RENFREWSHIRE VALUATION JOINT BOARD

INFORMATION HANDLING POLICY

IG10

Title	Information Handling Policy
Author	Assistant Assessor
Approved By	Management Team
Date of Approval	June 2020
Reviewer	Assistant Assessor
Review Date	As required

Review History

Review No.	Details	Release Date
1	Review by Data Protection Officer	2 February 2021
2	Review	9 February 2023

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 can make informed decisions on how best to protect it.

This policy applies to all employees. It should, however, be read alongside other RVJB policies and guidelines on wider issues relating to secure handling and secure transfer of information, in particular the **Data Protection Policy** and **Information Security Policy**.

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 and Remote Working, but this Policy also extends to any circumstances where Information (paper and electronic) needs to be removed from RVJB 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 RVJB Information accessed away from RVJB premises; including Information accessible via RVJB's network/ electronic means as well as paper-based Information. This Policy covers any circumstances in which RVJB information (paper and electronic) needs to be removed from RVJB premises, for example when it is being taken to and from external meetings and extends to all forms of working such as Home Working and Remote Working.

1.2 This Policy aims to ensure that all Staff accessing RVJB Information remotely are fully aware of their responsibilities. RVJB's Information is fundamental to RVJB'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 are aware of and adhere to relevant control measures to protect RVJB'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;
- RVJB's ICT Facilities must remain secure;
- RVJB's ICT Facilities are primarily for Business Use and for other approved purposes set out in the Information Technology Acceptable Use Policy and any associated policies or guidelines or as agreed with a Line Manager/ Senior Management Team; 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 RVJB premises. RVJB 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 RVJB's Information (whether paper or electronic) when this is moved from the office.

2.3 RVJB is obliged to ensure that appropriate operational, technical and organisational measures have been introduced to ensure RVJB Information and its associated infrastructure is protected against damage and risk. It is also vital that Information held by RVJB is not exposed to unnecessary risk.

2.4 The use of all ICT Facilities regardless of whether it is used on RVJB premises or elsewhere is governed by the Information Technology Acceptable Use Policy. This Policy operates alongside the Information Technology 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 RVJB policies, procedures and guidance, which Staff should be aware of, including but not limited to:

- Code of Conduct for Employees;
- Data Protection Policy;
- Information Technology Acceptable Use Policy; and
- Information Security Policy.

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

2.7 Any queries in respect of this Policy should be referred to the Assistant Assessor for Governance.

2.8 Any information security incidents should be reported immediately to the Assistant Assessor for Governance in line with RVJB's Information Security Incident Reporting procedures (see Appendix 2)

3. Definitions

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

Business Use means all use which is related to RVJB 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;

4. General Provisions

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

4.2 Staff must ensure that there is no unauthorised access to RVJB's Information.

4.3 All RVJB 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 RVJB Information in public places should be avoided to reduce the risk of 'shoulder surfing'. Staff should be aware of their surroundings when viewing RVJB Information to ensure that RVJB Information remains confidential and secure. Staff 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 RVJB 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 RVJB Information, should be reported immediately to the Assistant Assessor for Governance or another member of the Senior Management 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 RVJB equipment should be reported to the Assistant Assessor for Governance or another member of the Senior Management Team.

4.8 Advice on information handling, information security and data protection can be sought at any time from RVJB's Data Protection Officer.

5. Information Security

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

5.2 All Staff 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 pc or mobile communication devices are used out with RVJB premises they should be kept as securely as possible and out of view. Mobile communication devices should not be left unattended in a public place.

5.3 Staff 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.

5.4 RVJB Information should not be extracted from RVJB's Information systems and stored insecurely. RVJB Information must never be stored on a personally owned

device. This includes e-mailing Information to a personal or other insecure device, even for work purposes.

5.5 Staff should not leave Information (including papers, PCs, 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 must take particular care when they have decided to take RVJB information away from a secure location to avoid the information being misplaced or lost.

5.6 Disposal of Information must be done in a secure way. Paper-based Information must be shredded or disposed of in the Confidential Waste bags provided in the RVJB offices. Staff should liaise with RVJB's ICT team when disposing of electronic Information to ensure it is securely and irretrievably deleted, or otherwise rendered inaccessible.

5.7 Any transfer of Information to a third party must be done as securely as possible. The authenticity and validity of the recipient must be verified before transferring any Information.

5.8 RVJB's Information Security Policy provides further guidance on the importance of securing RVJB'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 for investigation.

6.2 Breach of this Policy may be regarded as a serious act of misconduct and may lead to disciplinary action.

6.3 If Staff are in any doubt about what constitutes acceptable or unacceptable use clarification should be sought from the Assistant Assessor for Governance or another member of the Senior Management Team.

6.4 Where any activity is discovered and the conduct is considered to be of a criminal nature, RVJB reserves the right to report the circumstances to the police for further investigation.

7. 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

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

From time to time, you may need to remove confidential information from the office to work from home or to other 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 RVJB-supplied devices for storing RVJB information. Do not store confidential RVJB information on your personal equipment.
- Ensure all RVJB equipment, documents and materials are used solely for RVJB purposes. They remain the property of RVJB and members of the household or other unauthorised people must not be allowed to use them.
- Use only your RVJB email account for sending or receiving emails related to RVJB 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 RVJB information and equipment locked away when unattended - they must not be accessible to unauthorised people.
- Keep confidential RVJB 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 RVJB information only on RVJB 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 RVJB and its service users, so please THINK TWICE when you're handling personal information.

Report any information security incident to the Assistant Assessor & Electoral Registration Officer as soon as possible, in line with RVJB'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.

Key Contact – Lindsey Hendry, Lindsey.Hendry@renfrewshire-vjb.gov.uk

Appendix 2: Information Security Incident Reporting Procedure for All Staff

INFORMATION SECURITY

INCIDENT REPORTING PROCEDURE FOR ALL STAFF

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

Lindsey Hendry
Assistant Assessor responsible for Governance
Lindsey.Hendry@renfrewshire-vjb.gov.uk
T: 0141 487 0635 | M: 07483 921 235

Everyone who works for RVJB is responsible for keeping information secure. This means all data, documents and records - in both paper and electronic formats.

The law requires us to have both technical and organisational measures to avoid loss of or unauthorised access to or disclosure of information.

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

Why is Information Security important?

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

Information Security is also crucial for RVJB'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 MUST be reported as an Information Security Incident.

Examples include loss of personal, sensitive personal or commercially sensitive information. This can be in either paper format or stored on a device such as a laptop, USB pen, CD, DVD. An incident can also be where information is emailed, posted or faxed to the wrong recipient or if there has been unauthorised access to files, folders, or systems.

Even if in doubt, please always contact Lindsey Hendry, immediately.