INFORMATION HANDLING POLICY

Version Control

Version	Description	Release Date	Issued By
1.00	Final Version	December 10	Information Security Officer

1. Introduction

1.1 Total security of information is impossible, particularly when it is removed from the office. However there are things that can be done to significantly reduce the risk of a compromise. Some actions utilise modern technology others are simply down to each individual applying common sense and taking sensible precautions.

1.2 Protection has to be proportionate. Impact of a compromise can range from catastrophic to an individual (eg., sex offender details becoming public) to nothing more than a minor inconvenience (eg., name and address). The question is, how can staff distinguish between these extremes and handle information in an appropriate and secure manner.

1.3 This policy describes the principles of securely handling information and how staff can make informed decisions on how best to protect it. The principles apply to all types of information to ensure that even operationally sensitive details are not accidentally compromised and at all times when information is removed from the office including regular, occasional, ad-hoc, remote or home working. Failure to apply it to personal information may breach the Data Protection Act.

1.4 For clarity, the term 'Information' refers to any individual or collection of data relating to council operations, staff or customers (for example budget details, minutes of meetings, policies and procedures, continuity plans, sickness records, holiday requests, staff appraisal notes, customer files or details of payments made or due)

1.5 The policy has been written to comply with the Data Protection Act 1998 (DPA), the HMG Security Policy Framework and the Scottish Governments Identity Management and Privacy Principles (draft 1 November 2009).

2. Policy

2.1 All information must be allocated an Information Owner, who is responsible for the strategic decision making on how, when and why information is collected, processed, shared, retained, destroyed and secured. Due to the potential legal implications in the event of compromise or weak security practices, this role must be filled at a senior level, typically Director. Day to day application or enforcement of the policy is normally delegated to those responsible for the staff who deliver a service, typically Head of Service or Section Manager.

2.2 Information Owners are responsible for:

a. ensuring that the information they are responsible for is adequately secure.

b. designating all information with a security classification level in line with the councils classification guidelines. When communicated to others the classification guides staff on how those records are to be handled in different situations and decreases the potential for accidental compromise.

c. Ensuring that staff understand how to handle information in line with the instructions given within the classification level chosen for a record.

d. ensuring that details of the information collection and processing is recorded in the ERC Information Asset Register (via the ISO)

e. ensuring personal information is only collected, used or shared where a legal justification exists or, where it is in the interest of the customer and is with consent or, a legal over-ride to consent exists.

f. Ensuring that access to personal or operationally sensitive information is restricted to only those who have an operational need to know. This may involve separating some kinds of files eg., Personnel sickness records from the basic personnel record to ensure only those who need to see the sickness record detail has access to that part of the record.

g. ensuring staff only share personal information with 3rd parties if the practice has been risk assessed and an Information Handling Protocol (sometimes also called a Sharing Agreement), developed and approved by the ERC ISO (with the exception of where a legal exception has been proven eg., court order). This obligation should be part of the contract between parties.

h. restricting removal of personal information from the office to by exception only.

i. ensuring that where removal of information is approved, the how and where it will be taken and used is risk assessed, confirming that there is a business reason why removal is appropriate, and identifying the additional security measures that the individual is to take and that these are communicated to the member of staff.

j. Communicating handling instructions to staff, including that whilst information is in their possession away from the office, they are individually responsible for ensuring they follow these additional security measures and protect the information while it is out of the office. the DPA, may be considered personally culpable in the event that the information is compromised.

k. ensuring that any member of staff authorised to take information out of the office has attended an ISO run Information Security Workshop.

l. restricting use of removable and mobile media and ensuring that where it is approved, it is risk assessed first to confirm there is a business reason for its use, and identifying any additional security measures that the individual using it must take and that these are communicated to all appropriate staff. Removable media commonly refers to things such as Cdroms and USB memory sticks, mobile media is items such as laptops. Both also refer to modern mobile phones, i-pods, mp3 players etc., which are all capable of storing information on them.

m. notifying staff that loss or theft of removable media or other form of compromise of information taken out of the office must be reported immediately to a Line Manager who in turn must report it immediately to the ISO and Legal Data Protection Officer (a compromise includes if an unauthorised person has been able to read personal details over your shoulder).

2.3 All removable and mobile media carrying personal information must be encrypted using the Council's authorised encryption solution irrespective of how much personal information is stored on it.

2.4 Staff issued with a laptop or responsible for pool laptops, are responsible for ensuring that these are connect to the council network at least once in every 28 days in order to update the security software.

2.5 Any decision about reporting or not reporting a loss or compromise of personal information to the Information Commissioners Office, must be authorised by the Solicitor to the Council or a member of the Legal team.

2.6 Transfers of bulk records (eg., 1000 customer files) must be risk assessed, authorised by the ISO and accompanied by a Information Sharing Protocol.

2.7 All transfers must be logged in the Departments Information Asset Register.

2.8 Access to personal information restricted to a need to know principle only.

2.9 All Departments must ensure that a retention period is defined for all information for staff to follow in line with Corporate Retention Guidelines.

3. Associated Documents

- Classification Guideline
- Good Practice Guide to Handling Information
- Good Practice Guide to taking information out of the office
- Good Practice Guide to sharing information with 3rd Parties
- Retention Guidelines

4. Revision History

Issue	Date of Issue	Revisions Made
1	December 10	First issue.
2	February 11	Added new policy statement that laptops must connect every 28 days. Included Revision History