Information Management & Handling Policy

1. Introduction

1.1 Information is critical to the effective and efficient delivery of services by East Renfrewshire Council to its customers and staff. In order to ensure that the Council can have confidence in its information, and that it will be available when it is needed, information must be managed and handled securely.

1.2 This Policy supports the Council's commitment to information security and provides the strategic approach for the secure management and handling of East Renfrewshire Council information.

1.3 Within this policy the term 'information' covers information systems and physical assets, including supporting processes, systems, networks, equipment, and hardcopy documentation. It can be written (e.g., letters, faxes, notes), electronic (e.g., email, word document or excel spreadsheet), verbal (e.g., when at a meeting or holding phone discussions) or images (e.g., photographs, video or CCTV). The term 'Customer' is used to denote personal information about clients, members of the public and staff.

2. Purpose

2.1 This Policy sets the foundation and provides the framework for secure information handling which is appropriate, cost effective, and pragmatic, and enables East Renfrewshire Council operations and service delivery.

2.2 The key objectives of this Policy are to:

- Provide the framework for procedures and guidance relating to information management, classification and handling.
- Ensure that all East Renfrewshire Council information, particularly personal and customer information, is treated securely and appropriately at all times.
- Ensure that all information collection, processing and sharing activities are identified and formally managed.
- Protect staff in the event a third party instigates criminal proceedings relating to loss or mishandling of personal data against them as an individual

3. Information Management

3.1 East Renfrewshire Council information must be managed and handled appropriately and securely at all times. All Council employees, Elected Members, and individuals with access to Council information, have an individual personal responsibility to ensure that information is protected and handled appropriately.

3.2 Access to all information must be restricted to those individuals who have a business need to do so.

3.3 Personal information must only be collected, processed, and/or shared where there is a legal justification or where it is in the interest of the customer (or staff) and is done with consent.

3.4 All information must be allocated an Information Asset Owner who is responsible for deciding how, when and why information is collected, processed, shared, retained, and destroyed. Information Asset Owners must be a senior manager. The role is about managing information, not systems, with the aim of providing a common, consistent and

unambiguous understanding of what information is held, how important, sensitive and accurate it is, how reliant you are on it, and who's responsible for it and helps ensure that you can use the information you need to operate transparently and accountably.

3.5 Information Asset Owners must identify all information, within their area of responsibility, and ensure that it is recorded in the Council Information Asset Register. They must also identify which information needs to be classified OFFICIAL-SENSITIVE.

3.6 East Renfrewshire Council will ensure that suitable information sharing agreements and protocols exist to enable information sharing, both within the Council and with external organisations, to be undertaken securely and appropriately.

4. Information Handling

4.1 Information handling standards have been developed to ensure that all East Renfrewshire Council staff know how to handle Council information appropriately. These standards are detailed within the Information Classification Procedure and the Acceptable use Policy and its framework and cover:

- Electronic and Hardcopy information.
- Access to information, including confidentiality, integrity, and availability.
- Use of mobile devices, including laptops, smart phones, CDroms and memory sticks.
- The encryption of information.
- Information sharing.
- Taking and working with information out of the office
- The Information Asset Register.
- Information classification.
- Information storage, retention and disposal.
- Dealing with the loss or theft of information or information storage devices.
- Transfer of files between the network and removable media
- Security within procurement

5. Compliance

5.1 East Renfrewshire Council employees, Elected Members, and individuals who have access to Council information, must adhere to the requirements of this policy and all associated information security policies and procedures.

5.2 Staff with access to Personal and Council operationally sensitive information must complete at least one information security related course per financial year.

5.3 Non compliance with this Policy will be subject to investigation and may lead to disciplinary action.

5.4 This Policy has been written to comply with Data Protection laws, the HMG Security Policy Framework and the Scottish Government Identity Management and Privacy Principles.

5.5 The Council monitors use of ICT facilities which can include the movement of electronic files within and off the network. Reports of such usage can be provided to relevant parties as part of normal working practise or during investigations into misuse.