EXE 191113

Item 14

Information Security and Management

EXECUTIVE MEMBER: Councillor Alan Holliday

LEAD OFFICER: Penny Mell, Head of Policy and Transformation

REPORT AUTHOR: Penny Mell, Head of Policy and Transformation

WHAT BENEFITS WILL THESE PROPOSALS BRING TO COPELAND RESIDENTS?

Information Management is recognised as a key enabler to support the delivery of the Councils corporate objectives and will provide a robust and consistent governance framework.

WHY HAS THIS REPORT COME TO THE EXECUTIVE?

(eg Key Decision, Policy recommendation for Full Council, at request of Council, etc.)

The report provides Members with the progress made in developing the Councils approach to Information Security and Management following a recent audit and provides details of the new Information Management Strategy.

RECOMMENDATIONS: It is recommended that

The Executive considers and agrees the Information Security and Management Strategy and notes the progress made in developing the Councils approach to Information Security and Management.

1. Introduction

1.1 In June 2012, Internal Audit conducted a follow up audit of the Council's arrangements for Information Security. The audit concluded that controls were satisfactory regarding IT responsibilities but weak with respect to corporate ownership of Information Assets. Whilst a number of recommendations had been actioned, a number remained outstanding. These outstanding recommendations were re-focussed as a consequence of the follow up audit to ensure that action to address the audit subsequently focussed on the implementation of the HMG Security Policy Framework (April 2012).

1.2 There are a number of compelling reasons for the Council, like any other organisation, to take information security and management seriously. The importance of keeping information secure is vital as failure could result in prosecution and significant fines. The Information Commissioner's Office (ICO) can impose fines up to £500,000 for serious breaches of the Data Protection Act.

1.3 The development of information management culture, however, is a significant undertaking for any organisation. The audit itself recommended that the Council should consider appointing an Information Security Officer to support the Senior Information Responsible Officer (SIRO) in the development and implementation of the HMG Security Policy Framework. This reflects the size of the challenge for the Council in moving from its current position to one which is more developed yet proportionate. The Corporate Leadership Team

is currently investigating how this commitment might best be met and in the meantime have commissioned external support to take some of the recommendations forward.

2. Progress

2.1 Since the audit, Corporate Leadership Team through the Head of Policy and Transformation, have commissioned an external specialist supplier to assist in progressing the work required to address the audit recommendations.

2.2 In the first instance, our external supplier was commissioned to assist in the development of our Information Security and Management Governance Framework. There have been two key aspects to this work. The first been the development of new policies to make good any deficiencies within the existing framework and secondly, a re-draft of the entire framework to ensure a consistency of approach between the ICT related and non ICT related aspects of Information Security and Management. Critically, this has included the development of a short and punchy Information Management Strategy which is designed to provide an overarching framework for all other Information Security and Management policies to sit within. A list of the policies and procedures within this framework can be found in Appendix A.

2.3 In most instances, these policies and procedures apply to all, that is: all permanent and temporary members of staff; contractors and suppliers; and Elected Members.

2.4 Breaching these policies and procedures can have serious consequences leading to disciplinary action and/or in some cases, criminal prosecution. It is therefore essential that the Council can properly invest in the training and development of staff and Members; and support, particularly Information Asset Owners (IAO) and Information Asset Administrators (IAA), to understand and implement with rigour the spirit of the policies set out.

2.5 We have developed a self-assessment toolkit which managers will be able to use in a supported way to identify their information holdings (if they have not done so already); identify their Information Asset Owners (IAO) and Information Asset Administrator (IAA) on a register; identify and address any risks.

3. Information Management Strategy

3.1 The Information Management Strategy sets out a framework for ensuring that the Council's information assets: remain confidential; maintain their integrity; and are available when needed, and to ensure compliance with all information based legislation, regulations, and other obligations.

3.3 It applies to all users of the Council's ICT or information and if a user is found to have breached this strategy, they must be subject to action under the council's Disciplinary policy.

3.4 The Strategy sets out a number of areas including key responsibilities, communication, security and governance.

3.2 The Strategy should be read in conjunction with other supporting policies contained within the Framework, and is attached as Appendix B.

4. Next Steps

4.1 Progress has been made in developing the Council's approach to Information Security and Management but there remains work to do.

4.2 Making these improvements fall within the Council's Change Programme Plan because efficient and effective data creation; processing, storage and destruction are fundamental in enabling efficient and effective working practices; allowing automation; creating a good customer experience; and complying with the law. It is central to the digitalisation of services.

4.3 Looking forward, we will be:

- Training IAOs and IAAS in the relevant policies and procedures;
- Working with Leadership and Management Group to apply the self-assessment tool kit through a phased roll out based on risk;
- Concluding the review of resources available to support this work; and
- Providing an all Member roles and responsibilities awareness raising session.

5 Conclusions

5.1 This report highlights some of the work that has been completed already but there is more work to do and this will need to be carefully balanced against the resources available to do the work both in terms of specialist capacity and the capacity of the IAO and IAA to discharge this responsibility amongst others.

6 Statutory Officer Comments

6.1 The Monitoring Officer's comments are: It is essential that the Council addresses the issues of information management and security in a robust and coherent manner and the proposals in the report represent a significant start.

6.2 The Section 151 Officer's comments are: Information Management is seen as a key risk for the council and these proposals provide a starting point for the treatment of these risks.

6.3 Policy Framework Comments: Information Management is recognised as a key enabler to support the delivery of the Council's Corporate Plan and as such features within the Change Programme Plan 2013/14.

6.4 EIA comment: Through the programme of work over the next 18 months we will seek to ensure that equalities considerations are made in how information is managed, in particular, where information is created and published for residents and other stakeholders.

6.5 Other consultee comments, if any: None

7 How Will The Proposals Be Project Managed And How Are The Risks Going To Be Managed?

Delivery of the actions will be monitored by the Council's Change Programme Plan with regular updates to the Audit Committee.

8 What Measurable Outcomes Or Outputs Will Arise From This Report?

Information Security and Management is key to ensuring that our legal obligations can be met and that maximum efficiencies can be made in each and every process that we run.

List of Appendices

Appendix A - List of Information Security and Management Policies and Procedures
Appendix B – Information Management Strategy

Appendix A: List of Information Security and Management Policies and Procedures

- Corporate Information Management Strategy
- Key Legislation
- Data Protection Policy
- Freedom of Information Policy (FOI)
- Information Management Security Incident Policy (Breach)
- Protective Marking, Handling and Disposal Policy
- Document Retention Policy
- Business Continuity
- Communications and Operations Management
- Connecting Via Secure Government Link (GCSX)
- Secure Information Transfer Policy
- Information Systems Acquisition Development and Maintenance
- ICT Disposal of Redundant Information Technology Equipment
- Email Acceptable Use Policy
- Internet Acceptable Use Policy
- Change Control Policy
- Access Control Policy
- Mobile Devices Acceptable Use Policy
- Physical Security Policy
- Password Policy

Copeland borough council

Proud of our past. Energised for our future.

Copeland Borough Council

Corporate Information Management Strategy

DRAFT

Document Control

Title: Corporate Information Management Strategy

Issued by: Head of Policy and Transformation

Date: xxx

Author Zurich

Status: Version 1.0

Revision History

Version	Originator	Summary of Changes	Date
Draft	P Mell	Amendments to first draft	18 Jul 2013

Distribution

Name	Title
P Mell	Head of Policy and Performance

DRAFT

Approvals

This document requires the following approvals before release:

Name	Title/Role
P Mell	Head of Policy and Transformation
CLT	
Executive	

Table of Contents

DRAFT

Authorisation Statement

Copeland Borough Council
Information Management Statement

The Council, as a provider of public services, recognises the importance of Information Management and states its commitment to information management and governance. Information Management is a framework for handling information in a confidential and secure manner to appropriate ethical, legal and quality standards. It is an encompassing term that relates to all laws, regulations, policies and procedures, behaviours and protocols for the creation, storage, use, sharing, retention and disposal of all information held by the Council.

As part of the Council's normal operations it stores and processes critical and sensitive information. This information is valuable and the Council is committed to ensuring its confidentiality, integrity and availability. The Council will manage risks to its information and ensure it is adequately protected against the threats, non-technical as well as technical, which can affect it. The Council must comply with relevant legislation that affects information security and governance, including, but not confirmed to the Data Protection, Freedom of Information and Human Rights Acts.

Compromised information can cause significant damage to the Council's operations and reputation. Information not appropriately and adequately protected can lead to serious compliance and legal failures. It is a valuable asset to the council and is the basis upon which strategic and critical decisions are made and operational tasks are performed. Accordingly, it is essential that the information is accurate and complete, properly managed, controlled and secured.

DRAFT

For these reasons, the Corporate Leadership Team on behalf of the Council has approved this Strategy for Information Management.

To support the strategy the Council's Senior Information Risk Owner will have authority for information management and security and will manage them through a set of policies, standards, procedures, best practices, control risk management and other measures and will have the authority to ensure compliance with them. This role will be supported by the Information Security Officer.

This Strategy applies equally to anyone who has access the Council's information and information processing systems. The Information Governance Group, on behalf of the Council, will ensure that everyone has access to the strategy and supporting policies. Anyone with access to Council information and information processing systems is responsible for understanding it and complying with it.

Signed:	**Date:**	**Chief Executive**
Signed:	**Date:**	**Leader of the Council**

1. Introduction

1.1 The Council, as a provider of public services, recognises the importance of Information Management and states its commitment to information management and governance.

2. Purpose

2.1 Information is a major asset that **Copeland Borough Council** has a duty and responsibility to protect.

2.2 The purpose and objective of this Information Management Strategy is to set out a framework for ensuring that the Council's information assets: remain confidential; maintain their integrity; and are available when needed, and to ensure compliance with all information based legislation, regulations, and other obligations.

2.3 The Information Management Strategy is a high level document, and is supported by:

- **Information Standards:** standards that apply to all users of the Council's information, and that are designed to meet: good practice principles defined within the international information security standard ISO 27001; Government Connect Code of Connection; Payment Card Industry Data Security Standards, and mandatory elements of the Government's own Security Policy Framework.

- **Sub-policies:** policies that provide more detail on how the Council will achieve compliance with the Information Standards.

- Procedures for colleagues to follow.

Together these documents form the Council's Information Management Framework.

DRAFT

3. Scope

3.1 This Information Management Strategy outlines the framework for management of Information within Copeland Borough Council

3.2 The Information Management Strategy and associated sub policies and procedures apply to all Users of the Council's ICT or Information, for whatever purpose it is being used. This includes: permanent and temporary employees; contractors; third party suppliers; and Elected Members.

4. Enforcement

4.1 If any user is found to have breached this Strategy and associated sub policies and procedures, they may be subject to action under the council's Disciplinary policy. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

4.2 In regard to the scope of this policy, any conduct and or actions which are unlawful or

illegal may constitute a personal liability.

4.3 If you do not understand the implications of this strategy or how it may apply to you, you should seek advice from the Information Security Officer.

5. Related Documentation

5.1 This Information Management Strategy should be read in conjunction with other supporting policies contained within the Information Management Framework.

6. Risks to Copeland Borough Council

6.1 Data and information collected, analysed, stored, communicated and reported may be subject to theft, misuse, loss and corruption.

6.2 Inadequate training and the misuse and breach of security controls may result in data and information being put at risk. The data can then be used to misrepresent the Council and result in the ineffective use of the council's resources.

6.3 Information security incidents can give rise to embarrassment, financial loss, non-compliance with standards and legislation as well as possible judgements against the Council.

7. Council Priorities

7.1 The priorities for developing the Information Management System Strategy are:

- To ensure adequate staff training and awareness so that everyone understands the role IMS plays in supporting future business success
- To design and implement technical and organisational measures that protect Copeland Borough Council against identified vulnerabilities that prevent customer and employee data being afforded the appropriate level of protection from its point of arrival and to the point of disposal.
- To establish and maintain an assurance framework over Third parties including outsourcing parties used by Copeland Borough Council to ensure they adopt appropriate IMS controls
- To establish a change management practice to ensure Information Management is closely linked to both business and IT strategy development so that future information security improvements can be identified and managed.
- To establish a risk based approach to IMS such that activities are driven by risk assessments and proper change control mechanisms
- To coordinate via the Information Governance Group (IGG) to enable integration with other Copeland Borough Council legal entities to drive a unified approach to IMS which gives benefit to all Council users, partners and customers.

8. Statement of Management Intent

8.1 It is the policy of the Council to ensure that:

8.2 Information will be protected from a loss of:

- **Confidentiality**: so that information is accessible only to authorised individuals.
- **Integrity**: in order to safeguard the accuracy and completeness of information and processing methods.
- **Availability**: so that authorised users have access to relevant information when required.

8.3 The Council has appointed an Information Security Officer to review and make recommendations on information management, policy standards, directives, procedures, incident management and security awareness training.

8.4 Regulatory, legislative and contractual requirements will be incorporated into the Information Management Strategy and supporting policies.

8.5 The requirements of the Information Management Strategy and supporting policies will be incorporated into the council's operational procedures and contractual arrangements.

8.6 The Council will work towards good practice principles identified in the ISO27000 series, the International Standards for Information Security.

8.7 All breaches of information security, actual or suspected, must be reported in the Council's Information Security Incident Policy.

8.8 Business Continuity Plans will be produced, maintained and tested, as detailed in the Business Continuity Policy.

8.9 Information security education and training will be available to all Users.

8.10 Information stored by the council is appropriate to the business requirements and will be processed in accordance with the principles of the Data Protection Act 1998.

9. Responsibilities

9.1 **The Corporate Leadership Team** is accountable and ultimately responsible for:

- Approving a framework for managing and overseeing its duties in relation to Information Management as set out in this Strategy.

- Commitment to, and support for, Information Management.

DRAFT

9.2 The Senior Information Risk Owner (SIRO) is responsible for:

- All aspects of Information Management
- Reviewing and authorising the Information Management Strategy and the associated policies and procedures that emphasise the following principles:
    - Confidentiality – information is accessible to authorised users only
    - Integrity – information is accurate and complete
    - Availability – authorised users only have access to data when they require it
    - Regulatory – compliance with legislative and external standards
    - Guidance on data classification
- Ensuring information security if publicised sufficiently
- Commissioning training to support the development of an effective information management culture
- The SIRO is supported by an Information Security Officer.

9.3 The Information Security Officer is responsible for:

- Being the designated Council owner of the Information Management Strategy
- The maintenance and review of supporting policies and procedures.
- The provision of training and education on information management for all Users, and
- Other specific responsibilities as defined by the SIRO and as set out within the associated job and role description.

9.4 Directors are accountable for:

- Effective procedures which comply with this Information Management Strategy and supporting policies.
- Ensuring the procedures used by officers under their line management are managed in accordance with this Strategy and ensuring that all officers are aware of, and can adhere to, the Information Management Strategy.
- Support for Information Management in terms of resources and commitment.
- Having in place control systems and measures, such as, for example procedures, to ensure the proper care and custody of information used under their line management.
- Ensuring that Information Management Strategy is reflected in Job Descriptions and roles where appropriate.

DRAFT

9.5 Information Asset Owners (Heads of Service) are responsible for:

- Ensuring Information Management is followed.
- Data is classified in accordance with the Protective Marking, Handling and Disposal Policy
- Staff can access Information Management policies readily, they are fully aware of their responsibilities and essential training needs.
- Security incidents are reported and addressed and corrective action is taken to help prevent similar incidents recurring.
- Information Asset Assistants are appointed to cover the daily security responsibilities.
- Ensuring that any necessary management reporting takes place.
- Ensuring the ICT department authorise network access to those employees that do not require access to an application

9.6 Information Asset Administrators (Line Managers) are responsible for:

- The data which they take through the Information Management data life cycle
- Ensuring Information Management policies are applied daily and the controls the Information Asset Owners have approved are operating satisfactorily.
- Ensuring that all permanent and temporary staff, contractors, partners, suppliers and customers of the council who have access to the Information Systems or information used for council purposes are made aware of and comply with the Information Management Strategy and associated policies.

DRAFT

9.7 The Council's Audit Committee is responsible for:

- Reviewing the adequacy of the controls that are implemented to protect the council's information and recommend improvements where deficiencies are found.

9.8 Every user accessing council information e.g. staff, elected members, temporary staff, contract staff are required to adhere to the Information Management Strategy and associated policies.

10. Commercial Activity

10.1 Users are not permitted to exploit, for personal use or commercial gain, any programs,

results, written output or other material developed using Council ICT resources, unless such exploitation has been specifically authorised by the SIRO in conjunction with a Director. The Council retains the copyright of all electronic information created using ICT resources.

10.2 ICT resources provided by the council may not be used for commercial activity, for advertising or for fundraising, except for Council-related activities, unless such activities have been specifically approved by the SIRO in conjunction with a Director.

10.3 Entering into any personal transaction that involves the council in any way (arranging for delivery of personal goods to a council address, for example) is prohibited.

11. Review

11.1 The security requirements for the council will be reviewed by the Information Governance Group and formal requests for changes will be raised for incorporation into the Information Management Strategy and associated policies.

12. Communication

12.1 The Information Management Strategy and associated policies will be communicated to each user who accesses information and information processing facilities.

DRAFT

13. Strategy and policy Standards

13.1 Organisation of Information Management

13.1.1 The security of information will be managed within an approved framework through assigning roles and co-ordinating implementation of this Information Management Strategy across the Council and in its dealings with third parties.

13.1.2 Specialist external advice will be drawn upon where necessary so as to maintain the Information Management Strategy and associated policies to address new and emerging threats and standards.

13.2 Asset Management

13.2.1 All assets (data, information, software, computer and communications equipment, service utilities and people) are accounted for and have an owner. The owner shall be responsible for the maintenance, correct usage and protection of the asset/s concerned.

13.3 Human Resources Security

13.3.1 Employee, contractor and third party terms and conditions of

employment/working and any supporting documents, e.g. role profiles, must set out information management responsibilities and show adequate screening and declaration processes in place (see separate third party questionnaire)

13.4 Physical and Environmental Security

13.4.1 Physical security and environmental conditions must be commensurate with the risks to the area concerned. In particular critical or sensitive information processing facilities must be housed in secure areas protected by defined security perimeters with appropriate security barriers and/or entry controls.

13.5 Communications and Operations Management

13.5.1 Responsibilities and procedures for the management, operation and on-going security and availability of all data and information processing facilities must be established.

13.5.2 The Records Management policy and associated Retention and Disposal Schedule must be implemented for all information holding systems both manual and electronic.

13.6 Access Control

13.6.1 Access to information and information systems must be driven by business requirements. Access shall be granted or arrangements made for Users according to their role, only to a level that will allow them to carry out their duties.

13.6.2 A formal user registration and de-registration procedure is required for access to all information systems and services.

DRAFT

13.7 Information Systems Acquisition, Development and Maintenance

13.7.1 Information management risks must be identified at the earliest stage in the development of business requirements for new information systems or enhancements to existing information systems.

13.7.2 Controls to mitigate the risks must be identified and implemented where appropriate.

13.8 Information Security Incident Management

13.8.1 Information security incidents and weaknesses must be recorded and mitigating action taken in a consistent and timely manner and where applicable all lessons learnt will be shared across the Council, thus mitigating the risk of future incidents.

13.9 Business Continuity Management

13.9.1 Arrangements must be to protect critical business processes from the effects of failure or disasters and to ensure the timely resumption of business information systems.

13.10 Compliance

13.10.1 The design, operation, use and management of information systems must take into consideration all statutory, regulatory and contractual security requirements.

14. Strategy and policy Governance

14.1 The following table identifies who within the council is Accountable, Responsible, Informed and Consulted with regards to this and the sub-policies of the Information Management Framework. In line with the Governments HMG Security Policy Framework 8 (version 8 April 2012), a critical aspect is to critically challenge the Councils approach to information management, assuring themselves and the Council's customers that information security arrangements are at the core of the organisation and the security measures are fit for purpose.

14.2 The following definitions apply:

- **Responsible** – the person(s) responsible for developing and implementing the policy.
- **Accountable** – the person who has ultimate accountability and council for the policy.
- **Consulted** – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- **Informed** – the person(s) or groups to be informed after policy implementation or amendment.

Responsible	Head of Policy and Transformation
Accountable	Chief Executive
Consulted	LMG, CLT.
Informed	All employees, contractors, third party suppliers and Elected Members.

15. Review and Revision

15.1 This Strategy and associated policies will be reviewed as it is deemed appropriate but

DRAFT

no less frequently than every 12 months.

15.2 Policy review will be undertaken by the Responsible Officer. Requests for amendments, clarifications or additions should be made to the Responsible Officer who will make representations to the Accountable body

DRAFT