Information Security Policy
Statement of Policy

The confidentiality, security and accurate processing of information are matters of great importance to Glasgow City Council. The purpose of the information security policy is to protect the Council, its Elected Members, staff and particularly the Citizens and Business of Glasgow that are our customers from information threats, whether internal, external, deliberate or accidental.

This information security policy will ensure the following:

- Confidentiality: ensuring that information is accessible only to those authorised to have access
- Integrity: safeguarding the accuracy and completeness of information and data processing methods
- Availability: ensuring that authorised users have access to information and assets when required
- Regulatory compliance: ensuring that the City Council meets its regulatory and legislative requirements

Where necessary, Glasgow City Council will take action to ensure all information is held securely. The Councils drive towards mobile and flexible working makes this even more of a strategic imperative as our working practices and policy must reflect and support this.

Policy Scope

This policy concerns information in all forms printed or written on paper, stored electronically, transmitted by post or electronically, carried on laptops or spoken in conversation.

The Council interacts with a number of related arms length organisations (ALEOs) which are wholly owned by or in partnership with the Council through a number of different legal structures. Where the information assets of such organisations relate to statutory duties of the Council or services provided on behalf of or in partnership with the Council, this Policy applies. The policy will be communicated to such organisations and where necessary protocols will be put in place to ensure the security policies of both the Council and the partner organisation are fully met.

ACCESS LLP has delegated authority through its agreement with the Council to develop and enforce ICT technical standards and policies to support the principles set out in this document.

The National Context and Implications

> ***11th June 08) "Two government documents relating to al Qaeda in Pakistan and the current situation in Iraq and both marked secret were left in a train".***
>
> ***17th June 2008 "A Cabinet ministers laptop containing sensitive files on extremism stolen from her office. The computer contained restricted government files on extremism and defence".***
>
> ***November 2007 "Saw the disappearance of personal details of millions of child benefit recipients on a disc sent by HMRC through the post".***

These incidents are only a few of the latest and highly publicised incidents in a series of embarrassing losses of government information, but highlight the importance of information security and the need to have the correct policies and procedures in place to ensure incidents which could put both citizens and national security at risk do not arise, and where localised incidents arise, no matter the scale, they are reported and handled effectively.

The three examples above are all different in nature, but demonstrate the significance of information security for government organisations, highlighting that not only do ICT systems need to be considered, but also that an effective policy must tackle the topic of information security as a total issue.

Governance

In order to ensure security of information, the following governance arrangements are required within the Council. These interrelationships between the parties involved are outlined in Appendix 1:

- The Corporate Management Team (CMT) recognises the strategic importance of information security to the organisation and support and directs the Council's strategy, setting the overall direction and ensuring resources for implementation..
- The Information Security Board (ISB) is chaired by the Head of Corporate Policy who is also a member of the CMT. The Board champions Information Security by providing strategic leadership and is attended by all Council Services and has representation from major ALOs.
- The Governance Unit is responsible on behalf of the ISB for the development of the Policy and for liaison with ACCESS LLP and the ICT functions of ALOs. The Unit will take advice from ACCESS on ICT and Property aspects of information security.

- The Information Security Management Group (ISMG) is composed of technical representatives of ACCESS, led by their Security Architect and chaired by the Head of ICT Strategy from the Council. ICT representatives of affiliates will be invited to attend. Members of the ISMG are responsible for technical aspects of information security and compliance with the policy technically, developing a sense of ownership around such issues and raising awareness of them throughout technical teams and in their interactions with their customers.

- Information Asset Owners will be identified at the service area level and will be accountable for ensuring that the risks in relation to the assets are identified and managed according to the appropriate level of security.

- The Glasgow City Council Information Security Policy will act as the key stone of the Information Security Management System (ISMS) to be prepared by ACCESS. The ISMS will set standards for the technical component which will be implemented throughout the ACCESS organisation.

- Governance is essential but education and indeed common sense must play their part and Information security is fundamentally a two way issue. The organisation must have the correct policies and procedures in place and cascade to staff, however staff must also take ownership of the policy, support its aims and observe the related detailed policies and guidelines. This applies to all staff, regardless of their contractual status within the organisation.

- Internal audit regularly review the Council with regard to information security issues as part of their strategic plan

Principles

The Council has identified 7 key principles of information security. The Action Plan to enable this will be maintained by the Information Security Board, and can be found on Connect.

Name & Statement	Rationale & Implications
P1. Data protection: Data must be protected.	Data and intellectual property are valuable to the Council and must be protected from loss, unauthorised use and disclosure. Loss of security control could cause harm to our customers and severely undermine public trust in the Council. We must always remember that much of the information which we handle belongs to our customers and that internal "owners" are responsible for safeguarding their rights.
	Access to buildings or systems must be properly controlled and authorised. Robust IT security solutions are required across the entire estate. The Council's network must be secured and safely open to facilitate direct customer interaction and partnership between organisations Sensitive information must be secured when transferred from the network across the Internet or to removable media including paper.
P2. Relevance and Consistency: Protection should be in relevant and in proportion to the risks and be applied consistently across the organization	Treating all assets as if they are the same leads to many of them having too much or too little protection. Inconsistency across the organisation likewise means that too much or too little protection is applied somewhere. We must strike the balance between the need to share and use information and the need to keep it safe.
	Information assets of critical risk will be highlighted by their owners. The Council will will work towards developing an information asset classification appropriate to organisational needs and the wider information security context.
P3. Security Is An Enabler: Security must help, rather than hinder, the business strategy.	Security, and being able to show we are secure, is crucial to building trust with partners and those with whom we share information Mobile working will bring great benefits to our business and can be done securely, if the risks are identified and managed, rather than avoided or ignored.

Name & Statement	Rationale & Implications
	We must share and evidence good security practice with our customers and partners. Standards protocols and processes are required to manage transfer of data and protecting information taken outside of secured offices
P4. The Right Access: The right access to data should be defined to meet the business requirements	Sharing of data must be a positive process, with explicit actions taken to achieve safe, protected access rather than access being achieved by default A balance must be struck between securing access to information to those who specifically require it to perform their tasks and making it available to enable greater effectiveness. Joining up public services is a key aspect of the Council's approach to e-Government
	Access levels and rights will be clearly defined and controlled through a formal process Links between HR and IT processes are required to facilitate regular reviews of user access rights and to allow access rights to be withdrawn promptly when staff leave or change roles User's identities will be authenticated
P5. Plan For The Unexpected: Do not assume that every eventuality has been anticipated and expect to have to fix things.	Regardless of vigilance, vulnerabilities will be found, new attack techniques will be developed and the surprising will happen. Processes must be flexible enough to cope with the unexpected, security defences layered so as to provide cover should one layer fail and risks from single points of failure managed.
	Access levels and rights both physical and technical must be clearly defined, controlled and authenticated Links between access rights and HR processes are important to ensure regular review and withdrawal of rights when an individual leaves or changes role
P6. Security For The Whole Lifecycle: Security should be considered throughout an information asset's life	Security should be built in from the start, not bolted on later, to avoid expensive redesign or security being left out. During its operational life, processes and procedures should be maintained, resources monitored, future capacity needs planned for and changes strictly controlled. At the end of an asset's life, it should be disposed of carefully, as insecure disposal can expose confidential information.

Name & Statement	Rationale & Implications
	Security should be considered at requirements stage for IT systems and designed in to the solution Requirement to archive information must be considered as part of a classification (as per Principle 2)
P7. Accountability: It must be possible to hold authorised users of information accountable for their actions	Accountability reduces the number of incidents by ensuring that everyone is aware of what they should be doing, deterring wrongdoing and assisting investigations. Segregation of duties is an important aspect of information security by making it possible for cross-checking to take place.
	Responsibilities for information assets should be clearly defined as part of a definition of job activities Each individual should have their own fully auditable access to systems and secure areas of buildings and appropriate monitoring of logs should be undertaken

Standards

Information security will be undertaken in line with the following standards

Standard	Definition
ISO/IEC 27002:2005	Code of practice for information security management
Payment Card Industry Data Security Standards (PCI DSS)	Standard developed by major credit card companies as a guideline to help organisations that process card payments to prevent fraud and other security vulnerabilities and threats
GSX Code of Connection (CoCo)	The Government Secure Extranet is a private wide area network across which secure interactions between connected organisations can occur
National Information Assurance (IA) Strategy (2007)	This outlines an approach for the UK in adopting information risk management by ensuring the correct level of professionalism, education and training; availability of IA products and services as well as compliance and adoption of standards
Information Technology Infrastructure Library (ITIL)	A set of concepts and techniques for managing information technology, infrastructure, development and operations

The Control Objectives for IT (COBIT)	Set of best practice measures for IT
Information Society Forum (ISF) Standard of Good Practice	This addresses Information Security from a business perspective, providing a practical basis for assessing an organisations information security arrangements
Central Sponsor for Information Assurance	Based within the UK Government Cabinet Office providing a central focus for information assurance activity across the UK
Department for Business Enterprise and Regulatory Reform (BERR)	BERR's information security team focuses on policy, both domestic and international, to embed good security practices within the UK business community
Scottish Information Commissioner	Responsible for enforcing and promoting the right to access public information created by the Freedom of Information (Scotland) Act 2002
The National Technical Authority for Information Assurance (CESG)	CESG is the UK Government's National Technical Authority for IA, responsible for enabling secure and trusted knowledge sharing to help their customers achieve business aims

Legislation

Information security will be undertaken in line with the following legislation

Freedom Of Information Act (2002)	Provides the right of access to recorded information of any age held by public sector bodies in Scotland. There is a duty on all local authorities to adopt and maintain a publication scheme approved by the Scottish Information Commissioner
The Computer Misuse Act (1990)	This was created to criminalise unauthorised access to computer systems and to deter the more serious criminals from using a computer or the data it stores by inducing a computer to perform any function with intent to secure access. The act has been modified by the Police and Justice Act 2006
Data Protection Act 1998	The main piece of legislation that governs protection of personal data in the UK. It provides a way that individuals can enforce the control of information about themselves
Human Rights Act (2000)	This act governs interception or

	monitoring of communications, most specifically article 8 which guarantees respect for an individuals private and family life, their home and correspondence. Public authorities can not interfere with these rights unless it's justifiable to do so
Electronic Communications Act (2000)	Gives legal recognition for electronic signatures and makes it simpler to amend existing legislation that could hamper the development of internet services
The Privacy and Electronic Communication (EC Directive) Regulations (2003)	Replacing the Telecommunications (Data Protection and Privacy) regulations 1999 and amendments 2000, these cover a range of issues relating to privacy in respect of electronic communications including telemarketing and cookies
Regulation of Investigatory Powers Act (2000)	Aims to ensure that various investigatory powers available to public bodies are only exercised in accordance with the Human Rights Act 1998. The act legislates for using methods of surveillance and information gathering to help the prevention of crime and terrorism.
The Copyright, Designs and Patents Act 1988	Current UK copyright law which gives creators of literary, dramatic, musical and artistic works the right to control the ways in which their material may be used.

Supporting Documents

To ensure the objectives of this policy are met all staff should adhere to the following guidelines and management have a responsibility for ensuring the material is understood and adherence appropriately monitored. These guidelines will be regularly updated in line with developments in Information Security.

- Acceptable Use Policy
- Computer user Code of Practice
- Creation of Incident Handling Processes
- Domain name Policy and Guidelines
- Email User Guidelines
- Guidance on the use of links
- Reporting of Security Incidents
- Guidance notes on USB Memory sticks
- User Access Management Guidelines
- Virus Protection Guidelines

Appendix 1: Governance