# Information Governance Strategy

October 2018

| | |
|---|---|
| *Owned by:* | Daniel Bainbridge |
| *Created Date:* | April 2018 |
| *Equality Impact Assessment completed:* | May 2018 |
| *MB Approval Date:* | 29 May 2018 |
| *JCC Consultation Date:* | N/A |
| *Executive/Council Approval date:* | N/A |
| *Date for review:* | May 2019 |
| *Last updated* | 1 October 2018 |

## Contents

# INFORMATION GOVERNANCE STRATEGY

## 1. PURPOSE

This Information Governance Strategy is about how the Council creates, communicates, stores, uses and distributes the information we need to deliver our services and corporate objectives. It covers all information in all formats – paper and electronic (including graphical, audio and video files). The Strategy sets out the Council's principal aims in terms of ensuring that the Council manages and processes information in a lawful manner and in a way that supports service delivery.

This Strategy is part of a set of information governance policies and procedures that support the delivery of the Council's strategic approach to Information Governance, and should be read in conjunction with these associated policies.

This Strategy applies to both Council staff and Councillors.

This Strategy will add value to the information resources used by the Council and will promote efficiency. It will demonstrate that the Council has a commitment to providing high quality information and takes its role as a custodian of information seriously.

Information is different from every other resource – when it is produced and used, it increases rather than decreases. This brings risks – information overload, breach of confidentiality, multiple versions of information and documentation.

## 2. FOREWORD

### 2.1 Background

Public authorities rely on the collection of an ever-increasing amount of information to inform their strategies and plans to provide services.

Waverley Borough Council ('the Council') is no different in this respect and must have in place an effective framework for collecting, accessing, storing, sharing and deleting this information.

Moreover, the Council needs to be open in the way it does its business, in particular in how it delivers its services and in how it makes decisions. The Council must be in a position to provide easily-accessible and understandable information about its services and the decisions it makes.

Over the years, public authorities have been making increasing use of advancing technology: computing equipment in general, the internet, mobile phones and touch screens. Through making better use of these new technologies and more effective ways of working, this Information Governance Strategy sets out how the Council will manage the information that it has to best ensure that the Council is effective in providing services that its residents want, protecting that information whilst complying with its statutory and regulatory responsibilities, and also in demonstrating transparent and accountable decision making.

## 2.2 Context

This Information Governance Strategy has been developed in response to the legislative requirements in relation to the management of information in its various guises by organisations. A term which is being widely used by public authorities is Information Governance. It is a framework to bring together all of the requirements, standards and best practice that apply to the handling of information. It allows organisations and individuals to ensure that information is accurate, dealt with legally, securely and efficiently within certain regulatory and standards frameworks.

Although this document aims to focus on Information Governance it is at the same time talking about Information Management. These terms are often seen as interchangeable, although the governance element is more about ensuring compliance with rules and procedures, particularly if they are regulatory. Information Governance is also about how roles and responsibilities are defined and about what information functions there are.

Information Management is the means by which an organisation efficiently plans, collects, organises, uses, controls, audits, disseminates and disposes of its information, and through which it ensures that the value of that information is identified and exploited to the fullest extent.

Information is also evolving from different mediums e.g. social media. The Council needs to ensure that any information produced by its staff is created and managed in a secure and professional way.

There has been a raft of new legislation in recent years which has placed new obligations on local authorities. There are regulations which require us to provide information within given timescales, to make information more accessible and to guard people's rights. In order to comply we must ensure we manage our information effectively, taking into account these new legal requirements. Below is a list of recent legislation which affects some or all services and are drivers for Information Governance:

- General Data Protection Regulation
- Data Protection Acts 2018 and 2008
- Human Rights Act 1998
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Local Government Acts 1972 to 2003
- Electronic Communications Act 2000
- Regulation of investigatory Powers Act 2000
- Consumer Protection Regulations 2000
- The Electronic Commerce Directive
- Re-use of Public Sector Information Regulations 2005

In order to comply with legislation and to ensure the Council manages its valuable information assets effectively, it is important to set out a strategic and corporate approach to Information Governance that becomes a shared vision across the whole

organisation. The strategy set out in this document will deliver a direction and framework in which to operate, and a platform from which the Council can further improve its services in a more cohesive manner through the improved provision of, and accessibility to, information held by the Council.

## 3. VISION

The vision is about **connecting people with the information they need whilst also keeping it safe and secure over its life-cycle** in order to protect our residents, customers, businesses and staff**.** Achieving this is critical to the Council's success.

Information Governance is at the heart of the way in which the Council delivers services to the public. If the Council does not have consistent and accurate information it cannot optimise its efficiency or measure improvements.

## 4. PRINCIPLES

**Available** – Our information will be available to those who need it, when they need it and to those who have the permissions to view or use it. This will include responsiveness to requests for information. We will avoid information overload and target information where it is needed

**Accessible** – Our information will be clearly identified and easily found when it is needed, in a timely fashion, by anyone with authority who needs to access it. We will maintain a clear information structure. We will share and exchange information efficiently where necessary.

**Electronic** – Our information and documents will be stored electronically. Over time, we will evolve our policies such that we will endeavour to only keep paper records where there is a legal requirement to do so.

**Secure** – We will ensure that there are controls in place when we store and transfer information, so that the information itself is protected and any risks associated with inappropriate disclosure are reduced. We will record the confidentiality of information. Non-confidential information will be openly published where required.

**Managed throughout its lifecycle** – It is essential that information is only kept for as long as necessary, whether it is through a legal requirement or a business need. Information when it is no longer required should be disposed of in a secure manner in line with our Records Retention and Disposal policy.

**Information assets** – We will make full use of our information assets and keep them safe.

**Generate an information culture** – Information should be managed in a common structured system. This encourages collaborative working and reduces duplication of work.

**Training** – Implement a training programme to enable staff to manage, share and work with information in a corporate way to ensure all of the above.

## 5. INTRODUCTION

Information, in all its forms, whether electronic, paper-based or in people's heads, is one of our critical resources. This Information Governance Strategy will act as the overarching strategy that governs all of the Council's documents in Section 9.

Information is a corporate resource to be shared and used as effectively as possible, it is **not** owned by the individual who created it but by the Council. 'Information' is distinct from 'data'. Whereas 'data' is any word, number, character or text without context and of little meaning to an individual, 'information' is data that has been processed in order to give it structure and meaning.

Security, sustainability and privacy are concepts the Council will always consider when producing or working with information.

Information Governance covers a vast scope. We can never expect to achieve perfection, but we have scope to improve our services by a range of improvements to our policies, frameworks, technology and training, and by seeking to promote a culture which recognises and delivers our information management vision. Failure to manage information properly exposes the Council to a significant financial, legal and reputational risk.

When reviewing or implementing technologies, Information Governance should be a principal consideration.

## 6. OBJECTIVES OF INFORMATION GOVERNANCE

The objectives of this Information Governance Strategy are:

- To instil an understanding of the importance, and an appreciation of the potential, of effective information governance.
- To help develop awareness, understanding and to promote the application of good practice in handling information, and develop skills in this area.
- To define what the Council considers are the principles and practice of good information management and to reduce risk.
- To identify the changes and investments needed to deliver the Council's vision of connecting people with the information they need whilst also keeping it safe and secure over its life-cycle.
- To support the Council's ambition to improve processes, to improve customer services, to become more efficient and to reduce costs.
- To ensure that the Council takes advantage of technology advances appropriate to conducting the Information Governance processes within the Council.

- To ensure business continuity and protect vital records to ensure the continued functioning of the Council if any disasters affect the Council.

## 7. RESPONSIBILITIES

### 7.1 The Council

Overall responsibility for the efficient administration of the Information Governance lies with the Council. An Information Governance Board has been created, chaired by a Director and consisting of senior officers with key functions to play in strategic oversight of the Council's Information Governance Strategy (including the Senior Information Risk Owner and IT Development Manager). Below the Information Governance Board sits the Information Governance Group with senior representatives from all service areas and which is responsible for practical implementation of the Council's strategic Information Governance actions.

### 7.2 Senior Information Risk Owner

As the governance of information and the protection of personal information are so important a senior member of staff is appointed as the Senior Information Risk Owner to oversee and ensure compliance with the Council's information governance responsibilities. The SIRO is responsible for ensuring that information governance is embedded into the organisation to ensure that the potential risks to corporate information and records are mitigated. It has been agreed that the Borough Solicitor will be the SIRO.

### 7.3 IT Development Manager

The IT Development Manager will be responsible for:

- Providing operational work and support including training, query resolution, incident support and legal compliance requirement.
- Security of the Council network and infrastructure.

### 7.4 Information Champions

These are members of staff within service areas who will liaise with the SIRO and the Data Protection Officer on all matters concerning administration of the Strategy. It is suggested that there will be at least one representative from each service area. In particular they will assist where necessary in ensuring compliance in respect to information management systems and ensuring awareness of the need for information governance within their agreed remit. This applies particularly to Personal Protected Information.

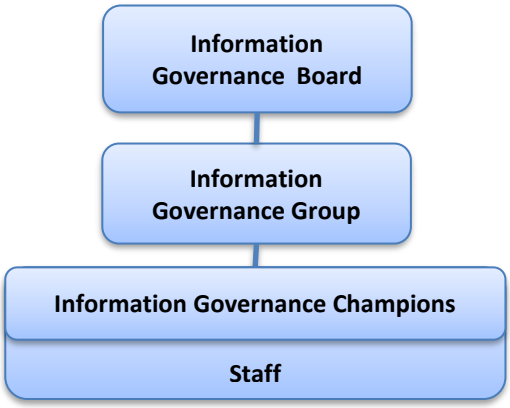
## 7.5 Managers

Managers are responsible for ensuring that staff under their direction and control are aware of the policies, procedure and guidance laid down on Information Governance and for checking that those staff understand and appropriately apply policies, procedures and guidance in respect of information Governance in carrying out their day to day work.

## 7.6 Staff

It is the responsibility of all staff to process information in accordance with the General Data Protection Regulation, and all other relevant data protection legislation, and to adhere to the policies, procedures and guidance that are laid down by the Council for information governance and security.

## 7.7 Information Governance Structure




The structure set out above will be used to embed the information governance principles at section 4 within the organisation, supported by regular training of Officers and Councillors and regular monitoring and updating of the various supporting policies and procedures set out at section 9 below.

# 8. INFORMATION GOVERNANCE REQUIREMENTS

## 8.1 Information Rights

Information Rights is a global term for Freedom of Information, Environmental Information Regulations and Data Protection. They are statutory functions and the information needed to comply with requests under these rules has to be gathered from across the Council. It is therefore essential that all our systems can be accessible and searchable to retrieve the information needed. Part of the Freedom of Information Code of Practice acknowledges that information is not held if it is managed in line with retention and disposal schedules.

We need to ensure we comply with these regulations and guidance from the Information Commissioner's Office to minimise the number of complaints it receives.

There needs to be policies on each of the areas and staff be made aware of their responsibilities as part of on-going training.

## 8.2 Information Security

Ensuring the security of the Council's information, both from internal and external sources is paramount. As well as information being available to the people who need it, it also needs to be protected from those who should not use it. As part of Information Governance the Council has an ICT Security Policy which covers all business functions and information contained on the Council's IT network and the relevant people who support that network.

Information Assurance is managing information-related risk. As part of Information risk there needs to be an information risk register. Examples of information risk which should be assessed include whether disaffected staff could do damage to information systems if they are given access to them or the risks associated with information falling into the wrong hands.

**Egress Email Encryption Software** enables secure data sharing. Egress Switch is provided by a company called Egress and is a secure email solution which allows the Council to send emails and file attachments securely and encrypted to third party recipients. Egress Switch enables third parties to communicate safely with the Council.

**Government Connect** (GCSX) enables secure data sharing up to Restricted level across Government. It is a key enabler of joined up working and shared services. To be a member of this community we have to instigate a number of procedures including Protective Markings. There is an annual process of accreditation we have to undertake to continue using Government Connect.

Rightly, much publicity has been made about the loss of sensitive data from public authorities. Residents, customers businesses and staff should all expect that any personal information given to the Council is stored and transferred when necessary safely and securely. Guidance has been published regarding data protection and information governance and the recommendations must be implemented across the Council. This includes appointing a Senior Information Risk Owner ("SIRO") and ensuring staff understand through training and guidance their responsibilities when handling personal information.

## 8.3 Email Management

Email has become an important part of the recording of decisions within the Council. It is important that the email lifecycle is correctly and securely managed. It must be treated as a business communication and not simply a tool. An email management policy exists as part of our overarching policy for use of information and communications technology by staff. All new and existing staff are trained in email management. Guidance will be given to staff and Councillors individually and also on the Intranet. As part of the email management policy staff must manage their emails

as they would documents. Emails will be deleted after five years. If they are needed as records and to comply with different retention and disposal schedules they must be moved out of Outlook.

## 8.4 Audit

It is essential for Information Governance that the Council routinely reviews the secure retention and handling of data. These considerations are integral to Internal Audit assignments. Each year, a risk-based Internal Audit plan is produced and the audit areas listed are reviewed over the financial year. This plan includes IT audits, covering such areas as network maintenance, disaster recovery / business continuity plans, servers, backup procedures etc.

In addition, Internal Audits included in the plan cover areas such as:

- Use of data (covering how and why data is collected, stored and used)
- Document Management systems
- Compliance with Data Protection and Freedom of Information legislation
- Compliance with the corporate document disposal policy

either as specific areas for audit review or as an integral part to other audit work.

The Internal Audit Client Manager (whether this be an employee or third party contracted to undertake that function) informs the Senior Information Risk Owner of any breaches and hardware failures affecting the loss or misuse of data identified as part of such an audit. They decide which other members of the Information Governance Board are to be informed, considering issues such as confidentiality and possible fraud investigations (if there needs to be an investigation (and particularly if there were any possibility of wrongdoing occurring)).

Also the Council should regularly undertake an **information audit** (separate to the Council's Internal Audit function) which identifies where information is located, its flow and how accessible it is. It should also look at the information needs of the Council and compare them with the systems that are in place to meet those needs and see if there are any gaps. It would be useful to help in assessing an information strategy's success as it can be used as a performance measurement. It is important when doing an information audit to match it against the organisation objective. As well as investigating the information needs of Waverley, the audit also needs to record the Council's information assets. As part of the Freedom of Information publication scheme and also a need for greater transparency there is a requirement for an information asset register. The Information Governance Board will set out guidelines for when such audits should take place.

## 8.5 Records Management

According to ISO 15489: 'Information and Documentation – Records Management' a **record** is information which is created, received and maintained as evidence and

information by an organisation or person, in pursuance of legal obligations or in the transaction of its business. A record is a primary source of information.

**Records Management** is the field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records.

**Retention and Disposal** is about managing the lifecycle of a record. As well as creating documents there is a need to decide how long a record is kept. Both the Freedom of Information Act 2000 and the Data Protection Act 2018 require that data should be kept for no longer than is necessary for the purpose it was created. If we destroy documents in line with the Council's retention and disposal policy then if requested in the future, there is no retort on the Council. Conversely, if the Council still held the documents, but should have destroyed them, then they are required to be disclosed. Some legislation states how long a record should be kept; other retention periods are devised from guidance or departmental policy.

Retention and disposal policies are applied to the information and not the media in which it was created e.g. Word documents, emails.

The Council's current retention and disposal policy was last revised and approved in April 2018 and is generally revisited annually. Retention and disposal schedules should be applied to all documents.

## 8.6 Training

Training is at the core of Information Governance. It is important that at all stages, staff and Councillors are fully aware of their responsibilities when it comes to managing information. Policies and procedures can be put into place but it is the responsibility of all to understand that the information they create and use is the property of the Council and is not just for here and now but as part of the corporate memory. Information and particularly personal information is an important resource. Many data losses are not done deliberately but they can have serious consequences. Councillors and staff must be made aware on how to handle information correctly. The Information Commissioner's Office is being given greater powers to investigate any data breaches.

Training will be delivered in a variety of different formats including face to face, induction and the intranet. All staff training will be monitored and recorded centrally by the Council’s Human Resources team in order to ensure that training is completed by all staff as and when it is required. Councillor training will be monitored and recorded by the Democratic Services team.

## 9. MONITORING COMPLIANCE WITH AND THE EFFECTIVENESS OF THIS INFORMATION GOVERNANCE STRATEGY

Compliance with this Strategy will be monitored through its associated policies and procedures as listed below:

- Information Management Policy
- Records Retention and Disposal Policy
- Email Management Policy
- IT Acceptable Use Policy
- Data Protection Policy
- Freedom of Information Policy
- Subject Access Request Procedure
- Staff Code of Conduct
- Photography Guidelines
- Telephone Policy
- Data Breach Procedure
- Relevant sections within the Council's Constitution
- Business Continuity Plan