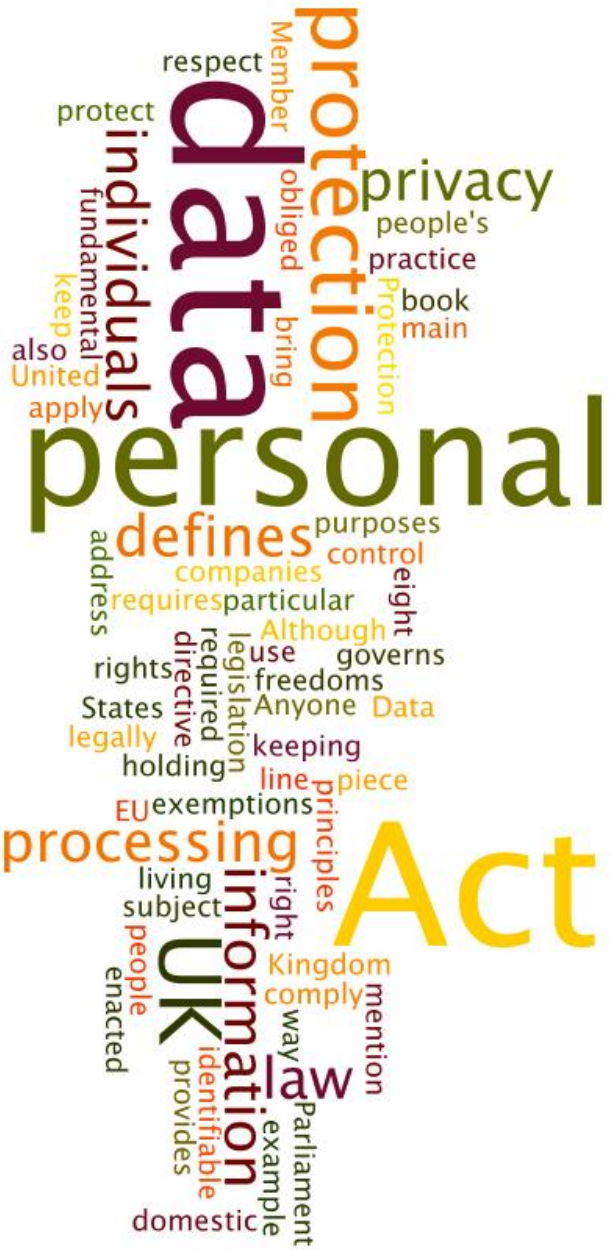
Warwick District Council

Information Governance Management Framework



Version: 1
Date Issue: April 2018
Next Review date: Issue date plus 12 months
Team Owners: Democratic Services
Protective Marking: Official

Contents

Approvals

Executive	5/4/2018

Review

V	N/A		

Author: Democratic Services Manager & Deputy Monitoring Officer

1. Introduction

1.1 Information is a vital asset for the provision of services to the public and for the efficient management Council services and resources. As well as protecting confidentiality and ensuring rights to access public and personal information, it plays a key part in governance, service planning and performance management.

1.2 Information governance is concerned with how information is held, obtained, recorded, used and shared by the organisation to achieve compliance with information governance laws and current best practice.

1.3 Information is used here as a collective term to cover terms such as data, documents, records, web content, images and biometric data.

1.4 It is essential that the Council has a robust information governance management framework, to ensure that information is effectively managed with accountability structures, governance processes, documented policies and procedures, staff training and adequate resources.

2. Senior Roles

2.1 Executive and Portfolio Holder

The Executive is the lead Councillor body responsible for ensuring governance and decision making within Council policies. The Leader as Portfolio Holder for Strategic Leadership has specific service responsibilities and this includes the Democratic Services team, who lead on information management, and IT.

2.2 Chief Executive and Corporate Management Team

The Chief Executive is the Head of Paid Service who leads the council's staff and advises on policies, staffing, service delivery and the effective use of resources. Together with Deputy Chief Executives they form the council's Corporate Management Team ensuring delivery of an effective council-wide information governance approach.

2.3 Senior Information Risk Owner (SIRO)

The Senior Information Risk Owner (SIRO) is overall responsible for managing information risk in the council and is a member of the Senior Management Team. The SIRO is the Deputy Chief Executive & Monitoring Officer and:

- ensures information governance compliance with legislation and council policies
- provides a focal point for managing information risks and incidents
- prepares an annual information risk assessment for the council.
- fosters a culture for protecting and using information within the council

2.4 Information Asset Owners

Heads of Service are designated Information Asset Owners and are responsible for the management of information risk for their service's information assets. This includes ensuring that their information assets are properly recorded in the Council's information asset register.

3. Key Policies

3.1 The key policies in the framework (shown below) are:
- The Data Protection Policy – aimed at all staff
- Information Rights Policy – aimed at the public
- Information Security & Conduct Policy – aimed at all staff

3.2 These policies are supported by sub-policies, standards and procedures are shown in the framework diagram. Outputs will be produced from use of these standards and templates, for example privacy assessments, awareness guides and training material.

4. Key Governance Body – Senior Management Team

4.1 The Senior Management Team's (SMT), which comprises of the Chief Executive, Deputy Chief Executive's and Heads of Service, will have information governance responsibilities are to:

- Approve and ensure a comprehensive information governance framework, policies, standards, procedures and systems are in place and operating effectively throughout WDC.
- Prepare the annual Information Governance Assessment and update the Information Risk Assessment, including action plans.
- Coordinate Information Governance compliance and improvement activities (DP, FOI/EIR, security, quality, and records management) across WDC.
- Monitor information handling and breaches, implement assurance controls (including regular audits) and take corrective actions
- Ensure training and action plans for information governance are progressed throughout WDC, evaluate the impact and effectiveness of governance training.
- Communicate the information governance agenda

4.2 The Group will meet as part of the regular SMT agenda and for the relevant items the Senior Information Risk Owner, Democratic Services Manager, ICT Services Manager, and Information Governance Manager, or their nominated deputy, will also attend the meeting.

4.3 They will also receive advice and guidance from Internal Audit, Legal Services, and other relevant organisations and officers as they require.

5. Resources

5.1 The Information Governance Manager will provide expert advice and guidance to all staff on all elements of Information Governance. The team is responsible for:
- Providing advice and guidance on information governance to all staff.
- Developing the Information Strategy, Information Governance Framework of policies, standards and procedures and the Information Governance Improvement Plan.
- Working with Information Asset Owners (and their representatives) to establish protocols on how information is to be used and shared.

- Developing Information Governance awareness and training modules for staff.
- Ensuring compliance with Data Protection, Freedom of information, Records Management, Information Security and other information related legislation via the regular information audit and register of processing activity update.
- Providing guidance and advice on Privacy Impact Assessments.
- Coordinating and processing corporate information requests, processing requests on behalf of business units and supporting information coordinators in other business units.
- Integrating Government and Information Commissioner guidance, policies and codes of practice
- Providing support to the Senior Information Risk Owner for internal Information Governance related issues.

5.2 The ICT Management team is the lead for technical security management of the infrastructure and technical security advice, including areas such as: PSN Code of Connection, PCIDSS and device policy.

5.3 The Legal Services team provide expert legal opinion on all information governance matters to all service teams.

5.4 There will be identified roles in the Service Areas whose role includes some aspects of information governance and ensuring compliance. These will vary according to the services provided.

6. Governance Framework Responsibilities

6.1 Service Area Management Teams

They are accountable for the effective management of information risk and information governance compliance, as well as supporting and promoting the policies, standards and procedures. The teams comprise of the Heads of Service and Managers for each service area.

6.2 Heads of Service

Each is an Information Asset Owner who is accountable for information assets within their business unit. They are able to understand how it is held, used and shared and address risks to the information. They are responsible for updating the Register of Processing Activity as required and at least annually.

6.3 Council Managers

Managers are responsible for the implementation and adherence to this policy framework and any associated standards and procedures within their service and teams.

6.4 Other Parties

Disregard for information governance policies by employees may be regarded as misconduct to which the council's Dismissal and Disciplinary Procedure applies and a serious breach of any policy may be treated as gross misconduct and may lead to dismissal.

Disregard by contractors and agents working for the council will be regarded as a contractual breach. Disregard by volunteers and work experience

students working for the council may lead to terminating their work agreement.

7. Training and guidance

7.1 Information Governance training for all staff will be mandatory as part of induction, to include all employees, secondees, agency and voluntary staff. This will be through e-learning modules that are accessible on any device.

7.2 Further modules as appropriate to the role will be available through e-learning or classroom session, developed internally or through recognised providers, for example the NHS.

7.3 All staff will be required periodically to complete update/refresher training.

7.4 Awareness sessions may be given to staff as required, at team meetings or other events.

7.5 Regular reminders on information governance topics are made through corporate and local team briefings, staff news and emails.

7.6 Policies, procedures, standards and advice are available to staff at any time on the Information Governance pages.

8. Information Security Incident Reporting

8.1 The Information security incident reporting procedure is available to all staff, and is available for download. All information security incidents involving digital or manual records whether actual or suspected, should be promptly reported to the ICT Services' Helpdesk via an individual's line or Service Area Manager, or to the Democratic Services Manager and Deputy Monitoring Officer.

9. Monitoring and review

9.1 This policy and the supporting standards will be monitored and assessed annually in line with legislation and codes of best practice and subject to audit review.

9.2 An Equality Impact Assessment/ Analysis on this policy was undertaken on ? and will be reviewed each time the policy is updated, or before if required.

10. Further Information

Democratic Services Manager, Riverside House, Milverton Hill, Royal Leamington Spa, CV32 5HZ
Telephone: 01926 456114

Appendix 1 Information Governance Framework

	IG Management	Confidentiality	Access to Information	Information Security	Records Management	Data Quality
Policies (Executive or Employment Committee approval)	Information Governance Framework	Data Protection Policy	Information Rights Policy	Information Security & Conduct Policy Information Security Incidents and Breaches Policy	Records Management Policy	Data Quality Policy
Sub-Policies (SMT approval)	N/A	Privacy Impact Assessments	Freedom of Information Act Publication Scheme	Information Asset Register Monitoring Policy (Electronic communications) Removable Media Policy Remote Working Policy Email Acceptable Usage Policy	Data Retention Sub-Policy Data retention Schedules	To be confirmed during 2018/19

				Internet Acceptable Usage Policy Data Handling Policy Software Policy Digital Forensics Readiness Policy GCSx Acceptable Usage policy Human resources Information Security Policy Information Risk Classification Schemes Physical Environmental Security Policy		

Training and Awareness	There will be a planned approach to training and awareness for each policy. This will be role based, regularly assessed and should equip each person to fulfil their responsibilities. **For example Requests for Information – A Quick Guide**

Procedures	N/A		Requests for information			
New and Changed Systems	N/A					
Compliance	There will be a timely and effective monitoring, reporting and compliance regime through, ¼ reports SMT and Annual reports through the Service Area Plans and Portfolio Holder statements as well as being a monitored feature within internal and external audits.					

Appendix 2 - External Legislation and Regulation

Data Protection Act 1998
Human Rights Act 1998
Freedom of Information Act 2000
Environmental Information Regulations 2004
Local Government Acts
Copyright, Design and Patents Act 1998
Computer Misuse Act 1990
EU Data Protection Regulation (GDPR) 2016 (applicable from 25 May 2018)
Privacy and Electronic Communications Regulations
CCTV - Code of Practice / Commissioner