection Policy, Information Security Policy and ICT Acceptable Use Policy. It is necessary for additional care to be taken when information is removed from the office to ensure that this is not lost, damaged or stolen. As such, this Policy has been developed to ensure that staff are aware of how to handle information securely when working away from the office, and to promote best practice when information needs to be removed from Council premises.

2 Recommendations

2.1 It is recommended that the Board approve the Information Handling Policy, which forms Appendix 1 to this report, and agree that this be reviewed on a two yearly basis.

---

3 Background

3.1 Working away from the office is now commonplace. The purpose of this Policy is to provide staff with a framework on secure handling of information when working away from the office. This relates to all Council Information accessed away from Council premises; including Information accessible via the Council's network by electronic means as well as paper Information. This Policy covers any circumstances in which Council information (paper and electronic) needs to be removed from Council premises, for example when it is being taken to and from external meetings and extends to all forms of working such as Home Working, Remote Working and Hot Desking.

3.2 The Council is committed to data protection compliance and information security is a significant component of that. The seventh data protection principle sets out that "Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data." A clear Policy and guidance on how to manage Council information when working away from Council premises will help comply with the requirements of the seventh data protection principle and is considered to be good practice by the Information Commissioner's Office.

3.3 This Policy aims to ensure that all Staff and Elected Members accessing Council Information remotely or removing information from Council offices are fully aware of their responsibilities. The control measures will help protect the Council's information against accidental or malicious destruction, damage, modification or disclosure.

Implications of the Report

1. **Financial** – none.

2. **HR & Organisational Development** – none.

3. **Community Planning –** N/A

4. **Legal** – this Policy ensures compliance with the provisions of the Data Protection Act 1998, in particular, the seventh data protection principle on information security.

5. **Property/Assets** – none.

6. **Information Technology** – none.

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. 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** – this Policy supports the management of information risk, such as a potential breach of the Data Protection Act 1998.

11. **Privacy Impact** - none

List of Background Papers

1. Information Handling Policy

Author: *Heather Syme, Senior Solicitor (Information Governance)*
0141 618 7022
heather.syme@renfrewshire.gcsx.gov.uk

Renfrewshire Council

INFORMATION HANDLING POLICY

(v.1)

August 2016

Document Control

Change Record

Version	Date	Author	Reason for Issue/ Change
1.0	May 2016	Heather Syme, Senior Solicitor (Information Governance)	

Document Review and Approval

Name	Action	Date	Communication
Allison Black, Managing Solicitor (Information Governance)	Review	March 2016	Email
Kevin Mullen, ICT Operations Manager	Review	March 2016	Email
Gillian Dickie, ICT Business Services Manager	Review	March 2016	Email
Frances Burns, Project Manager	Review	March 2016	Email
Andrea McMahon, Chief Auditor	Review	March 2016	Email
Raymond Cree, Principal HR Adviser	Review	March 2016	Email
Graham Campbell, Senior Health and Safety Officer	Review	March 2016	Email
Steven Fanning, Senior Health and Safety Officer	Review	March 2016	Email
Information Security Group	Review	March 2016	Email

Related Documents

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

Title	Information Handling Policy
Author	Heather Syme, Senior Solicitor (Information Governance)
Issue Date	August 2016
Subject	
Description	
Version	V1
Source	
Updating Frequency	2-yearly
Right	Not Protectively Marked
Category	
Identifier	

Contents

Scope

This Information Handling Policy sets out the requirements relating to the handling of information, in particular the transfer of information when moving information from or working away from the office. Care must be taken with information when doing so to protect against breaches of confidentiality, loss of integrity, interruption to availability, and non-compliance with legislation which would otherwise occur.

This policy describes the principles of securely handling information and how Staff and Elected Members can make informed decisions on how best to protect it.

This policy applies to all Services, employees and Elected Members of Renfrewshire Council and its Joint Committees. It should, however, be read alongside other Council policies and guidelines on wider issues relating to secure handling and secure transfer of information.

There are many ways of working, other than the 'traditional' office-based scenario from a desktop personal computer. This Policy will apply to all forms of working, such as Home Working, Remote Working and Hot Desking, but this Policy also extends to any circumstances where Information (paper and electronic) needs to be removed from the Council premises, for example transporting Information to and from external meetings.

The provisions of this Policy therefore apply to any person moving information from or working away from the office in any capacity.

1. Purpose

1.1. This Policy applies to any form of movement of Information. This means all Council Information accessed away from Council premises; including Information accessible via the Council's network/ electronic means as well as paper based Information. This Policy covers any circumstances in which Council information (paper and electronic) needs to be removed from Council premises, for example when it is being taken to and from external meetings and extends to all forms of working such as Home Working, Remote Working and Hot Desking.

1.2. This Policy aims to ensure that all Staff and Elected Members accessing Council Information remotely are fully aware of their responsibilities. The Council's Information is fundamental to the Council's business and stakeholders. As such, appropriate levels of information security must be implemented and maintained. It is the purpose of this Policy to ensure that Staff and Elected Members are aware of and adhere to relevant control measures to protect the Council's

Information against accidental or malicious destruction, damage, modification or disclosure, and to maintain appropriate levels of confidentiality, integrity and availability of this.

1.3. The following principles underpin this Policy:

- Personal data must be kept secure;
- The Council's ICT Facilities must remain secure;
- The Council's ICT Facilities are primarily for Business Use and for other approved purposes set out in the ICT Acceptable Use Policy and any associated policies or guidelines or as agreed with a Line Manager/ Senior Officer; and
- Inappropriate, unlawful or unauthorised activity is not permitted.

2. Introduction

2.1. Working away from the office can include both the use of mobile electronic devices and also the removal of paper Information from Council premises. The Council needs to consider the unique information security challenges and risks which will necessarily result from this way of working.

2.2. The aim of this **Policy** is to protect the confidentiality, integrity and availability of the Council's Information (whether paper or electronic) when this is moved from the office.

2.3. 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. It is also vital that Information held by the Council is not exposed to unnecessary risk.

2.4. The use of ICT all ICT Facilities regardless of whether it is used on Council premises or elsewhere is governed by the ICT Acceptable Use Policy. This Policy operates alongside the ICT Acceptable Use Policy and extends beyond use of equipment to the handling of all information, regardless of format.

2.5. This policy can be read alongside a number of other relevant Council policies, procedures and guidance, which Staff and Elected Members should be aware of, including but not limited to:

- Code of Conduct for Employees;
- Data Protection Policy;
- Guidelines on the use of Mobile Devices;

- ICT Acceptable Use Policy;
- Information Security Policy;
- Records Management Policy;
- Quick Start Remote Working User Guide;
- Use of Council Resources Policy; and
- Social Media Guidance

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

2.6. All Staff and Elected Members should read this Policy carefully in order to understand its terms.

2.7. Any queries in respect of this Policy should be referred to a Line Manager, Senior Officer or the Information Governance Team.

2.8. Any information security incidents should be reported immediately to the Senior Solicitor (Information Governance), in line with the Council's Information Security Incident Reporting procedures.

3. 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;

Information means data, documents and records covering the information lifecycle from their creation to their disposal, in both paper and electronic formats;

Personal Use means all use other than Business Use; and

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

4. General Provisions

4.1. Staff and Elected Members should consider whether Information can be transferred by secure e-mail rather than transferring paper Information outside of the office.

4.2. Staff and Elected Members must ensure that there is no unauthorised access to the Council's Information.

4.3. All Council Information being used at a remote location must be securely stored and not displayed in a manner which allows its content to be viewed by anyone else.

4.4. 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'. Staff and Elected Members should be aware of their surroundings when viewing Council Information to ensure that Council Information remains confidential and secure. Staff and Elected Members must ensure that any information is, insofar as possible, not visible by anyone else.

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

4.6. All security incidents, including actual or potential unauthorised access to Council Information, should be reported immediately to the Information Governance Team, in line with the Information Security Incident Reporting Procedures. Near misses and possible weaknesses should also be reported through this same method.

4.7. Any loss of a mobile device should be reported to the ICT Service Desk.

5. Information Security

5.1. The security of the Council's Information and ICT equipment is essential. Information security is the responsibility of all Staff and Elected Members.

5.2. The Council is a Data Controller under the Data Protection Act 1998.

5.3. 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.

5.4. All Staff and Elected Members are responsible for the security of the ICT equipment itself and for the data which is stored on it. All Information and devices should be stored securely at all times, when not in use, 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 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.

5.5. Staff and Elected Members 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.

5.6. Council Information should not be extracted from Council's Information systems and stored insecurely. This includes e-mailing Information to a personal or other insecure device, even for work purposes. Advice on electronic transfer of data should be sought from the ICT Service Desk.

5.7. Staff and Elected Members should not leave Information (including papers, laptop PCs and mobile devices) unattended in such a state as to risk unauthorised access to Information. If possible, Information should be locked when unattended or other appropriate security measures taken. Staff and elected members must take particular care when they have decided to take council information away from a secure location to avoid the information being misplaced or lost.

5.8. The Council's 'Information Security' policy (available on the Council's intranet, Renfo) provides further guidance on the importance of securing the Council's Information.

6. Actions in Breach of the Information Handling Policy

6.1. Suspected breaches of this Policy should be reported to the appropriate Line Manager, a Senior Officer or Group Leader (Elected Members) for investigation.

6.2. If Staff or Elected Members are in any doubt about what constitutes acceptable or unacceptable use clarification should be sought from their Line Manager, a Senior Officer or the Information Governance team.

6.3. 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.

7. 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

8. Monitoring & Review

This Policy will be reviewed in line with any legislative changes and examples of best practice relating to information handling and to reflect organisational requirements. In any event, this Policy will be reviewed every 2 years in order to maintain accuracy and relevance.

Appendix 1: Think Twice note on Working from Home

THINK TWICE!
Information Security: working from home

Handling personal information with care and respect is critical. Care should be taken not to lose or misplace information. This is everyone's responsibility.

It is crucial that all Council information, both electronic and paper, is treated with care to ensure that it is kept secure. Everyone who works for the Council is responsible for the information they handle at work – both in the office and outwith the office.

From time to time, you may need to remove confidential information from the office to work from home or to other non-Council premises. You must take care to protect the confidentiality of papers, files and documents, including those stored electronically.

Keeping information secure:

- Keep information and equipment locked out of sight during transport. If you are transporting information or equipment by car, lock it in the boot. Do not leave documents and equipment overnight in the car boot.
- Ensure information is not seen by other members of your household, visitors or other unauthorised people.
- Use only Council-supplied devices for storing Council information. Do not store confidential Council information on your personal equipment.
- Ensure all Council equipment, documents and materials are used solely for Council purposes. They remain the property of the Council and members of the household or other unauthorised people must not be allowed to use them.
- Use only your Council email account for sending or receiving emails related to Council business. Your personal email account or other email accounts must not be used for this purpose.
- Never carry personal information on unencrypted electronic media.
- Keep Council information and equipment locked away when unattended - they must not be accessible to unauthorised people.
- Keep confidential Council records at home for as little time as possible. Return them to their normal filing location in the office as soon as possible.
- Dispose of Council information only on Council premises, in line with confidential waste procedures.

It is important that personal information is properly protected and not left unattended. A careless mistake can have huge consequences for both the Council and its service users, so please THINK TWICE when you're handling personal information.

Report any information security incident to your Service Data Protection Officer, Line Manager or the Senior Solicitor (Information Governance) as soon as possible, in line with the Council's information security incident reporting procedure. It is important that you do this as soon as possible, so that steps can be taken to rectify this.

Full guidance is available on the Information Governance section of Renfo and the Information Governance team can provide advice at any time.

Key Contact - **Heather Syme,** Senior Solicitor (Information Governance),
heather.syme@renfrewshire.gcsx.gov.uk
0141 618 7022

Appendix 2: Information Security Incident Reporting Procedure for All Staff

Information Security Incident Reporting Procedure for All Staff

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

What is Information?

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

What is Information Security?

Information Security is protecting the confidentiality, integrity and availability of our information (including ICT systems) from actual or potential compromise or risk.

We do this through both technical and organisational measures designed to minimise the risk of loss, unauthorised access to or disclosure of such 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 various pieces of legislation, for example, e.g. the Data Protection Act 1998, the Privacy and Electronic Communications (EC Directive) Regulations 2003, as amended, and the Freedom of information (Scotland) Act 2002.

Failure to ensure that information is secure can result in a penalty of up to £500,000 by the Office of the Information Commissioner and, of course, significant reputational damage.

What should be reported as an Information Security incident?

Any loss 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, USB pen, CD, DVD, emailed to the wrong recipient, unauthorised access to files, folders, or systems. If in doubt, please ask.

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

Heather Syme, Senior Solicitor (Information Governance)
Email: heather.syme@renfrewshire.gcsx.gov.uk Tel: 0141 618 7022