Renfrewshire
Council

To: **Finance, Resources and Customer Services Policy Board**

On: **5 June 2019**

Report by: **Director of Finance and Resources**

Subject: **Review of Information Handling Policy**

1. Summary

1.1 The Council's Information Handling Policy was approved by the Finance and Resources Policy Board in August 2016. The purpose of this Policy is to ensure that the Council is complying with its data protection obligations in relation to its handling of personal information, particularly information which needs to be removed from the office for business purposes. 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 was developed to ensure that staff and Elected Members 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.

1.2 The Policy is subject to routine review. The revisals are minor and simply reflect the current Council structure and updated statutory references, with additional references to associated guidance.

1.3 The Council’s Information Security Group meets quarterly and is chaired by the Chief Auditor. There is representation from Legal Services and ICT and the Council’s statutory Data Protection Officer is also a member. The purpose of the Group is to ensure best information security practice within the Council, including the review of relevant policies, procedures and guidance. The Information Security Group have authority to review the Council’s Information Security Policy to maintain accuracy and relevance.

2. Recommendation

It is recommended that the Board:-

2.1 Approve the revised Information Handling Policy, which forms Appendix 1 to this report, and

2.2 Delegate authority to the Managing Solicitor (Data Protection Officer), in consultation with the Information Security Group to approve further reviews on a two yearly basis.

3 Background

3.1 The revised Policy continues 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 any electronic means as well as paper Information. It 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, including but not limited to Home Working, Remote Working and Hot Desking.

3.3 The aim of the revised Policy continues to be 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 revisals are minor and simply reflect current statutory references and Council structures, with additional signposting to associated guidelines.

Implications of the Report

1. **Financial -** None

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

3. **Community/Council Planning –** None

4. **Legal** - the revised Policy continues to ensure compliance with the Council's data protection obligations, in particular, those which relate to information security.

5. **Property/Assets -** None

6. **Information Technology –** None

7. **Equality & Human Rights** -

   (a) 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 because it is to ensure that Council information is kept adequately secure when removed from Council premises for business purposes. 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-** The revised Policy continues to support the management of information risk, such as a potential information security breach.

11. **Privacy Impact –** No Data Protection Impact Assessment (DPIA) is required as the Policy and revisals protect privacy.

12. **Cosla Policy Position –** Not applicable

List of Background Papers

(a) Background Papers - None

Author Allison Black, Managing Solicitor (DPO), extension 7175

Renfrewshire Council

INFORMATION HANDLING POLICY

(v.2.0)

June 2019

Document Control

Change Record

Version	Date	Author	Reason for Issue/ Change
1.0	August 2016	Heather Syme, Senior Solicitor (Information Governance)	
2.0	February 2019	Allison Black	

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
Information Security Group	Review	February 2019	Email and discussion

Related Documents

Ref	Document Name/ Version	Document Location
1	Information & Communications Technologies (ICT) Acceptable Use Policy	Intranet
2		
3		

Title	Information Handling Policy
Author	Allison Black (DPO)
Issue Date	June 2019
Subject	
Description	
Version	V2
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 working away from the office. Care must be taken with information when moving it or accessing this remotely to protect against breaches of confidentiality, loss of integrity, interruption to availability, and non-compliance with legislation.

This Policy outlines principles for securely handling information for Staff and Elected Members. It applies to all Services, employees and Elected Members of Renfrewshire Council and its Joint Committees who move Information or work away from the office in any capacity.

There are many flexible ways of working, in addition to the ‘traditional’ office-based work from a desktop personal computer. This Policy applies to all forms of working, including but not limited to Home Working, Remote Working and Hot Desking, but it also extends to any circumstances where Information (paper and electronic) needs to be accessed remotely or removed from Council premises, for example transporting Information to and from external meetings.

It should, be read alongside other Council policies and guidelines on wider issues relating to data protection, secure handling and secure transfer of Information.

1. Purpose

1.1. This Policy applies to any Council Information removed from the office or accessed remotely including Information accessible via the Council’s network or by any electronic means, as well as paper-based Information.

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. Staff and Elected Members 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.

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;

Data Protection Laws means the EU General Data Protection Regulation (GDPR), the Data Protection Act 2018 and any enactments thereunder or amendments thereto, the Privacy and Electronic Communications Regulation 2003 (PECR) and any legislation enacted that, in respect of the United Kingdom, replaces, or enacts into domestic law, GDPR or any other law relating to data protection, the Processing of personal data and privacy as a consequence of the United Kingdom leaving the European Union.

ICT Facilities means all facilities, approved devices**,** 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, regardless of how these are remotely accessed;

Personal Use means all use other than Business Use;

Special Category Data means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition, sexual life or genetic or biometric data.

3. Introduction

Working away from the office can include both the use of various electronic devices and 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.

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.

3.1 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.

3.2 The use of all ICT Facilities regardless of whether it is used on Council premises or elsewhere is governed by the ICT Acceptable Use Policy (AUP) ICT-Acceptable-Use-Policy-2014

This Policy operates alongside the ICT Acceptable Use Policy and extends beyond use of equipment to the handling of all Information, regardless of format.

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 Code-of-Conduct-for-all-Employees-2018;
- Data Protection Policy Data-protection-policy;
- Information Security Policy Information-Security-Policy;
- Records Management Policy Records-Management-Policy and
- Social Media Guidance Social-Media-Guidance-and-Guidelines

These documents are also available on the Council's intranet.

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

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

4. General Provisions

4.1. Staff and Elected Members should consider whether Information can be transferred more securely by electronic means than by transferring paper Information outside of the office. The Information Management Practical Advice document provides guidelines on available approved, secure ways to share information with internal and external stakeholders.

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, 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 or via unsecure networks should be avoided to reduce the risk of 'shoulder surfing'. Further guidance can be found in the Using Unsecured Public Wifi Networks document. 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 one of the Senior Solicitors in the Information Governance Team, in line with the Information Security Incident Reporting Procedures [INSERT LINK]. 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 the ICT equipment used to process this is essential. Information security is the responsibility of all Staff and Elected Members.

5.2. The Council is a Controller under Data Protection Laws.

5.3. Employees should be aware of their responsibilities when processing personal and Special Category 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.

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, particularly 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 or a vehicle.

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 Cyber Security Architect and Cyber Security Officer within the ICT Enterprise Architecture Team can provide advice on appropriate encryption methods.

Council Information should not be extracted from Council's Information systems and stored insecurely. This includes e-mailing Information to an unauthorised or other insecure device, even for work purposes and ensuring that sharing information online is only done through approved/secure platforms.

5.6. Advice on electronic transfer of data should be sought from the Cyber Security Architect or Officer.

5.7. Staff and Elected Members should not leave Information or ICT Facilities unattended in such a state as to risk unauthorised access to Information. If possible, Information should be locked away 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 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, the Information Governance Team or for Elected Members, the Group Leader 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, or the Information Governance team.

6.3. Where 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 by the Managing Solicitor (DPO) in consultation with the Information Security Group in line with any legislative or technological changes 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 - 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.
- Where possible use existing tools provided on Council equipment for sharing information electronically. See the Information Management Practical Advice document for further details. If you are unsure as to the best option speak to the Cyber Security Architect or Officer.
- Ensure information is not seen by other members of your household, visitors or other unauthorised people.
- Use only approved devices for storing Council information.
- Use only your Council email account for sending or receiving emails related to Council business.
- 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.
- 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 one of the Senior Solicitors (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 Contacts: -

Nina Hill, Senior Solicitor (Information Governance),
nina.hill@renfrewshire. gov.uk
0141 618 6702

Mark Conroy, Senior Solicitor (Information Governance)
mark.conroy@renfrewshire.gov.uk
0141 618 6707

Appendix 2: 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 EU General Data Protection Regulation, the Data Protection Act 2018 and any amendments, 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 significant fine 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:

Nina Hill, Senior Solicitor (Information Governance)
Email: nina.hill@renfrewshire..gov.uk Tel: 0141 618 6702

Mark Conroy, Senior Solicitor (Information Governance)
Email:mark.conroy@renfrewshire.gov,uk Tel: 0141 618 6707