SCHEDULE 6a

INFORMATION SECURITY POLICY

Essex County Council

Essex County Council Policy for Information Management and Security

Title	Essex County Council Policy for Information Management and Security
Author/Owner	Information Management IS
Status	Final
Version	1.2
Date reviewed	February 2015
Approved Date	February 2015
Next Review Date	February 2016
Security Classification	Official
Approved by	Corporate Governance Steering Board

This document is controlled and has been released electronically. The version on the ECC intranet is the up-to-date document. Hard copies are uncontrolled and may not be up-to date. Users of hard copies should confirm the revision by comparing it with the electronically controlled version.

Contents

1 Why do we need an Information Management and Security Policy? 3
2. Scope 3
3. Information Management and Security Policy Statement 3
4. Key Responsibilities 4
5. Approval and updating 5
6. Appendix A - Legislation 6
7. Appendix B – 7 Principles of Information summary 7

1 Why do we need an Information Management and Security Policy?

1.1 Essex County Council holds and processes personal information about the people of Essex, including the people who work with and on behalf of the Council. Information is received from many sources, including other public agencies and is also produced as part of providing day to day services. Information is a valuable Council asset and is used as the knowledge and evidence base for all Council plans, strategies and decisions. It includes all communications internally and externally with residents and partners as well as information about customers and service users.

1.2 Essex County Council will use all reasonable, appropriate, practical and effective security measures to protect the important business processes and assets in order to protect the information it holds, processes and stores.

1.3 Essex County Council must abide by the laws that govern how information is processed and how information and communications technology (ICT) is used. It is important that the people of Essex are able to trust anyone undertaking duties on behalf of the Council to act appropriately when gathering, holding, providing and protecting information.

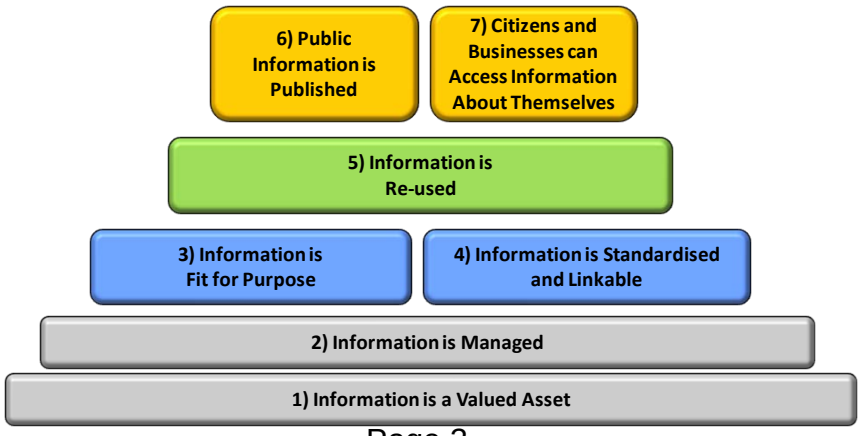
1.4 Essex County Council will ensure any deliberate act to jeopardise the security of information that is held, managed or stored by Essex County Council will be subject to disciplinary and/or legal action as appropriate.

2. Scope

2.1 This policy forms part of the ECC's Information Governance Framework and applies to everyone who undertakes duties on behalf of the Council including Members and applies to information which is either, printed or written on paper, stored electronically, shown on films or spoken in conversation (including phone recordings and taped interviews) and all devices, systems and networks used to manage and store information.

3. Information Management and Security Policy Statement

3.1 Essex County Council will apply the 7 Principles of Information (HM Government, 2011) which have been developed by HM Government to provide high-level guidance for managing information within the public sector. The principles apply to all information that is created, collected, held, used, shared, transformed, published or processed by Essex County Council and covers both structured and unstructured information, and information at all stages of its lifecycle[i]. A summary of the Principles are attached at Appendix B.



3.2 Essex County Council will adhere to the ISO 27001 Standard (Information Security Management Systems) as a framework for guiding the approach to managing information security and protecting the confidentiality, integrity and availability of information assets and business processes. This includes making a commitment to continual improvement and working towards a defined set of information security objectives.

3.3 Essex County Council recognises that the security of the information it holds is essential to the successful provision and delivery of services and will resource the protection of its information assets in ways that are appropriate and cost effective.

3.4 Essex County Council will ensure guidance and training are regularly communicated to all employees and anyone undertaking duties on behalf of the Council.

3.5 The processing of personal data is essential to many of our services and functions, and this processing will often involve sensitive personal data. Compliance with the Data Protection Act 1998 will ensure that this processing is carried out fairly and lawfully.

3.6 Both the Data Protection Act and Article 8 of the Human Rights Act 1998 stress that the processing of personal data needs to strike a balance between, on the one hand, the needs of the organisation to function effectively and efficiently and, on the other, respect for the rights and freedoms of the individual. This policy and associated standards set out how we will ensure that those rights and freedoms will be protected.

4. Key Responsibilities

4.1 Everyone undertaking duties on behalf of the Council, including Members, volunteers and partners must comply with this policy by protecting and managing information securely, reporting security incidents and highlighting weaknesses to the appropriate team. For a full list of responsibilities please refer to the Information Governance Framework on the Information Management & Security Policy and Standards intranet page.

4.2 Line Managers are responsible for ensuring that employees and anyone undertaking duties on behalf of the Council adhere to all information policies, standards and procedures and undertake annual training when dealing with sensitive information. This must be monitored and logged by the line manager.

4.3 The Chief Information Officer (CIO) is also the Senior Risk Owner (SIRO) and responsible for approving policy decisions, policy and standards updates and has responsibility for all information risks across the council ensuring they are managed effectively to deliver business goals.

4.4 The Information Policy Development Group (IPDG) are responsible for feeding in the organisational view into the development and approval of all information policies and standards.

4.5 The Information Governance Team are responsible for updating all information policies, standards and procedure and ensuring they go through the governance process; managing the Information Policy Development Group and co-ordinating information out to all relevant parties.

Joanna Killian
Chief Executive of Essex County Council

5. Approval and updating

This policy statement will be reviewed at least annually to ensure it remains current and appropriate for Essex County Council's business, in conjunction with IPDG and approved by the Operations Board. Any proposed amendments will be submitted to the appropriate governance point for consideration and approval.

Configuration Management

Version	Date	Summary of Changes	Changes made by
1.1	March 14	Final version	
1.2	Feb 15	Update to responsibilities	Susan Young

Failure to comply with this Policy and other supporting policies, standards or procedures may result in disciplinary action, dismissal or legal action being taken against you.

6. Appendix A - Legislation

6.1.1 There are a number of standards and procedures which have been developed to enable employees and anyone undertaking duties on behalf of the Council to be compliant when managing information.

6.1.2 A list of current legislation, which is in no way meant to be exhaustive is listed below:

- Caldicott Code of Confidentiality
- Care Act 2014
- CCTV Code of Practice 2008
- Children Act 2004
- Civil Contingencies Act 2004
- Civil Evidence Act 1995
- Code of Practice for Records management
- Common Law Duty of Confidence
- Communications Act 2003
- Communications Act 2003
- Computer Misuse Act 1990
- Copyright, Design and Patents Act 1998
- Council's Constitution - Financial Regulations
- Crime and Disorder Act 1998
- Criminal Justice and Immigration Act 2008
- Data Protection Act 1998
- Defamation Act 1996
- Electronic Communications Act 1988
- Environmental Information Regulations 2004
- Equality Act 2010
- Freedom of Information Act 2000
- Health & Social Care Act 2001
- Human Rights Act 1998
- Intellectual Property Act
- ISO27001 Information Security Management
- Local Government Transparency Code 2014
- Malicious Communications Act 1988
- Payment Card Industry Data Security Standards
- Privacy and Electronic Communications Regulations 2011
- Protection from Harassment Act 1997
- Public Health Act
- Public Records Act
- Regulation of Investigatory Powers Act 2000

7. Appendix B – 7 Principles of Information summary

This appendix summarises for ease-of-reference the key implications of each principle. Note that it is still important to read the main document section about each principle for further explanation and context - 7 Principles of Information (HM Government, 2011).

Principle 1 - Information is a Valued Asset

There is a declaration from the organisation to establish the importance of information to the business
The approach is defined for consistently identifying, categorising and cataloguing Information Assets and their usage
A framework for assessing and recording the value of information assets is established

Principle 2 - Information is Managed

A framework for managing information through the different stages of its lifecycle is established
The approach to digital continuity is defined
A framework for information risk assessment and risk management is established
The approach to ensuring legal and regulatory compliance is defined
The approach to Information Governance is defined
A skills framework and / or maturity model is established to develop organisational capabilities and culture for information management

Principle 3 - Information is Fit for Purpose

An approach is defined to determining the right quality of information to meet its purpose
A consistent approach is established to describing, recording, and communicating information quality
Processes and governance are established to monitor and assure information quality
An approach is defined to recording the relationship between information and its supporting technology platform and format

Principle 4 - Information is Standardised and Linkable

There is a commitment to Open Standards
Corporate standards are established for the organisation
A framework for linking information is established
A pragmatic approach for migrating to standardised, linkable data is established

Principle 5 - Information is Re-used

Opportunities to proactively offer re-use opportunities are identified
Mechanisms are established to understand and where possible, overcome the constraints on re-use
An approach is established for promoting information that can be reused
An approach is established to discovering information that can be reused
The approach to managing Reference / Master data is established

Principle 6 - Public Information is Published

A framework is in place for responding to legal obligations regarding public access to information
Going beyond the legal obligations, a framework is in place for proactively categorising information in terms of its relevance and suitability for publication
Channels and processes for publishing information are established
A pragmatic migration approach for publishing data is established

Principle 7 - Citizens and Businesses Can Access Information About Themselves

A framework is in place for responding to legal obligations regarding citizens' access to information about themselves and how it has been used
Going beyond the legal obligations, opportunities are identified to proactively make information about citizens available to them by default
The approach to discovering information about a person is established
A pragmatic migration approach is established for enabling citizens' to access information about themselves

[i] For example, some frameworks make a distinction between Data, Information, and Knowledge – with increasing value, interpretation and insight being added at each stage. This is useful and these definitions are considered further in the Resource Base. However in this document, for brevity, the word "information" is used throughout.

5 Appendix C - Applicable Controls and References for Audit Purposes

- PSN IA Conditions – Annex A Example Acceptable Use Statements
- SPF-MR1, MR2 – HMG Security Policy Framework v8 Mandatory Requirement
- HAN-1.1, HAN-1.2 – Hannigan: Mandatory Minimum Measures
- IS0-6.1.1, 6.1.2 - ISO27001
- Essex County Council Information Management and Security Policy
- Essex County Council Standards for Information Management & Security
- Essex County Council Standards on Data Protection
- Essex County Council Standards on Payment Card Security
- Essex County Council Standards for Records Management

(ISO-7.1.3 – MR7, H20.1; ISO-10.4.1 – MR7, MR9, 161, CLG19.1, CLG 19.2; ISO-11.7.1, MR9, MR10, CLG10.2, CLG10.3, CLG10.4; ISO-13.2.1, MR12, H9.2; ISO-15.1.5, MR6, MR7;)