Inverclyde council

AGENDA ITEM NO: 10

Report To:	**Policy and Resources Committee**	**Date:**	**30.03.10**
Report By:	**Corporate Director Improvement and Performance**	**Report No:**	**POL/10/10/PW/APr**
Contact Officer:	**Andi Priestman**	**Contact No:**	01475 712251
Subject:	**DRAFT INFORMATION GOVERNANCE AND MANAGEMENT FRAMEWORK**		

1.0 PURPOSE

1.1 The purpose of this report is to present a Draft Information Governance and Management Framework for approval by Committee.

2.0 SUMMARY

2.1 In February 2009 Internal Audit carried out a high level review of information governance and management across all services of the Council.

2.2 The review was initiated in response to the increased risk to the Council posed by ineffective information governance and management and a number of high profile cases where information had been poorly managed by other public organisations resulting in disruption to service delivery, reputational damage, regulatory censure and fines.

2.3 The review covered the following five key areas and determined the Council's current position against leading practice from the public and private sector:

- Culture
- Organisation
- People
- Process
- Technology

2.4 The review identified Information Governance and Management as a significant area of risk and one of the biggest challenges facing the Council that if not managed properly may result in reputational damage, regulatory censure, fines and impact on service delivery.

2.5 The CMT approved the review report in May 2009 and the Corporate Director Improvement and Performance was appointed as the corporate lead to take this initiative forward.

2.6 An improvement plan was developed to address those areas where the Council had the greatest gaps and a working group was subsequently established in December 2009 to develop the policies, procedures and processes that are required to manage information more effectively.

2.7 A Draft Information Governance and Management Framework has been developed by the Working Group for the Council and is attached at Appendix 1.

2.8 The Framework clearly defines the Council's approach to ensuring effective information governance and management and supports officers and members in managing information responsibly, putting them in a stronger position to deliver corporate objectives and the best possible service.

2.9 The framework will be supported by a portfolio of appropriate policies and operational guidance to drive this initiative forward.

2.10 Two key documents have now been considered and agreed by the Working Group which will assist the Council in improving how information is managed by employees as follows:

- Acceptable Use of Information Systems Policy (Appendix 2).
- Operational Guidance for the Management and Use of USB devices by members and employees has been developed and is attached at Appendix 3.

2.11 One of the key issues identified through the review was around culture and the need for education and awareness raising. A communications plan has been developed by the Working Group with proposals for an awareness raising campaign to be rolled out from April 2010.

3.0 RECOMMENDATIONS

3.1 It is recommended that Committee:

a. Approve the Information Governance and Management Framework;
b. Approve the revised Acceptable Use of Information Systems Policy;
c. Note the Operational Guidance for the Management and Use of USB Devices by members and employees; and
d. Agree that further reports on the Information Governance and Management Framework are submitted to Committee when appropriate.

Paul Wallace
Corporate Director
Improvement and Performance

4.0 BACKGROUND

4.1 Good information governance and management is becoming an area of increasing importance to all organisations. The Council holds an ever-increasing volume of sensitive information, including information on our customers, employees and suppliers/stakeholders. A spate of recent 'blunders' with information loss/theft in government departments has highlighted the need to ensure that the Council is doing everything it can to avoid making the same mistakes. The consequences of such mistakes are not only resource intensive and damaging to reputation, but more importantly, can have serious detrimental effects on individuals affected - physically, financially and/or emotionally.

4.2 Information resources are therefore as important as the Council's other key assets – human, physical, and financial assets. Skills, systems, processes and practices for managing these assets are well established whereas information governance and management remains a relatively new field. Best practice information management will require change in work practices, processes, employee skills and technology.

4.3 Information governance and management applies to all operational information received, created, held, shared, disseminated, disclosed, maintained, reviewed, retained or disposed of by all staff employed by the Council in the course of carrying out their duties and covers all formats of information including electronic, digital and hard copy.

4.4 As part of the 2008/09 Annual Audit Plan, Internal Audit carried out a high-level review of Information Governance and Management which included facilitated workshops for employees across all services.

4.5 The review was initiated in response to the increased risk to the Council posed by ineffective information governance and management and a number of high profile cases where information had been poorly managed by other public organisations resulting in disruption to service delivery, reputational damage, regulatory censure and fines.

4.6 The CMT approved the report and resulting improvement plan in May 2009 and the Corporate Director Improvement and Performance was appointed as the corporate lead to take this initiative forward.

4.7 An improvement plan was developed to address those areas where the Council had the greatest gaps and a working group was subsequently established in December 2009 to develop the policies, procedures and processes that are required to manage information more effectively.

4.8 As part of the work carried out by the group, an Information Governance and Management Framework has been developed by the Council and is attached at Appendix 1.

4.9 The Framework clearly defines the Council’s approach to ensuring effective information governance and management and supports officers and members in managing information responsibly, putting them in a stronger position to deliver corporate objectives and the best possible service.

4.10 The Framework will be supported by a portfolio of appropriate policies and operational guidance to drive this initiative forward.

4.11 Two key documents have now been considered and agreed by the Working Group which will assist the Council in improving how information is managed by members and employees as follows:

- Acceptable Use of Information Systems Policy (Appendix 2).
- Operational Guidance for the Management and Use of USB devices by members and employees has been developed and is attached at Appendix 3.

4.12 One of the key issues identified through the review was around culture and the need for education and awareness raising. A communications plan has been developed by the Working Group with proposals for an awareness raising campaign for all members and employees to be rolled out from April 2010.

5.0 IMPLICATIONS

5.1 Legal: The improvement plan will bring processes in line with regulatory and legislative requirements where applicable.
Finance: There are no financial implications arising from this report.
Personnel: The improvement plan will provide education and awareness raising opportunities for all members and employees who management information.
Equalities: Due cognisance of equalities issues have been taken into account in the preparation of this report.

6.0 CONSULTATIONS

6.1 Consultations took place with relevant officers who form part of the Working Group.

7.0 LIST OF BACKGROUND PAPERS

7.1 Internal Audit Review of Information Governance and Management (May 2009) – available from the Chief Internal Auditor

DRAFT

Information Governance and Management Framework

March 2010

Version 1.0

CONTENTS

1 INTRODUCTION

1.1 Information Governance and Management is the way by which the Council manages and handles all organisational information - in particular the personal and sensitive information of customers, partners, suppliers and employees. It allows the Council to ensure that personal information is dealt with legally, securely, efficiently and effectively, in order to deliver the best possible service.

1.2 This Framework brings together the requirements, standards and best practice that apply to the managing and handling of information. It has four fundamental aims:

- To support the provision of high quality services by promoting the effective and appropriate use of information;
- To encourage responsible staff to work closely together, preventing duplication of effort and enabling more efficient use of resources;
- To develop support arrangements and provide staff with appropriate tools and support to enable them to discharge their responsibilities to consistently high standards;
- To enable Services to understand their own performance and manage improvement in a systematic and effective way.

1.3 Good information governance and management is becoming an area of increasing importance to all organisations. The Council holds an ever-increasing volume of sensitive information, including information on customers, employees and suppliers/stakeholders.

1.4 A spate of recent 'blunders' with information loss/theft in government departments has highlighted the need to ensure that the Council is doing everything it can to avoid making the same mistakes. The consequences of such mistakes are not only resource intensive and damaging to reputation, but more importantly, can have serious detrimental effects on individuals affected - physically, financially and/or emotionally.

1.5 Given the significant risks identified with regard to Information Governance and Management it is essential that the Council has a clear Framework in place to ensure that all information is managed effectively, efficiently and securely.

1.6 The Council is corporately committed to effective Information Governance and Management – it is also committed to ensuring that services, management, employees and elected members are suitably supported to fulfil their responsibilities with regard to the management and handling of information.

1.7 An initial programme of education and awareness raising will begin in April 2010 to support the Framework.

2 PURPOSE

2.1 The purpose of this Framework is to clearly define Inverclyde Council's approach to ensuring effective information governance and management and support officers and members in managing information responsibly, putting them in a stronger position to deliver the corporate objectives and the best possible service.

2.2 Inverclyde Council is committed to the secure use of information and information technology systems which are fundamental to the successful operation of the Council's business.

2.3 This Framework applies to all operational information received, created, held, shared, disseminated, disclosed, maintained, reviewed, retained or disposed of by all staff employed by the Council in the course of carrying out their duties. This document covers all formats of information including electronic, digital and hard copy.

2.4 Aim

This Framework will deliver a consistent, effective approach to information governance and management across the Council at all levels. This will aid the achievement of Inverclyde Council's corporate goals.

The approach is to use best practice tools and techniques to manage the information which the Council holds, with the aim of ensuring that the information is:

- Held securely and confidentially
- Obtained fairly and lawfully
- Recorded accurately and reliably
- Used effectively and ethically and
- Shared appropriately and legally

It is the express policy of the Council to:

- Protect the information assets of Inverclyde Council and its customers from unauthorised or accidental disclosure, modification, denial of access, misuse, loss or destruction, through the use of logical, physical, procedural and personnel controls.

- Permit the use and sharing of information by legitimate users only in accordance with best practices and legal and regulatory compliance. In particular, all employees, information systems, and where applicable contractors and suppliers shall comply with relevant legislative and regulatory requirements for information governance and management.

- Use security risk management techniques, including information classification, to determine the threats to information assets and adopt cost effective and practical solutions to remove or reduce the risk.

- Develop, maintain and operate secure information systems to provide a service of excellence to our customers.

- Prevent the infection and spread of computer viruses and other malicious software on all information systems.

2 PURPOSE (CONTINUED)

- Develop, test and maintain business continuity plans, as necessary, to remove or reduce the impact on the business of any disruption to information systems, premises or personnel.

- Demonstrate commitment to the principles of this Framework by including information security as a factor in the evaluation and placing of contracts with suppliers.

- Promote awareness of information security amongst our employees and our contractors and suppliers as appropriate. Through communication of policies, standards, procedures and guidelines and through training and awareness campaigns.

- Monitor and review the implementation of this Framework and report regularly on compliance including auditing of employees use of Council information systems.

- Review at least yearly the information security policy and associated guidelines and update as necessary.

The Framework aims to focus on the organisation's information governance processes, and looks to raise the awareness of information governance and its importance throughout the organisation, enabling front line staff, managers and directors to manage information in a controlled way.

2.5 Objectives

To facilitate the effective delivery of the Information Governance and Management Framework, the following objectives have been developed:-

- To manage information corporately ensuring cost-effective, timely and high quality information to enable effective delivery of the services required for the Council to achieve its strategies and objectives. This area would include the continuous delivery of good technology infrastructure, applications and other services, as well as the ability to monitor service performance against objectives.

- To ensure that the Council's infrastructure and processes can provide the right information to the right people at the right time for the right purpose by:
    - Ensuring future developments adhere to all relevant national standards and improving current operational systems to comply with national standards.
    - Improving business continuity arrangements.
    - Improving information sharing and collaboration between partner agencies.

- To promote a strong information governance and management culture for employees and elected members.

2 PURPOSE (CONTINUED)

2.6 Scope

The Information Governance Framework is directly applicable to the Council's Directorates and Services as follows:-

Directorate	Services
Education and Communities	Education; Education Planning and Culture; Safer and Inclusive Communities
Community Health and Care Partnership	Children and Families and Criminal Justice; Community Care and Health; Planning, Health Imp and Commissioning; Mental Health and Addictions
Regeneration & Environment	Regeneration and Planning; Environmental and Commercial Services; Property Assets and Facilities Management; Legal and Democratic Services
Organisational Improvement and Resources	Finance; Organisational Development, Human Resources and Performance; Customer Service and Business Transformation

Where appropriate, strategic partnerships and specific projects will also be covered by the Framework, following due engagement with partners to develop and deliver the information governance and management requirements in these areas.

2.7 The Information Governance and Management Framework is objective driven and forms part of the overall corporate governance framework for the Council.

2.8 The complete integration of information governance and management into the culture of the organisation can only be achieved through the full commitment and understanding of all stakeholders, including:-

- Elected Members;
- Corporate Management Team;
- Senior Managers; and
- All Council Officers.

All of these stakeholders have a role to play in the control environment within which the Council operates, whether in connection with policy setting and decision making, the accountability challenge process, the implementation of Council objectives, setting of internal controls or the provision of a safe working environment.

3 ROLES AND RESPONSIBILITIES

Ultimate responsibility for the delivery of Council objectives lies with the Council, Chief Executive and Corporate Directors.

Specific responsibility for executing this Framework rests with the Corporate Director Organisational Improvement and Resources who has delegated overall responsibility for information security to the Head of Customer Service and Business Transformation including the implementation and monitoring of compliance with information technology security requirements.

Management Responsibilities

Heads of Service are responsible for ensuring the promulgation and implementation of this Framework within their area of responsibility. They shall make regular reviews of information security controls and procedures so as to provide and maintain the confidentiality, integrity and availability of all information assets. They shall ensure that sufficient resources are allocated to carry out this Framework in their areas of responsibility.

Line Managers

- General responsibilities to ensure staff are familiar with the latest information governance and management Framework and supporting guidance.
- Ensure that where staff have information risk management responsibilities, this is reflected in their work objectives.
- Responsibility to act upon information risks identified by staff which cannot be managed at employee level.

Individual Responsibilities

The key to effective information security is a positive attitude and pro-active approach by every individual. All members, employees, contractors and suppliers have a responsibility to ensure that information is protected against interference, misuse, theft or unavailability. They shall ensure that information security procedures and controls are implemented effectively and are responsible for reporting to their line manager any security incidents that arise.

4 DELIVERING THE FRAMEWORK

4.1 "Good strategy in this context sets the direction of travel and makes sure that the fundamentals are right...and people, process and technology are the enablers for strategy and need to be changed and shaped over time to deliver it."

The Poynter Report – June 2008

The key step is to get the right balance between **people**, **process**, **organisation** and **technology** and understand the **risk culture** of the Council.

4.2 In early 2009, the Council carried out a review of Information Governance and Management which covered the areas set out in Diagram 1.

The review identified Information Governance and Management as a significant area of risk and one of the biggest challenges facing the Council that if not managed properly may result in reputational damage, regulatory censure, fines and impact on service delivery.

An improvement plan was developed to address those areas where the Council has the greatest gaps and a Working Group was subsequently established to develop the appropriate policies, operational procedures and processes that are required to manage information more effectively.

An Information Governance and Management Framework has been developed by the Working Group (Diagram 2) which sets out the appropriate policies and operational procedures that are necessary to support national and local Information Governance initiatives and the associated legal requirements within the Data Protection Act 1998 and the Freedom of Information (Scotland) Act 2002.

4.3 To take the agenda forward, the Corporate Director Organisational Improvement and Resources has lead responsibility for Information Governance and Management.

4.4 Operationally, an Information Governance and Management Working Group has been established to steer the development of the overall approach and to provide a mechanism for ongoing monitoring and review. The Working Group members are required to be of appropriate seniority and experience, and are identified and nominated by Corporate Directors to represent the interests of the Directorate or of specific services within each directorate.

The Corporate Director Organisational Improvement and Resources chairs the quarterly meetings of the Working Group.

4 DELIVERING THE FRAMEWORK (CONTINUED)

4.5 The role of members of this group has been defined as being to act as representatives of their directorates/services and provide a conduit between the Corporate Management Team and directorate/service teams.

The terms of reference for this group are as follows:-

1. To implement the Information Governance and Management improvement plan for the Council. Key activities include:-

   i. To promote and raise awareness of information governance and management throughout the Council.
   ii. To develop and communicate relevant policies and procedures in relation to Information Governance for the Council.
   iii. To develop relevant training programmes for new and existing employees in relation to Information Governance and Management.
   iv. To develop and implement necessary processes to strengthen the system of internal control over Information Governance and Management.
   v. To develop the necessary standards and guidance which promote and co-ordinate information security across the Council.

2. To monitor and assess the processes to ensure that the Council is in compliance with relevant laws and regulations in relation to Information Governance and Management.

Diagram 1

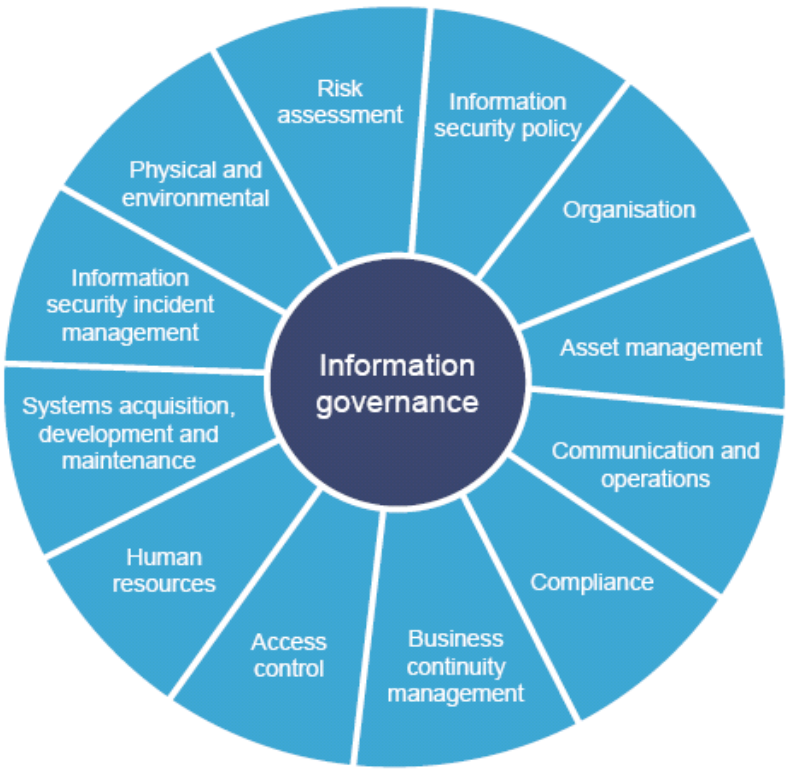
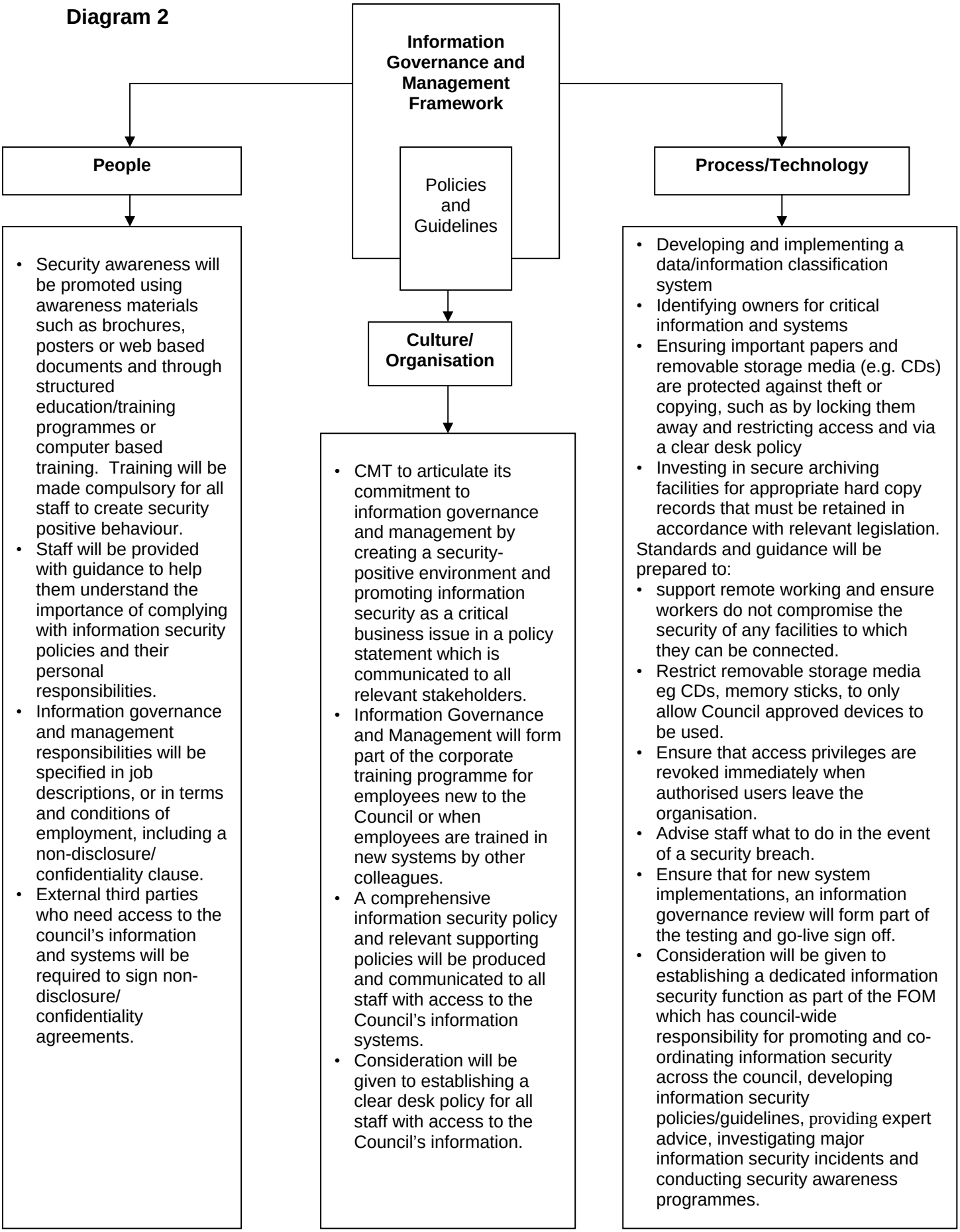


Diagram 2


Information Governance and Management Framework
People
Policies and Guidelines
Process/Technology
Culture/ Organisation
• Security awareness will be promoted using awareness materials such as brochures, posters or web based documents and through structured education/training programmes or computer based training. Training will be made compulsory for all staff to create security positive behaviour.
• Staff will be provided with guidance to help them understand the importance of complying with information security policies and their personal responsibilities.
• Information governance and management responsibilities will be specified in job descriptions, or in terms and conditions of employment, including a non-disclosure/ confidentiality clause.
• External third parties who need access to the council's information and systems will be required to sign non-disclosure/ confidentiality agreements.
• CMT to articulate its commitment to information governance and management by creating a security-positive environment and promoting information security as a critical business issue in a policy statement which is communicated to all relevant stakeholders.
• Information Governance and Management will form part of the corporate training programme for employees new to the Council or when employees are trained in new systems by other colleagues.
• A comprehensive information security policy and relevant supporting policies will be produced and communicated to all staff with access to the Council's information systems.
• Consideration will be given to establishing a clear desk policy for all staff with access to the Council's information.
• Developing and implementing a data/information classification system
• Identifying owners for critical information and systems
• Ensuring important papers and removable storage media (e.g. CDs) are protected against theft or copying, such as by locking them away and restricting access and via a clear desk policy
• Investing in secure archiving facilities for appropriate hard copy records that must be retained in accordance with relevant legislation.
Standards and guidance will be prepared to:
• support remote working and ensure workers do not compromise the security of any facilities to which they can be connected.
• Restrict removable storage media eg CDs, memory sticks, to only allow Council approved devices to be used.
• Ensure that access privileges are revoked immediately when authorised users leave the organisation.
• Advise staff what to do in the event of a security breach.
• Ensure that for new system implementations, an information governance review will form part of the testing and go-live sign off.
• Consideration will be given to establishing a dedicated information security function as part of the FOM which has council-wide responsibility for promoting and co-ordinating information security across the council, developing information security policies/guidelines, providing expert advice, investigating major information security incidents and conducting security awareness programmes.

4 DELIVERING THE FRAMEWORK (CONTINUED)

4.6 Sub-groups have been established to review the Framework and work together to develop the policies and processes required to support the Framework. The sub-groups will have responsibility for developing training and communication plans relating to their particular area within the overall Framework.

4.7 As the Information Governance and Management Framework is being rolled out and embedded throughout the Council, it is imperative that staff, managers, heads of service, directors and elected members understand its principles and how these are adopted in practice.

4.8 It is intended to provide a short briefing to managers who will be involved in rolling out the Framework to their teams.

The corporate induction process will also be used to raise awareness of the Framework and the expectations of new employees who are handling information as part of their job.

4.9 If a service identifies that there are specific training requirements, a tailored training package will be designed and delivered to meet the required needs.

4.10 So that the Information Governance and Management Framework is communicated to as wide an audience as possible, a communications plan has been developed by the Working Group with proposals for an awareness raising campaign to be rolled out from April 2010.

4.11 Following the endorsement of the Framework by the Policy and Resources Committee in March 2010, this Strategy will be made available on the intranet. A copy of the Framework will also be issued across services and externally to our partners.

4.12 A series of briefings will also be undertaken to communicate the Framework through the Service Management Teams.

5 OUTCOMES AND VALUES

5.1 The Council aims to demonstrate the achievement of its objectives by:-

- Ensuring sound systems of internal control in relation to information governance.
- Incorporating information governance risks into major service reviews including best value and project management and tender evaluation processes;
- Regular monitoring and review of information governance and management arrangements; and
- Ensuring that legislative responsibilities in relation to information governance are responded to and met.

5.2 The implementation of the Framework will allow the Council to demonstrate the following values relating to Information Governance and Management:

The Standards:

- Requirement for information to comply with relevant national standards;
- Classification, grading and recording of Council information;
- Eradication of unnecessary duplication;
- Quality of information;

Business Management:

- Duty to obtain and manage information;
- Compliance with national standards for information governance and management;
- Cost-effectiveness in information management;
- Commitment to an information culture;
- Information as a business asset - recognising the value of information used in decision making.

People Management:

- Ownership of information;
- Users' responsibilities towards information;
- Competency in handling information;
- Investment in appropriate resources, skills and training.

Information Sharing:

- Duty to share information lawfully;
- The right information for the right person at the right time;
- Protection of sensitive information;
- Obligations of those receiving information.

Data/Information Management:

- Review, retention and disposal of information;
- Conformity/compliance with external requirements;
- Use of appropriate information technology;
- Security of information;
- Storage of information;
- Data Protection Act 1998;
- Freedom of Information (Scotland) Act 2002

Inverclyde council

Information Governance & Management Framework

Acceptable Use of Information Systems Policy

Version 1.3

Produced by:

Customer Services & Business Transformation
Inverclyde Council
Municipal Buildings
GREENOCK
PA15 1LX

17/03/2010

INVERCLYDE COUNCIL IS AN EQUAL OPPORTUNITIES EMPLOYER

Inverclyde council

THIS POLICY BOOKLET IS AVAILABLE ON REQUEST, IN LARGE PRINT, BRAILLE, ON AUDIOTAPE, OR COMPUTER DISC.

DOCUMENT CONTROL

Document Responsibility		
Name	**Title**	**Service**
	Inverclyde Council Information Systems Acceptable Use Policy	CS&BT

Change History		
Version	**Date**	**Comments**
0.1		
0.2	27/12/2006	RS – changes as per meeting 11/12/06
0.3	10/5/07	RS – Laptop physical security measures
0.4	14/5/07	RS – format changes
0.5	29/5/07	RS – Extended para 2 – section 1 + added music/video streaming SW
1.0	25/10/2007	Final version for approval by committee
1.0	21/11/2007	Approved version – P&R 20/11/2007
1.1	20/01/2010	Added Appendix 1 for GSx – Personal Commitment Statement
1.2	19/02/2010	Information added wrt removable storage media
1.3	17/03/2010	Revised following consultation with Information Governance & Management Working Group

Distribution		
Name	**Title**	**Location**
Corporate Directors & Heads of Service		

Distribution may be made to others on request

Copyright

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying or otherwise without the prior permission of Inverclyde Council.

1. General Principles

This policy applies to all Council employees and elected members and covers the use of the Internet and email, as well as equipment security and working from home on Council business.

NB Staff authorised to use GSx/GSi accounts should note the detailed contents of the GSx/GSi Personal Commitment Statement contained within Appendix 1.

Information and Communications Technologies are an integral part of the business of Inverclyde Council. The Council gives access to ICT systems, email and the Internet to relevant employees, in order to enhance their ability to perform their duties. The Council will always endeavour to be as flexible as it can be in allowing a reasonable level of personal use of email and the Internet and such use by employees should always be outwith core hours. However, should this right be abused, the Council reserves the right to withdraw personal use without notice.

How employees communicate with people reflects on the individual and on the Council as an organisation. The purpose of this policy is to ensure that all employees: -

- understand what is and is not acceptable use of ICT systems, especially email and the Internet
- are aware that all electronic communications are monitored and logged
- understand that, under the Freedom of Information Act (2002), all files and communications may be released to the public
- understand the implications of inappropriate use of ICT systems
- Notwithstanding the above, all employees understand that their rights to privacy will be respected

All information relating to customers and Council operations is confidential. All employees ***must*** treat the Council's paper-based and electronic information with utmost care.

Downloading, copying, possessing and distributing material from the Internet (or any other source) may be an infringement of copyright or other intellectual property rights. Therefore, in general, employees ***must not*** download or copy any material onto Council ICT equipment, unless the information is clearly for business purposes.

Whilst ICT systems are provided primarily for business use, the Council will allow occasional personal use, at the discretion of the employee's line manager, provided that this use does not: -

- conflict with work or business activities
- violate any Council policies or law
- involve any inappropriate content
- involve any use for personal entertainment
- involve the use for any business purpose, other than that of the Council
- involve the ordering of any goods/services over the Internet, other than approved goods for business use. (e.g. Personal banking, payment of bills, booking of personal, non business flights etc)

Employees may be asked to justify the amount of time they have spent on the Internet, or the sites they have visited or the level of personal use of email. Failure to provide a satisfactory explanation may result in disciplinary action, under the Council's disciplinary procedures.

The Council will respect all employees' rights at all times and also places a level of trust in its staff to use these facilities professionally, lawfully, consistently with their duties and with respect for colleagues.

Employees who do not follow the guidelines in this policy may be liable to disciplinary action, under the Council's disciplinary procedures.

In addition to invoking the disciplinary procedure, the Council reserves the right to restrict or deny access to email or the Internet to any employee at work and, in such cases, will give reasons for doing so.

Any employee who is unsure about whether something he/she proposes to do might breach this e-mail and internet policy or is proposing to do something not specifically covered in this policy should seek advice from his/her manager and/or Customer Services & Business Transformation.

2. Monitoring of Communications

The Council will exercise the rights and obligations of a data controller under the Data Protection Act 1998 in relation to staff communications.

The Council has a responsibility to both its employees and the organisation to ensure that ICT systems, email and Internet access are used in a safe, legal and businesslike manner.

In order to ensure the above:-

- all email communication, including incoming and outgoing personal email, and Internet access is monitored at all times and logged automatically by ICT systems
- all emails are filtered for inappropriate language, content and attachments
- ICT systems automatically prevent access to Internet sites that are deemed inappropriate, because of content or because of the security implications of the technology used within the site.

From time to time, there may be circumstances under which it may be necessary for the Council to retrieve and use this recorded information. Whenever this is the case, the Council will endeavour to inform an affected employee when this is to happen and the reasons for it.

Examples of circumstances under which it may be necessary to examine this information include the following:-

- If the Council suspects that the employee has been viewing or sending offensive or illegal material. (e.g. racist, sectarian, nudity etc)

- If the Council suspects that an employee has been using the e-mail system to send and receive an excessive number of personal communications or spending an excessive amount of time viewing websites that are not work related.

- If the Council suspects that the employee is sending or receiving e-mails that are detrimental to the Council

Where an employee is absent through illness or on annual leave, the Council may require to open emails sent to the employee. The opening of emails in these circumstances ***must*** be authorised by the Head of Customer Services & Business Transformation, the employee's Head of Service in consultation, where appropriate with the Head of Legal & Administration.

3. Use of Council ICT Equipment

Employees ***must*** take reasonable care of all ICT equipment issued to them. Basic security guidelines for staff using Council owned equipment include:-

- Store laptops out of sight. If a laptop is used as an office desktop machine, it ***must*** be removed from the desk and stored securely overnight, in a locked drawer or cupboard.

- Rotate storage locations, if possible, of laptops. Changing patterns can make it harder for thieves to prepare for the theft.

- The Council will supply an appropriate carrying case or backpack for transporting the laptop safely and inconspicuously.

- Keep the laptop close at hand. Staff should not leave the laptop case unattended, even for a short time. If possible, remain in physical contact with it at all times.

- Whilst travelling by car, staff ***must*** ensure that the laptop is locked out of sight in the boot of the car, to prevent opportunistic theft.

Employees ***must not***

- connect Personal Digital Music/Video Players to their Council PC

- install or use music or video streaming software, except where express permission has been given by the Head of Customer Services & Business Transformation

- store MP3/WMA (or similar) files, AVI/MP4 (or similar) video files on their local or network drives. They may not use the council network to distribute such files. (Where Services require to utilise such files with respect to providing training or other purpose, prior approval from the Head of Customer Services & Business Transformation ***must*** be obtained.)

- download, install or store games, screensavers and/or wallpapers from the Internet or from any other source

- use Council ICT equipment for any other business purposes, other than those directly related to the Council

- use these facilities to operate any business and/or service operated by them or a third party

- make any attempt to circumvent network security restrictions

- take equipment home or move equipment without permission of their line manager.

4. Use of Electronic Mail

Employees should expressly agree with the recipient, wherever possible, that the use of email is an acceptable form of communication, bearing in mind that if the material is confidential, privileged, price sensitive or commercially sensitive, unencrypted email is not secure.

Some intended recipients may have rigorous email gateway protocols (or firewalls), which can automatically screen all incoming email for content and source. If this is the case, consider whether this means of communication is appropriate.

Employees ***must not***: -

- send or forward messages which are defamatory, libellous, obscene or otherwise inappropriate. The use of email in this way will be treated as misconduct under the Council's disciplinary procedure. In serious cases this could be regarded as gross misconduct and lead to dismissal.

- forward any obscene or defamatory email, whether received unwittingly or otherwise and from whatever source, to any other address.
- impersonate any other person when using email or amend any messages received
- open unsolicited email
- open any attachments from unknown senders
- respond to or forward any chain emails
- forward social emails from friends and colleagues
- click on any unknown or suspicious embedded links.

All email communication is monitored and filtered for inappropriate language, content and attachments. Suspicious emails are quarantined and intended recipients within the Council are sent a message detailing the content and ***must*** give approval before the email is released. If the recipient does not wish to receive the message it is automatically deleted. Details of all quarantined messages are retained. Where it cannot be established by Customer Services & Business Transformation that an email or an attachment to an email presents no risk to the Council Network under no circumstances will that email be released.

5. Use of the Internet

When using an Internet site, employees ***must*** always read and comply with the terms and conditions governing its use.

Employees are ***specifically prohibited*** from downloading and installing software without authorisation from Customer Services & Business Transformation. Any such requests will be judged on whether the software fulfils a business requirement that cannot be provided from the range of software already provided and supported by Customer Services & Business Transformation. Customer Services & Business Transformationwill check that the source is safe before allowing installation. Customer Services &

Business Transformationis also responsible for keeping a record of the licences for all software used in the Council, whether the software was free or paid for. Employees may not download software for non-business related purposes.

Employees are expressly prohibited from: -

- downloading any material that is copyright protected unless authorised to do so by the copyright owner
- downloading any images, text or material which are obscene or likely to cause offence (e.g Racist, sectarian, nudity etc)
- downloading any such material not required solely for business purposes
- introducing any software which has not been authorised (either from on-line or other sources)
- ordering any goods/services over the Internet, other than approved goods for business use
- seeking to gain access to restricted areas of the network
- knowingly seeking to access data which they know or ought to know to be confidential unless authorised to do so
- introducing any form of computer viruses
- carrying out any “hacking” activities
- opening any email via Web Mail accounts. Eg Hotmail, Yahoo Mail, AOL, NTLWorld etc. unless authorised to do so.

For information, the following activities ***are criminal offences*** under the Computer Misuse Act 1990: -

- Unauthorised access to computer material ie hacking
- Unauthorised modification of computer material
- Unauthorised access with intent to commit/facilitate the commission of further offences

Customer Services & Business Transformationhave implemented filtering software that prevents access to sites that are deemed inappropriate because of content or because of the security implications of the technology used within the site. This software monitors and logs all sites visited by

council employees and employees are directed to a warning page when a blocked site is accessed.

Where staff are involved in creating, amending or deleting the Council's web pages or content on the Council's web sites, such work should be consistent with their responsibilities and be in the Council's best interests. Employees ***must*** always ensure that the proper vetting procedures have been complied with and the information is accurate and up-to-date.

6. ICT Systems Security

Employees ***must***: -

- not use ICT systems in any way that may damage, overload or affect the performance of the system or the internal or external network.
- ensure that all confidential information is secure and used only for the purposes intended and is not disclosed to any unauthorised third party.
- keep their user names and passwords confidential at all times.
- ensure that they lock their computer whenever they move away from it for any length of time (Press Ctrl-Alt-Delete simultaneously then click Lock Computer. This will ensure that the machine can only be unlocked with the original password.)

7. Remote and Home Working

This section applies to the use of Council laptops and PCs when accessing Council systems from outwith Council premises. e.g. Home access

Where employees have been given the facility to access the Council Network from home, or any other remote location, they will be provided with a Council owned Laptop or Desktop PC. Employees are not permitted to access the Council network remotely with their own equipment.
It is anticipated that very few staff should have a permanent requirement for a USB memory device, those who do will be issued with a council owned and managed device only after their requirement has been approved at service manager level or above and with the agreement of the Head of Customer Services & Business Transformation. Individuals will be fully responsible for the safe use and management of these devices and the consequence of any data loss should be understood and acknowledged.

Where a temporary requirement for a USB memory device is identified, the ICT Servicedesk will issue a device from a centrally held stock. It will be issued for a fixed period of time and only for the purposes identified in the request. Again the

Individual will be fully responsible for the safe use and management of this device and the consequence of any data loss should be understood and acknowledged.

Use of Council owned laptops and PCs is covered by Display Screen Equipment Regulations 1992. A Display Screen Equipment Assessment is required and a home visit may be carried out by the Council's Health and Safety Officer to ensure home workstations comply with the requirements of the regulations.

All employees ***must***:

- password protect any work which relates to the Council's business
- position themselves so that work cannot be overlooked by any other person
- take reasonable precautions to safeguard all passwords and the security of any computer equipment on which they do the Council's business
- apply an appropriate level of security to any personal data which comes into their knowledge, possession or control through their employment with the Council, so that the personal data is protected from theft, loss, destruction or damage and unauthorised access and use
- inform the police and Customer Services & Business Transformationas soon as possible, if a laptop in their possession or any computer equipment on which they do the Council's work has been stolen
- ensure that any work which they do remotely is saved on the Council's network or transferred to the Council's network as soon as reasonably practicable.

8. Data Protection

On occasion, Council employees may possess or control personal data. When in possession of such personal data, employees ***must***: -

- keep the data confidential and not disclose any information to any other person unless authorised to do so by the Council
- familiarise themselves with the provisions of the Data Protection Act 1998 and comply with its provisions
- process personal data strictly in accordance with the Data Protection Act 1998 and other policies and procedures issued by the Council
- not make personal or other inappropriate remarks about clients or colleagues on manual files or computer records, since the subject of

such remarks has a right to see information the Council holds on that individual.

Inverclyde Council views any breach of the Data Protection Act 1998 and its data protection policy as gross misconduct which may lead to summary dismissal under its disciplinary procedures.

If an employee makes or encourages another person to make an unauthorised disclosure knowingly or recklessly, they may be held criminally liable.

Appendix 1 GSx/GSi Personal Commitment Statement

I understand and agree to comply with the security rules of my organisation as well as the GSi Code of Connection as explained to me in security awareness training I have received.

For the avoidance of doubt, the security rules relating to secure e-mail and IT systems usage include: -

I acknowledge that my use of the GSi may be monitored and/or recorded for lawful purposes; and

- I agree to be responsible for any use by me of the GSi using my unique user credentials (user ID and password, access token or other mechanism as provided) and e-mail address; and
- will not use a colleague's credentials to access the GSi and will equally ensure that my credentials are not shared and are protected against misuse; and
- will protect such credentials *at least* to the same level of secrecy as the information they may be used to access, (in particular, I will not write down or share my password other than for the purposes of placing a secured copy in a secure location at my employer's premises); and
- will not attempt to access any computer system that I have not been given explicit permission to access; and
- will not attempt to access the GSi other than from IT systems and locations which I have been explicitly authorised to use for this purpose; and
- will not transmit information via the GSi that I know, suspect or have been advised is of a higher level of sensitivity than my GSi domain is designed to carry; and

- will not transmit information via the GSi that I know or suspect to be unacceptable within the context and purpose for which it is being communicated; and
- will not make false claims or denials relating to my use of the GSi (e.g. falsely denying that an e-mail had been sent or received); and
- will protect any sensitive or not protectively marked material sent, received, stored or processed by me via the GSi to the same level as I would paper copies of similar material; and
- will not send protectively marked information over public networks such as the Internet; and
- will always check that the recipients of e-mail messages are correct so that potentially sensitive or protectively marked information is not accidentally released into the public domain; and
- will not auto-forward email from my GSi account to any other non-GSi email account; and
- will disclose information received via the GSi only on a 'need to know' basis; and
- will not forward or disclose any sensitive or protectively marked material received via the GSi unless the recipient(s) can be trusted to handle the material securely according to its sensitivity and forwarding is via a suitably secure communication channel; and
- will seek to prevent inadvertent disclosure of sensitive or protectively marked information by avoiding being overlooked when working, by taking care when printing information received via the GSi (e.g. by using printers in secure locations or collecting printouts immediately they are printed, checking that there is no interleaving of printouts, etc.) and by carefully checking the distribution list for any material to be transmitted; and

- will securely store or destroy any printed material; and
- will not leave my computer unattended in such a state as to risk unauthorised disclosure of information sent or received via the GSi (this might be by closing the e-mail program, logging-off from the computer, activate a password-protected screensaver, etc., so as to require a user logon for activation); and
- where my organisation has implemented other measures to protect unauthorised viewing of information displayed on IT systems (such as an inactivity timeout that causes the screen to be blanked or to display a screensaver or similar, requiring a user logon for reactivation), then I will not attempt to disable such protection; and
- will make myself familiar with the security policies, procedures and any special instructions that relate to the GSi; and
- will inform my manager immediately if I detect, suspect or witness an incident that may be a breach of security; and
- will not attempt to bypass or subvert system security controls or to use them for any purpose other than that intended; and
- will not remove equipment or information from my employer's premises without appropriate approval; and
- will take precautions to protect all computer media and portable computers when carrying them outside my organisation's premises (e.g. leaving a laptop unattended or on display in a car such that it would encourage an opportunist thief); and
- will not introduce viruses, Trojan horses or other malware into the system or GSi; and
- will not disable anti-virus protection provided at my computer; and

- will comply with the Data Protection Act 1998 and any other legal, statutory or contractual obligations that my employer informs me are relevant; and
- if I am about to leave my employer, I will inform my manager prior to departure of any important information held in my account.

Enter Name: Gordon McLoughlin **Position**: Risk Owner

Date: 20th January 2010

for and on behalf of all users at: Inverclyde Council
(Connecting organisation)

Information Governance and Management Framework

Operational Guidance on Management and Use of USB Devices

March 2010

V1.0

CONTENTS

1 Introduction

Portable USB Memory devices have become very popular due to their small physical size and large storage capacity. Employees across all services have found them to be an extremely convenient and easy to use method of transporting Council information. However, the proliferation of these devices and their ease of use however has increased the level of risk to the Council as a result of the use or misuse of such devices.

The two biggest risks to the Council from an Information Governance and Management perspective have been identified as the loss of data from stolen or misplaced devices and the introduction of viruses or malware from outside of the Council Network.

The Information Governance and Management Working Group has recognised these risks as a significant threat to the security of the information held on the Council's network and as such the use of unencrypted devices should no longer be permitted and only fully secured and encrypted devices should be used to store Council Data.

2 Aims of the Guidance

The use of secure USB devices supports flexible working and operational service delivery. However, risks to data security are increased and appropriate controls are required. This guidance attempts to achieve an acceptable balance between efficiency, effectiveness and security.

3 Scope

The scope of this guidance extends to data held in any electronic format.

The guidance applies to:

- all employees, including those working from home or from other locations, and elected members
- other workers (including casual and agency workers, secondees and contractors)

who use the Council's equipment and networks, or process the Council's data.

4 Operational Procedures

All unencrypted USB Memory Devices currently provided by the Council will be withdrawn within a set period of time and securely destroyed of in line with the Council's current procedure for the secure destruction of ICT equipment.

Privately purchased USB devices will be prohibited from being used on the Council Network. Owners of such devices who are concerned about the data they hold and who wish to take advantage of the Council's secure disposal facilities will be allowed to hand in such devices for destruction. A USB amnesty will be held with central collection points available to "dump" unwanted devices.

It is anticipated that very few staff should have a permanent requirement for a USB memory device, those who do will be issued with a Council owned and managed device only after their requirement has been approved at service manager level or above and with the agreement of the Head of Customer Service and Business Transformation.

4 Operational Procedures (Continued)

Individuals will be fully responsible for the safe use and management of these devices and the consequence of any data loss should be understood and acknowledged.

Where a temporary requirement for a USB memory device is identified, the ICT Service Desk will issue a device from a centrally held stock. It will be issued for a fixed period of time and only for the purposes identified in the request. Again the member or employee will be fully responsible for the safe use and management of this device and the consequence of any data loss should be understood and acknowledged.

ICT Services are currently implementing an upgrade of existing security softare to allow the control of such devices to be managed centrally.

5 Roles and Responsibilities

Head of Service/Service Manager/Head of Customer Service and Business Transformation

The requirement for a USB memory device must be approved by a Service Manager or above with the agreement of the Head of Customer Service and Business Transformation.

ICT Service Desk

The Service Desk will be responsible for the issue and management of the USB memory device from a centrally held stock.

Member/Employee

Each member or employee issued with a temporary USB device will be fully responsible for the safe use and management of the device.

Each member or employee should be aware of, understand and acknowledge the consequence of any data loss.

6 Security Incidents

Damage to or loss of a temporary USB device issued to an employee must be immediately reported in the first instance to the ICT Service Desk.

The employee must also inform the relevant Service Manager of the loss of a temporary USB device and confirm the volume and type of data currently held on the device.