Information Governance Policy

This policy was agreed by the Trust Board on 19 December 2017 to be used as an interim policy by Sandwell Children's Trust.

The intention is to review this policy by 1 July 2018 to ensure that it is fit for purpose for the Trust.

Sandwell Children's Trust

Information Management Unit

Information Governance Policy

Document Type: Tier 1 Policy

Version: 1-0 FINAL

Date Issued: 2014

Document Control

Owning organisation	Sandwell Council
Title	Information Governance Policy
Author	James Trickett
Protective Marking	IL0: UNCLASSIFIED
Review Date	May 2016

Revision History

Revision Date	Editor	Previous Version	Description of Revision
23rd April 2014	James Trickett	n/a	Final version

Document Distribution

Please note – once printed, this documented is uncontrolled. The latest version will always be found on the Council's intranet.

Document Approvals

Approval required	Date approved
JCP	25th March 2014
Leader Decision Making Session	23rd April 2014

Contents

1.0 Introduction

1.1 Information is a vital asset of the Council for the provision of services and efficient operation of services. It plays a critical part in ensuring informed and efficient decisions are made.

1.2 It is of paramount importance that information is efficiently managed and that appropriate policies, procedures, standards and governance are provided to deliver this.

1.3 Information Governance is a framework in which information should be managed in accordance with legal and ethical standards. This Policy provides the top level framework under which the Council can operate.

1.4 This Policy and all complementary policies, procedures and standards form part of a wider Information Governance Framework which details how the Council governs the use of information and information systems.

2.0 Purpose

2.1 The purpose of this Policy is to outline a robust information governance framework that ensures Sandwell Council is able to:

- Meet its legal obligations with respect to effective information governance e.g. Data Protection, Freedom of Information;

- Recognise that information supports the delivery of Council objectives and Scorecard priorities;

- Ensure that information is treated as valuable, useful and reliable asset in much the same way it does for its workers, finances and property.

3.0 Objectives and Scope

3.1 Sandwell Council will maintain a robust Information Governance Framework to ensure the Council:

- Holds its information securely
- Obtains and uses information fairly and efficiently
- Records and maintains information accurately and reliably
- Shares information appropriately and lawfully
- Uses information effectively and ethically

3.2 The Information Governance Framework will also seek to ensure information is available to support continuous service improvement, transparency and openness, accountability and transparency.

3.3 This Policy applies to:

- All information held or processed by Sandwell Council
- All information systems operated, managed or maintained by Sandwell Council
- Any individual using information held by Sandwell Council – this can be Officers, Members, Contractors, third party agencies
- Any individual requiring access to Sandwell Council information

3.4 This Policy is complemented by a range of other Policies:

- Information Security Policy
- Information Acceptable Use Policy
- Records Management Policy
- Information Risk Policy
- ICT and Electronic Communications Acceptable Use Policy
- Data Protection Policy
- Freedom of Information Policy
- Public Sector Network Acceptable Use Policy

These Policies will in turn be supported by the Council's overarching Information Governance Framework document and individual Codes of Practice, procedures and specific guidance.

4.0 Legal and Regulatory Requirements

4.1 Information governance is mandated by various legal requirements:

- Data Protection Act 1998
- Freedom of Information Act 2000
- Human Rights Act 1998

4.2 The Council is also obliged to meet other best practice guidance:

- Records Management Best Practice
- Standards and Copyright Law
- Information Sharing Best Practice
- Privacy and Confidentiality

4.3 Supplementing best practice and legal requirements are organisations:

- Public Sector Network Code of Connection
- N3 Information Governance Toolkit
- Payment Card Industry Data Security Standards
- ISO27002
- Information Assurance Maturity Model

5.0 Key Principles

5.1 The Council recognises the need for an appropriate balance between openness and confidentiality with regards to the management and use of information. It fully supports the principles of corporate governance and recognises its public accountability, but equally it places importance on the need for the confidentiality and security of the information it holds

– particularly that which is personal, sensitive personal or commercially sensitive information.

5.2 The Council also recognises the need to appropriately share information with organisations and agencies which work with it or provide services. Any sharing will be undertaken lawfully and in conjunction with all agreed protocols and contracts.

5.3 The Council believes accurate, timely and relevant information is essential to provide effective and efficient services. It is therefore the responsibility of all Officers and anyone updating or using Council information (or that which is provided to it) to ensure quality is upheld and to promote the principles of information governance.

5.4 The following 4 strands underpin this Policy:

- Openness – Non confidential information maybe disclosed by appropriate means such as the Publication Scheme (operated under the Freedom of Information Act) and the Open Data principles. Conversely, appropriate information will be defined as being confidential and managed under the principles of the Data Protection Act to ensure its protection and non disclosure where this would be unlawful;

- Legal Compliance – The Council will adhere to the requirements of all appropriate legislation with regards to information governance with a specific emphasis on all personal, sensitive personal, patient identifiable data and commercial information. It will only be shared where justifiable and lawful and where necessary with the appropriate consent of the data subject;

- Information Security – The Council will establish and maintain policies, procedures and technical safeguards to ensure all its information assets are adequately and appropriately protected. Ongoing audits and annual tests will be performed to ensure that security arrangements are adequate. Information which needs to be transferred or shared for anything other than direct service provision

will be pseudonymised or anonymised to maintain the confidentiality of individuals;

- Quality Assurance – Quality and effective services can only be provided if the information used to base decisions is accurate. Quality assurance must be maintained throughout the life of information with particular emphasis at is point of creation or acquisition. Information Asset Owners will be responsible for ensure the Council's mandated requirements for effective information quality and information governance are embedded and maintained in their respective service areas. Standard and consistent definition of data items will be used wherever possible.

6.0 Management and Organisational Responsibilities

6.1 This top level Information Governance Policy sets direction and mandatory requirements across the Council supplemented by the other "tier 1" Policies described in section 3 above.

6.2 Tier 1 Policies are approved by Management Board and Elected Members and as dictated by Council processes in consultation with Trade Unions.

6.3 The Council's Senior Information Risk Owner in conjunction with the Council's Information Management Unit and Corporate Information Governance Group will produce, maintain and approve all other supporting information governance documents.

6.4 All Officers must report incidents related to information governance as per the Council procedures. They should be aware of their responsibilities and know where to obtain guidance when required.

6.5 Managers must support their teams in upholding the principles of Information Governance through appropriate guidance and provision of training.

7.0 Training

7.1 Training and awareness will be provided to all service areas to varying levels of details dependent on roles, responsibilities and skill requirements.

7.2 All Officers will be required to undertake and refresh basic information governance training (encompassing Data Protection, Freedom of Information, Information Security / Assurance and Records Management). Training will be delivered by appropriate means including workshops, classroom sessions, e-learning and where appropriate – hardcopy / printed learning materials.

8.0 Systems and Processes

8.1 The Council will augment its policies, procedures and training via appropriate systems to ensure correct fulfilment and embedding of information governance – these might include online e-learning, policy enforcement / awareness systems or systems which support the automation or enforcement of rules e.g. information classification.

9.0 Review

9.1 This Policy will be reviewed every 3 years from the date of approval or prior to this if there are significant changes in legislation or regulation.

End of document