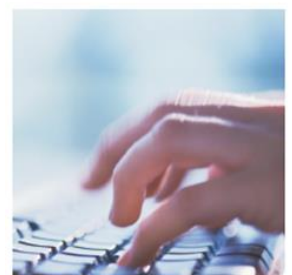




Information Management and Governance Strategy 2016 - 2018

Craven District Council



'Craven District Council aims to develop a culture amongst officers and elected members that properly values, protects and uses information for the benefit of the Council, its residents and other customers, and at the same time respects the rights of those who seek to obtain information about the Council'

www.cravendc.gov.uk

Craven District Council

CONTENTS

1	INTRODUCTION	3
1.1	What is information management and governance?	3
2	CONTEXT	5
3	COMMUNICATION, CONSULTATION AND ENGAGEMENT	6
4	STRATEGIC OBJECTIVES	7
4.2	The detailed objectives of the Strategy.....	7
4.3	Benefits to the Council.....	8
4.4	Implementation	9
5	RISKS	10
6	CRITICAL SUCCESS FACTORS	11
7	GOVERNANCE ARRANGEMENTS	12
	APPENDIX - GLOSSARY	13

1 INTRODUCTION

This document sets out the Council's strategy for Information Management and Governance for the period from 2016 to 2018. It complements and is aligned with the separate ICT Strategy. It should be read in conjunction with the related Implementation Plan, which sets out how the Strategy will be implemented.

The Council's Corporate Leadership Team has already demonstrated a commitment to improve information governance and this Strategy builds on that commitment.

1.1 What is information management and governance?

'Information Management and Governance' includes the policies, procedures, and practices, taking account of laws and best practice that should, when taken together, ensure the security and confidentiality of information throughout the organisation. The strategy, if implemented, will embed best practice within the Council's business activities.

In the context of a local authority, information management and governance will always include:

- **People** - the officers and elected members who handle and process the Council's information assets on a daily basis.
- **Places** – the physical security of the Council's buildings, premises, and systems.
- **Processes** - the day-to-day activities which are applied by the Council's officers and members in the handling of information, which should comply with the policies that have been agreed.
- **Procedures** – the policies and procedures which the Council deploys to implement the measures in the Council's strategy.

For the purpose of this strategy, the term 'information' covers data, documents, maps, records, emails, web pages, and film and voice recordings which are held in many formats within a variety of manually compiled and electronic systems.

Craven District Council aims to develop a culture amongst officers and elected members that properly values, protects and uses information for the benefit of the Council, its residents and other customers (i.e. members of the public).

1.2 Why is there a need for such a strategy?

Effective information governance balanced in a proportionate way against risk forms the basis of dealing with the challenges presented by the scale and diversity of the Council's business activities; the nature and risks presented by the use of information technology; the external demands and expectations of residents and members of the public; and the requirements of the legal framework and the external regulators.

There is an increasing need to share information across the wider public sector and with certain other organisations, in order to provide improved customer services, and encourage collaborative working.

Increased use of modern technologies means that access to information by members of the public and staff working in organisations means that information is often immediately accessible and available (or expected to be so), and there is a voracious appetite for information to be provided electronically and on-line, and immediately.

Coupled with this increased use of technology, there is a rapid and pervasive growth in different channels that enable access to and delivery of information.

Information is increasingly recognised as a valuable asset, not just the personal details of millions of taxpayers and benefit recipients, held by government and other public authorities, but also information which helps influence local political decisions on the environment, economy, planning, health, leisure and tourism, etc. Therefore it is essential that there is a coherent strategy for managing information effectively, and securely, and that the related policies, standards, and guidance are complied with.

The strategy records the determination of the Council's leadership team to improve the handling, storage and use of information in a consistent manner across all the Council's services. It will also better prepare the Council for the implementation of the new General Data Protection Regulation when it is introduced across EU member states in the coming years.

2 CONTEXT

2.1 National

The national context comprises an array of legislation that places obligations on organisations to properly handle and protect information about individuals, and the provision of information by public authorities about their activities, supported by guidance from the regulator for data protection and freedom of information – the Information Commissioner.

In addition, changes are likely to be introduced during the period of this strategy, as the UK Government implements the General Data Protection Regulation (on current estimates, likely to be in the second half of 2018).

At the same time, the possibility of data loss incidents, and the recurring threats to information management which continue to remain a high priority for organisations in general to address, and public authorities in particular.

The strategy also takes account of:

- The Local Government Data Handling Guidelines (2008)
- The Local Public Services Data Handling Guidelines (2012)
- Information Commissioner's Office's (ICO) letter to all local authorities to improve data protection (2013)
- ICO's Audit findings from visits to Local Authorities (2014)
- The Transparency Code (2015)

2.2 Local

The Strategy supports the Council's Plan and the related ICT Strategy. In particular, the delivery of this Strategy will support the Council's Priority of Financial Resilience, by reducing the risk of unwelcome intervention by the regulator, and in the worst case, of enforcement action, and possible monetary penalties for failure to comply with our legal obligations.

The delivery of efficient technology will enable better use of information and other assets. New technologies should allow improvements in the quality of services provided, and enable more secure ways of working, including better information (including document) management.

Previous Internal Audit reports have made a number of recommendations to the Council concerning the need to improve information management. This strategy and the related Implementation Plan will address the weaknesses so identified.

3 COMMUNICATION, CONSULTATION AND ENGAGEMENT

Communications will be achieved through the Communications Plan as described in the IT Strategy. This will ensure a consistent and seamless approach, and ensure convergence between the two Strategies.

Consultation will be achieved through the Information Management Group, and routine reports will be made to CLT and the Audit and Governance Committee.

4 STRATEGIC OBJECTIVES

4.1 Strategic Themes

This Strategy comprises the following strategic themes:

1. Improving Information Governance
2. Protection of the Council's information (including personal data)
3. Promoting employees' and elected members' responsibility to protect personal data of residents, customers, employees, etc (e.g. by providing training and awareness)
4. Providing effective and timeous management of requests for information
5. Promoting effective information sharing and maximising the use of information for the public good
6. Improving compliance

4.2 The detailed objectives of the Strategy

These are to:

- **Implement** a suitable and proportionate information governance regime, including **embedding** improvements to accountability throughout the Council, and supporting the Information Management Group and the Audit and Governance Committee.
- Improve the Council's culture for employees and elected members so that information is properly **understood, valued, protected and better used**, and support the introduction of HR policies and a **Training Framework** that support this aim.
- Establish a **Policy Framework** and deploy best practice information management policies, standards and procedures that are consistently applied across the Council.
- Ensure that the Council's **legal obligations** in the handling, storage and use of personal data are fully **compliant** under the Data Protection Act.
- Introduce a **Performance Management Framework** to ensure that the Council's legal obligations in the provision of information in response to requests are fully complied with (under the Freedom of Information Act, Environmental Information Regulations, Reuse of Public Sector Information Regulations, and the Data Protection Act).
- Support the development of technical information **procedures, practices and guidance** to ensure that information held and processed is accurate, up-to-date, complete, and readily available when required.

- Support the **sharing of information** with other public services partners so that the maximum public benefit can be achieved so enhancing public services through greater access to and availability of information (within the law).
- Comply with the requirements of the **Transparency Code**.
- Ensure that **audit recommendations** are implemented, and that such recommendations are properly tracked.
- Ensure that a periodic assessment can be conducted so as to provide **assurance** to the Corporate Leadership Team, Information Management Group and Audit and Governance Committee that improvements are progressing at an appropriate pace.

4.3 Benefits to the Council

The following benefits will accrue from the implementation of the Strategy:

- Better management and protection of information.
- Raising the level of public trust and confidence in the Council's management of information.
- Reduced risk of accidental loss, theft or corruption of information.
- Reduced the risk from inappropriate data sharing.
- Through the role of Information Asset Owners ensures that the Council is aware of its information assets, and is better able to understand and mitigate related risks.
- Through the role of the Senior Information Risk Owner, ensure that the Corporate Leadership Team better understands the risks to information that the Council manages.
- Mitigating the likelihood of complaints to the ICO over the handling of information and responding to requests.
- Mitigating the likelihood of enforcement action by the ICO, and risk of consequential financial penalties and reputational damage due to inadequate procedures.
- Reduced rework.
- Minimising the duplication of information.
- Minimising the wastage in collection and collation of information.
- Improve business decisions by ensuring that information is accurate and up to date.

- Enhancing officer awareness of the need for organisations to protect information.
- Ensure that the linked standards of Confidentiality, Integrity and Availability are promoted.

4.4 Implementation

The Information Management and Governance Implementation plan provides the vehicle by which the implementation of this Strategy will be measured. This Plan follows the framework provided by the Local Authority Data Handling Guidelines and the Local Public Services Data Handling Guidelines.

Monitoring of implementation will be overseen by the Council's Information Management Group, and a separate progress report will be made to the Council's Audit and Governance Committee.

5 RISKS

The delivery of the Information Management and Governance Strategy will be through a portfolio of managed activities falling within the ICT Transformation programme as detailed within the Implementation Plan.

Some of the key risks associated with the delivery will be:

- Funding constraints, if the resources allocated to the Information Governance Project are not continued during the period of this Strategy.
- Loss of skilled resource to lead on the implementation activities, and also loss of key resources in other parts of the Council providing support.
- Failure of individuals (officers and members) to understand their responsibilities and apply policies effectively.
- Lack of support from the Council's leadership team, including support of the Service Managers.
- Changes in scope which may impact on cost, quality, timescales and resourcing.
- Resource constraints associated with running significant concurrent work activities.
- Important and urgent organisational business priorities emerging which require significant assistance outside of the planned activities in the Implementation Plan.

6 CRITICAL SUCCESS FACTORS

Although the successful implementation of this Strategy obviously depends on the Implementation Plan, success will be measured by the following (in no particular order):

- An improved **culture of awareness** throughout the Council, including visible compliance with physical security procedures, and respecting and valuing information.
- **Improved engagement of senior officers** across the Council, through the new Information Management Group.
- **Measurable awareness activities**, supported by regular employee and member involvement and assessments of engagement.
- An improvement in **Freedom of Information compliance** with the timely provision of responses to requests.
- **Greater visibility and coherence and a consistent presentation of the Council's policies** relating to Information Management.
- A corporate approach to **Information Management which** continues to be supported including the implementation of relevant standards.
- A comprehensive **Information Asset Inventory** with clear accountability by Information Asset Owners.
- The use of **Privacy Impact Assessments on all new projects** involving the use of personal data.
- **Published privacy notices** for all the Council's activities, and a **published Information Charter**.
- **Regular communication** to employees and members of relevant and topical Information Governance issues.
- Successful implementation of the new **General Data Protection Regulation** in 2018.

The Strategy does not anticipate any reduction in requests for information, or of internal or external reviews against decisions. To some extent, such requests, particularly when they are made by local residents, demonstrate local awareness of information rights under the legislation. The Council has very few cases where the ICO has intervened. However, it is expected that as this Strategy is rolled out, the likelihood of enforcement action by the ICO due to a failure of compliance with the Data Protection Act, and the Freedom of Information Act is less likely over time.

7 GOVERNANCE ARRANGEMENTS

Governance will be provided through the Information Management Group (IMG) which is chaired by the Senior Information Risk Owner (SIRO), and include representation from senior managers and Information Asset Owners. Progress reports will be provided to the CLT and the Audit and Governance Committee. IMG will be supported by ICT & Transformation Services.

The IMG will review the Information Risk Register at every meeting, and support the SIRO in providing an assessment of the prevailing level of risk. The proposed terms of reference of the IMG includes the following:

To:

- Provide leadership support for improvements in information management and governance across the Council's activities.
- Consider and approve the Council's framework of policies for information management and governance.
- Regularly review the Council's information risk register, and where improvement is necessary to support changes.
- Regularly review the Information Management and Governance Implementation Plan.
- Approve the programme of culture change activities, including communications strategy, awareness programme, compliance activities, etc.
- Review the reports of any information security related incidents, lessons learned, and to make further recommendations.
- Review progress in responding to requests for information, including timeliness (for responses dealt with under the FoI Act, EIR, and Data Protection Act SARs).
- Review any data sharing arrangements.
- Review the Council's compliance with the Transparency Code.
- Recommend changes to HR processes/policies so as to support better compliance by officers.
- Report to the CLT and the Audit and Governance Committee on the level of assurance that applies across the Council.

APPENDIX - GLOSSARY

Term	Description/Definition
Automated data	Broadly speaking, any information held on a computer, or information recorded with the intention of putting it on a computer.
CLT	Craven District Council's Corporate Leadership Team.
Data	Information in a form which can be processed. It includes both automated data and manual data.
Data controller	A person or organisation who either alone or with others decides on, and controls the content and use of personal data. Data controllers are usually organisations, who handle automated data. There are some exemptions, such as certain charitable organisations. Data controllers are registered with the Information Commissioner's Office and are subject to regulation.
Data processor	An individual or organisation that processes data on behalf of a data controller, but it does not include an employee of a data controller who processes such data in the course of their employment. Examples will include any service provider who delivers services, or performs any function on behalf of the data controller. Data controllers should have a formal contract with a data processor. Data processors are not subject to regulation by the Information Commissioner's Office.
Data Protection Act 1998	Also known as the DPA, sets out the way that organisations must handle personal data of individuals. It includes the Eight Data Protection Principles that organisations must observe. The DPA includes provisions for the prosecution of those who commit criminal offences, and enforcement penalties for organisations who fail to comply with the Act.
Data subject	An individual to whom personal data relates.
Environmental Information Regulations 2004	Also referred to as EIR, similar to the Freedom of Information Act (see below), providing public access to recorded information held by public authorities on activities that impact on the environment. There are very limited exemptions from disclosure.
Freedom of Information Act 2000	Also known as the FoIA, is the legal means by which members of the public can obtain information held in recorded form from public authorities. Nearly all requests have to receive a reply within 20 working days. There are certain categories of information that are exempt from the Act, including information about individuals (personal data).
General Data Protection	(GDPR) a new regulation which has been developed for implementation across all EU countries intended to strengthen

Term	Description/Definition
Regulation	and unify data protection for individuals in the member states. It is likely to be implemented in the UK during 2018.
Information Asset Inventory	A register or inventory of all information assets across the Council, detailing where held if on systems, the numbers of individuals recorded, and the relevant IAO who is responsible for the particular asset.
IAO	Information Asset Owner - this senior officer is usually the Service Manager who is responsible for ensuring that the risks to, and the opportunities for exploiting, information assets for which they are responsible, are monitored. The IAO does not need to be the creator or the primary user of an asset, but they must understand its value to the organisation. Any incidents relating to information assets must be reported to the SIRO.
Information Commissioner's Office	Also known as the ICO, is the public regulator for matters arising under the Data Protection and Freedom of Information Acts. The ICO can investigate incidents involving personal data, and take enforcement action against data controllers, including levying Civil Monetary Penalties or fines. The ICO can also take enforcement action against public authorities that fail to comply with the Freedom of Information Act and EIR.
ICT	Information & Communication Technology
Information Charter	Sets out the standards that individuals can expect from an organisation that holds their personal data or other information. An information Charter is published by the organisation, and demonstrates how the organisation values and can be trusted with personal information.
Manual Data	Information that is kept as part of a relevant filing system or with the intention that it should form part of a relevant filing system.
Personal data	Information relating to a living individual who can be identified from that information, or from information that is in, or likely to come into the possession of the data controller. This can be a very broad definition, depending on the circumstances.
Privacy Impact Assessment	A means by which the impact on individuals' privacy as defined by the Data Protection Act can be assessed, so as to ensure that any new initiative, systems, or other proposals can comply with the Act from the initial design and through later stages of implementation.

Term	Description/Definition
Privacy Notice	Advises individuals of what they can expect when an organisation collects their personal data, including what will be done with the information, and, for example, seeks the individual's permission to share it with others.
Processing	<p>Performing any operation or set of operations on data, including:</p> <ul style="list-style-type: none"> • Obtaining, recording or keeping data • Collecting, organising, storing, altering or adapting data • Retrieving, consulting or using data • Disclosing the data by transmitting, disseminating, sharing or otherwise making it available • Aligning, combining, blocking, erasing, deleting or destroying the data
Relevant filing system	Any set of information, while not computerised, is structured by reference to individuals, or by reference to a criteria relating to individuals, so that specific information is accessible.
Subject Access Request	Or SAR, is a legal means by which an individual can obtain a copy of their personal data that is held by a data controller. An organisation has 40 calendar days to reply. Data controllers can charge up to £10 for responding to a SAR.
Sensitive personal data	Data in specific categories which data controllers are expected to take greater care of, including information relating to an individual's racial origin (ethnicity), political opinions, religious or other beliefs, trade union membership, physical or mental health, sexual life, criminal convictions or the alleged commission of an offence.
SIRO	Senior Information Risk Owner – member of the CLT with particular responsibility for information risk across the Council.
SLT	The Council's Senior Leadership Team made up of all Service Managers.

Document Information

Project Name	Craven IMG Strategy
Version	0.4
Status	Draft
Date	25/01/2016

Purpose

The purpose of this document is to define the Information Management and Governance Strategy for Craven District Council for the period 2016-2018.

Distribution

Copy to	CLT
	SLT
	ICT Staff
	Lead member for Internal Services
	File

Document History

Version	Date of Production	Version Description	Author
0.1	14/12/2015	Initial Draft	DRN
0.2	14/12/2015	Updated Draft	DRN
0.3	18/01/2016	Updated Draft	DRN
0.4	25/01/2016	Minor amendments to objectives from review.	DM
1.0	22/03/2016	Released for publication following CLT review.	DM

Key Personnel

Author	David Roper Newman, Information Governance Officer
Contributors	ICT & Transformation Manager, CLT, SLT, Audit & Governance Committee
Reviewers	Paul Ellis, Director of Services Darren Maycock, ICT & Transformation Manager
Owner	Darren Maycock, ICT & Transformation Manager