



# Falkirk Council

## Information Security Policy

Version	Date
Version 2	May 2011

## Contents

No	Section	Page
	Contents	2
1	Introduction	3
2	Policy Scope	3
3	Policy Purpose & Objectives	4
4	Management of Information Security	5
5	Security Management & Responsibilities	6
6	Security Incidents	7
7	Data Sharing	8
8	Principles of Information Security	9
9	Acceptable Use Policy	16
10	Homeworking/Remote Working	16
11	Review of the Policy	17
12	Summary	18
Appendix A	Legislation	19

## **1. INTRODUCTION**

- 1.1 Falkirk Council relies on information to fulfil its outcomes, goals and obligations. Information and the systems we hold and use represent an extremely valuable asset both to the Council and potentially to others. The increasing reliance on information technology for the delivery of the services provided by the Council make it necessary to ensure that these systems are developed, operated, used and maintained in a safe and secure fashion.
- 1.2 Threats to Information Security are becoming more widespread, ambitious and increasingly sophisticated. The consequences of the loss and misuse of confidential and sensitive information can not only be significant to the organisation but can be devastating to individuals. It is essential, therefore, that all information processing systems within the Council, in whatever format, are protected to an adequate and effective level from disruption or loss of service or compromise whether through accidental or malicious damage.
- 1.3 It is necessary to have an Information Security Policy (the Policy) to provide the guidelines and framework for ensuring that the confidentiality, security and integrity of information held by the Council, its services and officers is maintained.

## **2. POLICY SCOPE**

- 2.1 The Information Security Policy Applies to:
- All employees of Falkirk Council;
  - All Elected Members of Falkirk Council; and
  - All employees and agents of external organisations who in any way support or access any Council information system.
- 2.2 Information covered by this policy includes that which is:
- Stored on computers or mobile devices
  - Transmitted across networks - both internally and externally
  - Printed
  - Written
  - Sent by fax
  - Stored in electronic format on an external device or media e.g. on CD, DVD, USB drive etc.
  - Sent/received via e-mail
  - Stored in databases
  - Held on microfiche
  - Held on CCTV tapes
- 2.3 The document also outlines the Council's policy in relation to the use of ICT equipment and especially the areas of:-

- Fraud
- Theft
- Use of unlicensed software
- Private work
- Hacking
- Sabotage
- Misuse of personal data
- Use of the Internet and email
- Disposal of Equipment
- Compliance with relevant legislation (see below and Appendix A)

2.4 The Policy has also been produced in line with the British Standard on Information Security BS7799-2 which is acknowledged as the appropriate industry standard for Information Security.

2.5 The Policy also recognises that some aspects of information security are governed by legislation. The most notable Acts are:

- The Data Protection Act 1998
- Copyright, Designs & Patents Act 1998
- Computer Misuse Act 1990
- Human Rights Act 1998
- Regulation of Investigatory Powers (Scotland) Act 2000
- Regulation of Investigatory Powers Act 2000
- Freedom of Information (Scotland) Act 2002
- Electronic Communications Act 2000
- Telecommunications Act 2003

2.6 A more detailed explanation for each of the above is contained in **Appendix A**.

### **3. POLICY PURPOSE & OBJECTIVES**

3.1 The purpose of security in any information system is to preserve an appropriate level of:

#### **Confidentiality**

The prevention of the unauthorised disclosure of information.

#### **Integrity**

The prevention of the unauthorised amendment or deletion of information.

#### **Availability**

The prevention of the unauthorised withholding of information or resources.

3.2 The Policy objectives are to:

- Ensure that staff and Elected Members have an appropriate awareness and concern for information security and an understanding of their personal responsibility for information security.
  - Ensure that all contractors, their agents and employees have a proper awareness and understanding of their responsibility towards the systems and information of the Council.
  - Provide a framework giving guidance for the establishment of standards and procedures for implementing information security.
  - To meet the general objectives of BS7799-2 Code of Practice for Information Systems Security.
  - To ensure that all employees and Elected Members are aware of the legislation surrounding information and information systems security.
- 3.3 The Policy applies to all locations from which Falkirk Council systems are accessed - including home use.
- 3.4 The Policy applies to all systems and information regardless of the purpose for which it is held or the format in which it is held.

#### **4. MANAGEMENT OF INFORMATION SECURITY**

- 4.1 Information Security is the responsibility of all the employees and Elected Members of the Council. The Corporate Management Team through Corporate and Neighbourhood Services will be responsible for overseeing, monitoring and reviewing the Policy as appropriate.
- 4.2 The Head of Service with responsibility for ICT has overall responsibility for the security of the Corporate Systems and Network. They will delegate the tasks of implementing, monitoring, documenting and communicating these aspects of Information Security to appropriate officers within Corporate & Neighbourhood Services ICT in compliance with this Policy and legislation.
- 4.3 Service Managers and System Administrators are responsible for ensuring that all staff are aware of their responsibilities under the Policy and have access to the contents of this document. This Policy should be made available to all staff as part of the corporate induction process.
- 4.4 All providers of Information Services must take all reasonable steps to ensure the security, integrity and availability of data within the service provided.

#### **5. SECURITY MANAGEMENT & RESPONSIBILITIES**

##### **Objective**

- 5.1 The objective of the Policy, as detailed in Section 3 of this document, is to ensure that all employees, Elected Members and Service Providers are aware of the security risks and of their responsibilities in minimising the threat to the Council.
- 5.2 Information Security is a shared responsibility. The Council is not reliant on a single person or group of people in order to ensure that the confidentiality, integrity and availability of its Information is maintained.

### **Systems & Data Management**

- 5.3 Throughout the Council, there are many people are responsible for the management of systems and data. These can be Systems Managers or Administrators or Service Managers responsible for specific areas of data.
- 5.4 Staff involved in Systems and Data Management have a responsibility to ensure that:
- In conjunction with Corporate & Neighbourhood Services ICT, software licenses to use their systems are accurate, up to date and purchased in accordance with the financial regulations of the Council.
  - Access to the system/data is controlled in an effective manner.
  - Any violation or misuse of the system/data is reported immediately in the appropriate manner.
  - System users are adequately trained.
  - System users are aware of their obligations with regards to Information Security and in particular to this Policy.
  - Any transfers of data whether internally or externally are handled according to any required standards e.g. those laid down by the DWP or GSX Code of Connection and are commensurate with the risks associated with the data.
  - Any disposal of Information, regardless of the format in which it is held, is done so securely and in accordance with this Policy and Records Management guidelines.
- 5.5 When Services are purchasing or creating new systems, the principles laid down in this Policy must be incorporated into the specification or tender.

### **Systems Development**

- 5.6 All System Developments must comply with this Policy and appropriate consideration must be given to data and system security within the business case and system specification.

### **Management Responsibilities**

- 5.7 It is the responsibility of all Managers to ensure that:
- All staff are made aware of their security responsibilities.
  - All appropriate staff have signed the Acceptable Use Policy.
  - All staff are appropriately trained in the systems which they use.
  - Staff are only able to gain access to authorised systems.

- Staff involved in the transfer or sharing of data are aware of the relevant security procedures required for this.
- They have implemented procedures to minimise the Councils' exposure to fraud, theft or disruption to its systems.
- All staff changes are noted as soon as possible through system administrators or the ICT Service Desk to ensure that passwords and system access may be withdrawn, amended or deleted as appropriate.
- Where they are responsible for System Managers/Administrators, they ensure that specific reference to their role with regards to Information Security is within the job description of the individuals.
- All staff have access to and are aware of this Policy and its contents.

### **Employee and Elected Members**

- 5.8 It is the responsibility of each employee and Elected Member to ensure that no breaches of Information Security occur as a result of their actions.
- 5.9 Employees and Elected Members are responsible for ensuring that any breach, or suspected breach, is reported immediately in the agreed manner outlined within this Policy.

### **System Administrators**

- 5.10 Systems administrators must ensure that:
- All staff who have access to the system are entitled to do so as per authorised requests from relevant managers from and have a level of access appropriate to their job.
  - All staff are appropriately trained in the system prior to being granted access.
  - All staff involved in the transfer or sharing of data to or from their system are aware of the procedures required to do this to ensure the security of the data.
  - Arrangements are in place to ensure that system activity is audited.
  - Any security breaches are reported as soon as possible in the manner outlined in this Policy.

## **6. SECURITY INCIDENTS**

- 6.1 A Security Incident can be defined as an event that has, or could have, resulted in a loss or damage to Council Assets or an event which is in breach of the Council security procedures.
- 6.2 Security incidents are many and varied. They can include, but are not restricted to:
- the loss of a laptop or USB Key;
  - theft or loss of data held in electronic format;
  - a break in to Council premises;
  - paper files going missing;
  - the disclosure of confidential information; and

- the unauthorised use of corporate data.
- 6.3 All employees and Elected Members have a responsibility to report security incidents as quickly as possible through the defined channel. This obligation also extends to employees and agents of external organisations contracted to support or access the information systems of the Council.
- 6.4 Any individual who is aware of a security breach or incident or who suspects that this policy is being violated by another individual must report the violation immediately to his or her Manager in the first instance. In the case of Elected Members, this should be reported to the Director of Corporate and Neighbourhood Services or Head of Service responsible for ICT.
- 6.5 Any breach of the policy will be investigated as appropriate by ICT, with managers and Human Resources involved as is necessary. Security breaches should be reported through the ICT Service Desk and will be logged.
- 6.6 Any breach of the policy may result in an employee being subjected to the Council's disciplinary procedure. For Elected Members, any breaches will be referred to the Director of Corporate and Neighbourhood Services or Head of Service responsible for ICT.

## **7. DATA SHARING**

- 7.1 Falkirk Council is engaged in sharing data with partner agencies and organisations for a number of different purposes. The security objective of data sharing is to enable an efficient flow of information without compromising its security, integrity or confidentiality. This is of particular importance where the data which is shared is personal data as defined and regulated by the Data Protection Act 1998.
- 7.2 Falkirk Council works with partner organisations and is a member of the Forth Valley Data Sharing partnership. Data is shared between Falkirk Council and partner agencies both to fulfil a legal obligation and in the delivery of Services to the people of Falkirk. Partners in this context include, but are not limited to:
- NHS Forth Valley
  - Central Scotland Police
  - Scottish Prisons Service
  - Department of Work and Pensions
  - Inland Revenue
  - Scottish Government
  - Central Scotland Fire & Rescue Service
- 7.3 Data must only be shared where it is legally permissible and this may require the consent of the data subject.
- 7.4 Data may be shared in a number of different formats and Falkirk Council is a member of the Government's Secure Extranet. The most appropriate method of

transfer must be used based on an assessment of the risks associated with the sensitivity and classification of the data being transferred.

- 7.5 The Forth Valley Data Sharing Partnership has created a Data Sharing Protocol to which Falkirk Council agreed. However, although this provides the framework for sharing data in a standard format amongst partners, this does not give license to share data without recourse to the legality of doing so. Separate data sharing agreements should be in place where specific types of data are shared between partner organisations.
- 7.6 When sharing data, the requirements of this Policy and any relevant legislation must be adhered to. A risk assessment should be undertaken by Managers to ensure that all measures have been taken to ensure that the integrity and confidentiality of data is maintained, the transfer method is the most appropriate and any appropriate data encryption tools used.

## **8. PRINCIPLES OF INFORMATION SECURITY**

- 8.1 The Information Security Policy is based on the 10 principles set out in ISO-17799. The ten principles are:

- Business Continuity Planning
- System access control
- System development and maintenance
- Physical and environmental security
- Compliance
- Personnel security
- Security Organisation
- Computer and network management
- Asset classification and control
- Security policy

- 8.2 The responsibilities and obligations of the Council, its employees and Elected Members are now looked at in relation to each of these Principles.

### **Business Continuity Planning**

- 8.3 The objective of the principle is to protect the business activities and critical business processes of the Council from the effects of major failures or disasters.
- 8.4 Each Service is responsible for preparing and maintaining their own Business Continuity Plan, The Municipal Buildings and Council Headquarters also has a Plan and ICT has their own plan for the corporate systems housed in the main Computer Suite and for both the Wide Area Network and Corporate mobile and land based telephone networks.
- 8.5 All Business Continuity Plans (BCP) will be developed, documented, tested and updated regularly to reflect the changing business needs of the Council. Services are required to report on the content and robustness of their BCPs periodically to the Corporate Risk Management Group.

- 8.6 With regards Information Security, the BCP will:
- Identify critical computer and paper based systems
  - Identify and prioritise key system users
  - Identify areas of greatest vulnerability based on a risk assessment
  - Have an agreement with users on identified disaster scenarios and what levels of disaster recovery are required
  - Incorporate immediate actions to be taken in response to various scenarios
  - Document fallback procedures to be taken to provide contingency planning for any systems experiencing complete failure.
- 8.7 All employees and Elected Members should be aware of the existence of the plans and all staff directly involved in the execution of the plans should be trained accordingly and have an up to date copy of the BCP.

### **System Access Control**

- 8.8 The objectives of this principle are to
1. Control access to information
  2. Prevent unauthorised access to information systems
  3. Ensure the protection of network equipment & services
  4. Prevent unauthorised computer access
  5. Detect, investigate and take action against unauthorised activities
  6. Ensure information security when using mobile computing and in the Homeworking environment.
- 8.9 In order to meet these objectives the Council will:
- Control access to areas where information is stored either electronically or in paper/other format e.g. the Computer Suite area has a controlled access door with a further controlled access door to the Computer room itself. A gas fire extinguishing system is in place in this area. The computer room is also control by an independent alarm system out of working hours.
  - Require compliance with this Policy and the AUP for all system users.
  - Provide filtered access to the Internet to reduce the risk of illegal or inappropriate material being accessed.
  - Ensure that passwords are required to access systems and that these are changed routinely wherever possible. System time outs will also be activated where possible. Users have a requirement under the Financial Regulations of the Council to ensure that passwords are not disclosed.
  - Ensure that access to systems is controlled by Managers & System Administrators who have a responsibility to ensure that access to systems is kept up to date e.g. by ensuring that employees are removed when they cease to be employed by the Council.
  - Ensure that the Council's network is as secure as possible with appropriate technical measures employed to maintain its integrity e.g. an appropriately configured firewall is in place, maintained and supported.

- 8.10 Passwords for network access will all require to be 'strong' in order to decrease the risk of unauthorised access to systems or 'hacking'. Current requirement for these include being a combination of at least 3 character types i.e. upper case alpha, lower case alpha, numeric or symbols, changed regularly and be at least 8 characters in length. ICT will advise all users of the requirements for password configuration should these change.
- 8.11 All passwords should adhere to basic rules including that they should not be easily identifiable with the individual. Names and family names, pet names and even car registration numbers should be avoided as these can easily be linked to the individual and may permit hacking.

### **System Development & Maintenance**

- 8.12 The objectives of this principle are to:
1. Ensure security is built in to all systems
  2. Prevent unauthorised loss, modification or misuse of data
  3. Protect the confidentiality, availability and integrity of information
  4. Ensure IT projects and support activities are conducted in a secure manner
  5. Maintain the security of operating system and application systems software and associated data.
- 8.13 To meet these objectives the Council will:
- Make available the required security measures for the development, testing and implementation of systems within ICT project management documentation.
  - Ensure that appropriate and proportionate security measures are built in to systems as they are developed and maintained. These will include:
    - Password protection
    - Control of access to information
    - Data validation
    - Backup and recovery procedures
    - Access to audit trails
    - Compliance with legislative requirements
  - Ensure that tenders for third party software include requirements for the operational security of a system and associated data.
  - Ensure that change control procedures are implemented for any changes, amendments or upgrades to these systems. This should be notified and recorded through the ICT Service Desk system.
  - Ensure that any data transfer to partners or between systems is done in a secure manner.
  - Ensure that all ICT staff have signed the AUP with the additional agreement on security and confidentiality of information they may be asked to access in the course of their duties.

### **Physical & Environmental Security**

8.14 The objectives of this principle are to:

1. Prevent unauthorised access, damage or interference to business premises and information.
2. Prevent loss or damage to or compromise of assets and interruption to business activities.
3. Prevent compromise or theft of either information or information processing facilities.
4. Provide resilience in the case of a security incident.

8.15 To meet these objectives the Council will ensure that:

- Access to non public areas of Council Buildings is restricted and Staff are issued with identification badges which must be worn at all times during working hours. Visitors should be provided with, and display, visitor badges.
- Employees and Elected Members are aware of their responsibilities for all keys, badges, access devices, portable computer equipment, telephones and paper files in their possession. These must be accounted for and returned when leaving the employment of the Council.
- All mobile devices **MUST** be encrypted.
- All USB keys **MUST** be encrypted keys. Please contact the ICT Service Desk for further information on this.
- All laptops and netbooks **MUST** have encryption software loaded. Please contact the ICT Service Desk for further information on this.
- All PDAs require to have additional security features and passwords enabled. Separate advice on this will be issued by ICT.
- Any loss of the above should be reported immediately in the defined manner.
- Access to the ICT facilities is controlled and alarmed and limited to a small number of ICT personnel.
- The FM200 extinguishers are maintained and activated in the main and off-site computer rooms.
- Access to the records management and archives file stores is controlled and restricted as appropriate.
- Servers and network cabinets and equipment are kept in 'safe' areas and in locked rooms wherever possible.
- Backups are held securely.
- Public access to Council provided computers is managed and the appropriate Acceptable Use Policy signed by members of the public accessing this facility either on site or by wireless connection. These guidelines will be reviewed and updated as necessary.
- Pupils should not be allowed to access Council provided Computers, and in particular the Internet, without appropriate supervision.

### **Compliance**

8.16 The objectives of this principle are to:

1. Avoid breaches of any criminal or civil law, statutory, regulatory or contractual obligations and of any security requirements
2. Ensure compliance of systems with organisational security policies and standards
3. Maximise the effectiveness of and to minimise interference to/from system audit processes.

8.17 To meet these objectives the Council will:

- Undertake to comply with all relevant legislation as noted in **Section 2** of this policy and as detailed in **Appendix A**. It should be noted that "all relevant legislation" is not limited to the acts noted in this Policy.
- Ensure that necessary training, guidance and information is provided in the above by the Governance Section of the Chief Executive Office.
- Ensure compliance with contractual obligations for third party software.

### **Personnel Security**

8.18 The objectives of this principle are to:

1. Reduce risks created by human error, theft , fraud or misuse of facilities
2. Reduce the risks caused by misuse of equipment provided by the Council
3. Ensure that users are aware of Information Security threats and concerns and equipped to support and comply with this Policy in the course of their normal work.
4. Minimise the damage from security incidents and malfunctions and learn from such incidents.

8.19 To meet these objectives the Council will ensure that:

- Security responsibilities are clearly defined in the job descriptions of appropriate staff.
- All staff accessing computer systems will sign the Acceptable Use Policy.
- Training will be provided to all computer users.
- All new members of staff undertake Induction Training which should include both the AUP and this Policy.

### **Security Organisation**

8.20 The objectives of this principle are to:

1. Manage Information security within the Council
2. Maintain the security of organisational information processing facilities and information assets accessed by third parties
3. Maintain the security of information when there responsibility for information processing has been outsourced to another organisation.

8.21 To meet these objectives the Council will:

- Require that this Policy be maintained and reviewed and updated by ICT as defined in **Section 11** of this document.
- Ensure that appropriate and active management of records is undertaken in line with the guidance provided to services by the Records Management Working Group.
- Access to the Council's network by third parties for the support of systems or for Homeworking is strictly controlled. Users should access the network through agreed protocols using the WHALE remote access system.
- Protocols are developed for data sharing as defined in **Section 7** of this policy.

## **Computer & Network Management**

8.22 The objectives of this principle are to:

1. Ensure the correct and secure operation of information processing facilities
2. Minimise the risk of systems failures
3. Protect the integrity of software and data
4. Maintain the integrity and availability of information processing and communication
5. Ensure the safeguarding of information in networks and the protection of the supporting infrastructure
6. Prevent damage to assets and interruptions to business activities
7. Prevent loss, modification or misuse of information exchanged between organisations.

8.23 To meet these objectives the Council will ensure that:

- Virus protection is installed and regularly updated in all appropriate ICT equipment.
- Staff are advised to only install authorised and licensed copies of software. Falkirk Council is a member of the Federation Against Software Theft (FAST).
- System backups are taken regularly and those of major systems are held both on and offsite.
- Network traffic is constantly monitored. Capacity Planning is undertaken and reported through the ICT Strategy Group
- System access logs are maintained and reviewed as appropriate.
- Network access by third parties is strictly controlled.
- Network Security is constantly reviewed and penetration testing is regularly undertaken by external experts.
- System documentation is maintained and updated.
- All reasonable means of protection of data transferred across the network or to partner agencies are taken.
- All electronic data is disposed of in a secure manner.
- All hardware failures are logged and details recorded on the ICT Service Desk system.
- All incidents are recorded in the manner defined in this Policy.

## **Asset Classification & Control**

8.24 The objectives of this principle are to:

1. Maintain appropriate protection of corporate assets.
2. Ensure that information assets are recorded.
3. Ensure that information assets receive an appropriate level of protection.

8.25 To meet these objectives the Council will:

- Identify all computer equipment. ICT will ensure that an accurate record is kept.
- Require Services to advise ICT of all purchases of ICT equipment and software prior to purchases being made.
- Ensure that ICT maintain a register of all software installed on Council computers in accordance with the FAST auditing requirements.
- Ensure that no equipment or software is installed on the Council's network without prior approval of ICT.

## **Security Policy**

8.26 The objective of this principle is to provide management direction and support for information security.

8.27 The policy development will focus on:

1. The frequency and impact of security breaches and incidents
2. Compliance with the Council Policy
3. Compliance with relevant legislation
4. The security of working policies and procedures
5. The requirement for training in all aspects of information security - in particular those relevant to the duties of the job of the individual.

8.28 To meet the objective the Council will:

- Formally approve this Policy.
- Endorse the requirements of the Policy.
- Ensure that all Employees and Elected Members take their responsibility in relation to Information in accordance with this Policy.

## **9. ACCEPTABLE USE POLICY**

9.1 Falkirk Council also has an "Acceptable Use Policy" also known as the AUP. The AUP sets out the rules by which Falkirk Council expects users to employ the ICT services and equipment provided to them by the Council in order to carry out their duties in a sensible, professional and lawful manner in accordance with law and with the Council's Code of Conduct for Officers and Members.

- 9.2 The AUP sets out the Council's policy on the use and monitoring of ICT and seek to strike a balance between a users' right to privacy and the Council's responsibility to ensure appropriate use of ICT.
- 9.3 All employees and Elected Members are expected to sign the AUP on joining Falkirk Council as acceptance of the principles, guidance and requirements therein.

## 10. HOMEWORKING/REMOTE WORKING

- 10.1 All employees and Elected Members should be aware of the standards that should be used when working from home for at a location other than their normal workplace when dealing with Council owned information assets.
- 10.2 All Homeworking should be carried out in compliance with the Council's Homeworking Policy and have the authorisation of the relevant line manager. The Policy is available on the Intranet.
- 10.3 When using Council systems or equipment (such as laptops) or using your own computer equipment to work on Council business away from Council's premises, the following rules apply:
- All staff must have signed the AUP and be aware of and adhere to the guidelines for Homeworking/Remote Working within this.
  - Similarly, staff must be aware of the Council's Home Working policy when working from home.
  - All work, not publically available, related to the business of the Council must be password protected.
  - 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.
  - All reasonable precautions should be taken to safeguard the security of any Council equipment or data regardless of the medium it is stored in – paper, diskette, CD, USB device or laptop.
  - Where data to be used at home is of a personal, sensitive or confidential nature such files should be both password protected and encrypted. Advice on encryption methods can be obtained from the ICT service through Customer Contacts.
  - All mobile devices used in remote or home working must be encrypted as described in **Section 8** of this Policy.
  - Where users are part of the GSX mail system, they should only send **protectively marked information** in accordance with the requirements of the GSX Code of Connection.
  - Paper files must be kept in a secure location at all times e.g. locked in the boot of a car if making house calls or travelling between work premises or in the employees' home overnight.
  - In accordance with principle seven of the Data Protection Act 1998, appropriate measures must be taken to ensure the security of personal data

which comes into your possession in the course of your employment to prevent it from theft, loss, destruction or harm either accidental or malicious.

- Any files saved remotely should be transferred to a Falkirk Council System as soon as is practicable.
- Employees must not show (or allow to be shown) any data to any members of their family or visitors to the household.
- Any security breach identified when working from home or remotely should be immediately notified to the relevant line manager who should deal with the incident in the manner defined in **Section 6** of this Policy.

## **11. REVIEW OF THE POLICY**

- 11.1 It is intended that from time to time, as is required by changes to legislation, technology or Council policy, these Guidelines will be reviewed. Sections and appendices can be added to reflect new or amended procedures and guidelines when determined. In any case, this document will be reviewed on a 3 yearly basis.
- 11.2 The Policy has also been reviewed by Internal Audit in terms of the policy's scope and content. Internal Audit will periodically review the content, implementation and effectiveness of the policy as part of their strategic plan.
- 11.3 The Corporate Management Team through Corporate and Neighbourhood Services will be responsible for overseeing, monitoring and reviewing the Policy as appropriate.

## **12. SUMMARY**

- 12.1 The purpose of this Policy is put in place a framework to protect the information assets of the Council from al internal, external, accidental or deliberate threats.
- 12.2 The Information Security Policy aims to ensure that:
- Information will be protected against unauthorised access;
  - Confidentiality of information will be assured;
  - Integrity of information will be maintained;
  - Information will be processed accurately;
  - Regulatory and legislative requirements will be met;
  - Information Security training will be available;
  - All security breaches will be reported and investigated in the defined manner;
  - Business Continuity plans will be produced, tested and maintained;
  - Access controls to systems and other information assets will be reviewed to comply with this Policy; and
  - Employees and Elected Members are aware of their individual responsibilities in relation to information Security.

## ***Appendix A***

### **Legislation**

The Council has to comply with all relevant legislation covering systems, data, information security, ICT equipment and the obligations of the individual towards there.

All employees, Elected Members and all employees and agents of external organisations who in any way support or access any Council information systems must comply with the following Acts. They may be held personally responsible for any breach of current legislation as listed below.

The following are brief descriptions on 'key legislation' affecting information security.

This list is not exhaustive but covers the main legislation. For further advice on legal responsibilities, please ask the Governance Section for advice.

### **Data Protection Act 1998**

- Computers are in use throughout society – collating, storing, processing and distributing information. Much of the information is about people - 'personal data'. This is subject to the Data Protection Act 1998.
- The Council is only allowed to record and use personal data if, under the Act, there is a legitimate purpose for doing so and if details of the information, its use and source have been registered with the Information Commissioner.
- The Act defines strict rules about how the information is used and to whom it is disclosed.
- The Act gives rights to individuals about whom information is recorded regardless of the format in which it is held.
- They may request copies of the information about themselves, challenge it if appropriate and may be eligible to claim compensation in certain circumstances.

Separate guidelines covering the responsibilities of employees and Elected Members under the Act are available via the Council's Intranet site

### **Copyright Designs and Patent Act 1998**

- Under this Act, any duplication of licensed software or associated documentation (e.g. manuals) without copyright owner's permission is an infringement under copyright law. All proprietary software manuals are usually supplied under license agreement, which limits the use of the products to specified machines and will limit copying to the creation of backup copies only. However in some instances, site licenses, permitting the use of software on all machines within a specified site are obtainable.
- To combat the problems of illegal copying, software suppliers have formed their own organisation to police the use of software throughout the UK. The 'Federation Against Software Theft' (FAST) is able to conduct 'spot' checks on organisations, including local authorities, under a court order and without prior warning.
- Falkirk Council already is a member of FAST and is accredited to silver standard.
- According to the Act, individuals found to be involved in the illegal reproduction of software may be subject to unlimited civil damages and to criminal penalties including fines and imprisonment.

Separate guidelines covering the responsibilities of employees and Elected Members in relation to software licensing are available via the Council's Intranet site

## **Computer Misuse Act, 1990**

The Computer Misuse Act, 1990 was introduced to deal with three specific offences that were not adequately covered under existing laws:

- Unauthorised access or attempt to access computer material (such as 'hacking'). Under this offence it is not necessary to prove the users intent to cause harm;
- Unauthorised access with intent. For example, hacking is carried out with the intention of committing a more serious crime such as fraud. Under this offence, if a plan has been hatched which involves the unauthorised use of a computer, the unauthorised use will be sufficient to prove an attempt to commit the crime;
- Unauthorised modification. This part of the act makes it an offence to intentionally cause unauthorised modification such as the introduction of viruses.

The intention of the act is to enable an organisation to take legal action to protect their data and equipment from unauthorised access and damage.

## **Freedom of Information (Scotland) Act 2002**

This Act requires that all recorded information is potentially liable to disclosure including all expressions of fact, intent and opinion.

If a request for information is made, the Act prohibits destruction of the information until it is given out in response to the request. Responses must be provided in line with the timescales set out in the Act.

Any person making a request for information to a public authority is entitled-

- to be informed in writing by the public authority whether it holds information of the description specified in the request, and
- if that is the case, to have that information communicated to them

## **Human Rights Act 1998**

The Act gives effect to the rights set out in the European Convention on Human Rights. It requires public authorities such as the Council to act in accordance with the Convention rights. The most relevant right for the purpose of this policy is the right to privacy in Article 8 of the convention.

## **Regulatory Investigatory Powers (Scotland) Act 2000**

The interception of communications including computer communications such as email, are unlawful unless in accordance with the RIPA (Scotland) Act 2000.

The Council may monitor and record communications for the following purposes:-

- To establish facts and monitor performance of standards.

- In the interests of national security.
- To deter crime.
- To detect unauthorised use of the system.
- To secure a system.

The separate Regulation of Investigatory Powers Act 2000 covers the whole of the UK.

## **Electronic Communication Act 2000**

The main purpose of the Act is to help build confidence in electronic communications. The Act creates a legal framework for electronic commerce, It:

- clarifies the legal status of electronic signatures.
- gives the Government powers to modernise outdated legislation so that the option of electronic communication and storage can be offered as an alternative to paper.
- provides a fallback to self-regulatory scheme that will ensure the quality of electronic signature and other cryptography support services.

## **Telecommunications Act 2003**

This Act provides legislation to govern fraudulent and improper uses of telecommunications equipment.