Information Commissioner's Office

Information governance strategy 2014-16

ico.
Information Commissioner's Office

Contents

1.0 Executive summary

This strategy describes the ICO's information governance aims and deliverables for the next two years.

It confirms the ICO's commitment to compliance with information rights legislation. It also confirms our commitment to good practice through the implementation of, and adherence to our own guidance.

It sets out an approach that will deliver all of the essential compliance elements, in a way that also actively enables and supports the delivery of corporate objectives, and exploits opportunities for business benefits. It is an approach that will be flexible and responsive to new or changed operational requirements, and that will enable the organisation to take proportionate risk.

It demonstrates how effective information governance can help us to make the best use of our information, and as a consequence, assist in the delivery of our objectives and the improvement of our business processes.

It is an approach which will further our corporate objectives to be open and transparent about what we do, and to be accountable for the actions we take. It will give confidence to those who provide personal information to us that their information will be managed appropriately.

The Information Governance team will set out and communicate our information governance strategy and champion the information governance agenda. Engaging with business areas across the ICO it will ensure that corporate information governance policy is reviewed and that it properly aligns with business and operational requirements. The team will work with, and provide specialist advice and support to our staff and Information Asset Owners (IAO). The Information Governance team will actively engage with the Good Practice teams to share experience and examples of good practice and to ensure that messages conveyed externally are consistent with our internal processes.

This strategy excludes the ICO's obligations in relation to the handling of information requests made to the ICO under the Data Protection Act 1998 and the Freedom of Information Act 2000.

2.0 Introduction

This strategy covers the period 2014-16 and describes the continuing development, implementation and embedding of a robust information governance framework needed for the effective management and protection of the ICO's information.

Information governance describes the approach within which accountability, standards, policies and procedures are developed and implemented, to ensure that all information created, obtained or received by the ICO is held and used appropriately.

The ICO has a responsibility to manage and protect a wide range of information including:

- information provided by individuals relating to their concerns about how their personal information has been processed;
- information obtained by the ICO during the course of our investigations;
- information obtained in order to produce a public register of data controllers;
- information about our development of policy and guidance;
- information obtained during the audit process; and
- information which supports the running of our organisation including records relating to staff and our IT.

3.0 ICO corporate plan 2014-17

In the corporate plan 2014-17 the ICO describes its goal as achieving a society in which all organisations who collect and use personal information do so responsibly, securely and fairly. We want all those who handle information:

- to routinely meet their legal obligations in the way they respond to people exercising their rights;
- to have a high level of awareness of all their wider obligations under information rights law with those obligations routinely met in practice; and

- to ensure that good information rights practice is embedded into the culture and day to day processes of organisations and into emerging technologies and systems.

In our corporate objectives we commit to continually reviewing and improving our own compliance with information rights legislation underpinned by our value of being a model of good practice and not asking others to do what we are not prepared to do ourselves.

This information governance strategy is a clear statement of the ICO's commitment to compliance with information rights legislation and demonstrating good practice. It demonstrates our investment and support for this business priority.

The strategy describes our commitment to ensuring effective information governance as a means to enable our business, to ensure we can make the best use of our information and to provide a solid foundation to enable us to be open and transparent about what we do.

At the same time it takes account of, and supports the ICO's operational objectives and ensures that a balance is struck between operational and compliance objectives.

4.0 Regulatory environment

The context in which the ICO operates is unusual. We are subject to the laws for which we are responsible being a data controller with obligations set out in the Data Protection Act 1998 and a public authority with obligations under the Freedom of Information Act 2000. We are in effect our own regulator.

The legal and regulatory framework is outlined below and includes:

The legislation regulated by ICO:

- The Data Protection Act 1998
- The Freedom of Information Act 2000
- The Environmental Information Regulations 2004
- Privacy and Electronic Communications Regulations 2003

Other related legislation:

- The Public Records Act 1958
- The Re-use of Public sector Information Regulations 2005
- Computer Misuse Act 1990

- Regulation of Investigatory Powers Act 2000

Related guidance and codes of good practice:

- Security Policy Framework (Cabinet Office).
- Public Service Network (PSN) Code of Connection.
- The ICO's published guidance and codes of practice.

We will continue to monitor the progress of any new EU data protection regulation or changes in UK law and respond promptly to any change.

5.0 Scope

This strategy includes within its scope:

- management of the life cycle of the ICO's records and information from creation or receipt to disposal or transfer to The National Archives for permanent preservation;
- information security; and
- the collection, management and use of personal information created, received or obtained by the ICO.

This strategy excludes the ICO's obligations in relation to the handling of information requests made to the ICO under the Data Protection Act 1998 and the Freedom of Information Act 2000.

Contact details for the information access team are provided here (internal link only) and are also on our website.

6.0 Information governance aims

The ICO's six information governance aims are outlined here. Deliverables to support the achievement of these aims are described in section 7.0. Achievement of these aims will deliver essential compliance elements but will also enable and support our business and deliver business benefits.

6.1 Policy

We will implement information governance policies which are embedded in the day to day operations of the ICO and which are compliant with relevant legislation, standards and codes of practice and demonstrate good practice.

We will implement risk based information governance policies which are clear, accessible, and flexible and aligned with business requirements.

6.2 Awareness

We will ensure that there is a high level of staff and supplier awareness of information governance policy and processes to help achieve compliance and to reduce the risk of non-compliance through human error.

We will foster a culture of personal responsibility, ownership and commitment to high standards in information handling to support and enable our business processes.

6.3 Monitoring and assurance

We will ensure that there are processes in place to check whether information governance policy is being implemented and to measure the effectiveness of the control environment.

We will work with the business areas and Information Asset Owners prompting feedback about the practical operation of policy. We will respond and make changes where necessary. The Information Governance team and Good Practice teams will work together to share experience gained internally and externally and to maximise the opportunity to learn from examples of good practice. We will work with the Good Practice teams to assess our effectiveness in implementing the ICO’s own published guidance.

6.4 Records and information management

We will ensure that effective processes are in place to manage our records and information. From creation or receipt through to disposal, we will meet our obligations under the Public Records Act and the records management guidance set out in the code of practice issued under s46 of the Freedom of Information Act.

The effective management of our records and information will ensure that we know what information is available to us and where it is stored. It will enable us to promptly retrieve information, saving time, effort and electronic and physical storage space. It will also enable us to respond promptly to information requests, and through the timely publication of information, increase our openness and transparency about what we do.

6.5 Information security

We will implement information security policies which take account of legislative requirements, HMG guidance and the codes of connection we are subject to, but which are appropriate, proportionate, measured and part of business as usual.

We will work with the business areas to ensure that information security policy is aligned with operational requirements finding solutions appropriate to the ICO's risk appetite. We will support our staff by ensuring that information security policy and processes are clear and accessible, that help and guidance are available when needed, and by providing appropriate training to minimise the risk of human error.

6.6 Collection and use of personal information

Personal information received or obtained by the ICO is managed and used responsibly, securely and fairly.

We will promote transparency and openness about how we handle personal information providing confidence to the individuals and third parties who pass personal information to us.

7.0 Deliverables

The deliverables to support the achievement of the ICO's information governance aims over the next two years are outlined here.

7.1 Policy

	Delivering compliance	**Business benefits and opportunities**
A review of all information governance policy	Policies which achieve legal compliance, demonstrate good practice and are in accordance with the ICO's own published guidance	Opportunities for the business to input to the review process and to ensure that revised information governance policy is clear and fully aligned with business and operational requirements

7.2 Awareness

	Delivering compliance	**Business benefits and opportunities**

Communication and promotion of the revised information governance policies to IAO's, staff and third parties who work with the ICO	High levels of awareness to minimise risks of non-compliance through human error	Information tailored to job roles and business processes
Developed and implemented training programme for IAOs	Local ownership and accountability for information governance issues driving compliance	Development opportunity for individuals and the opportunity to develop an IAO forum to discuss and share experience and good practice
Designated information security and records management weeks to raise awareness and prompt discussion	Increasing awareness to minimise risk of human error and non-compliance	Opportunity to raise issues, share experience and seek clarification

7.3 Monitoring and assurance

	Delivering compliance	**Business benefits and opportunities**
A developed and embedded integrated assurance framework as part of business as usual with twice yearly self-assessments.	A tool to provide assurance to the SIRO and audit committee and to monitor compliance	Structured opportunity for IAO's to consider information governance compliance. An opportunity to identify and address corporate issues identified by IAO's
A review of the pre-employment personnel security check process and the adoption of any recommendations.	Appropriate organisational measures in place to satisfy the requirements of principle 7	Reduced risk of employing inappropriate staff potentially saving time and costs
A review of IT processes including taking and storing IT back up media and the disposal of IT equipment and the adoption of any	Appropriate technical and organisational measures are in place to satisfy the requirements of principle 7	Confidence that information will be available to the business when required and information will be securely disposed of when no longer required

recommendations.		
Physical security measures are tested, validated and assured by audit.	Appropriate technical and organisational measures are in place to satisfy the requirements of principle 7	Reassurance to staff about their safety in the workplace and minimising the risk of security incidents interrupting business continuity

7.4 Records and information management

	Delivering compliance	**Business benefits and opportunities**
Compliance with the retention and disposal schedule for non-casework records	Supports compliance with principles 3,4 and 5 and the code of practice issued under s46 of FOIA	Easier, quicker access to current records and information saving time and effort and making best use of electronic and physical space.
Well defined records and information management requirements fed into the project to replace Meridio	Ensures replacement system is capable of compliance with relevant legislation	Opportunity to use the business experience and lessons learned from our first EDRMS implementation to feed into and influence the requirements for a replacement system.
Procedures developed for the annual transfer of records to the National Archives	Meeting our obligations under the Public Records Act	Promotes our commitment to transparency and, openness. Opportunity to ensure the process for selecting records for transfer is clear and minimises future work to review records
Report on the issues which the ICO needs to address regarding digital obsolesce.	Meeting our obligations under the Public Records Act	Ensuring business continuity and future proofing our information
Paper files are being stored and managed in accordance with the ICO's policy	Supports the implementation of S46 guidance (FOIA) and satisfies the requirements of	Ease of access to information and prompt retrieval when required. Making best use of physical space.

	principles 3,4,5 and 7	
Naming conventions are consistently applied to the ICO's records and information	Supports implementation of S46 guidance (FOIA) and supports the handling of information requests	Information can be located promptly when required and best use can be made of the information we hold
The roles of the Local Records Officers and Local Records Officer Forum are refreshed	Supports delivery of compliance with all relevant legislation	Opportunity for staff to develop new skills, to share experience and good practice and to promote the benefits of good information management at the local level.
Promote transparency and openness through the timely publication of the ICO's information	Supporting the principles of openness and transparency set out in the FOIA	Helps to manage the expectations of stakeholders, provide information and insight into our operational activities and save time by avoiding repeat information requests

7.5 Information security

	Delivering compliance	**Delivering business benefits**
Embedded new Government Classification Scheme (GCS) with good awareness of and implementation of the handling guidance for all types of the ICO's information	Satisfying the requirements of principle 7 and the Security Policy Framework	Clear straightforward baseline controls reducing complexity
Implementation of secure email or the right tools for secure information sharing	Satisfying the requirements of principle 7	Providing a secure mechanism for sharing information with third parties
Review of current arrangements for secure mobile working	Satisfying the requirements of principle 7	New opportunities to consider and improve the business experience of mobile working.

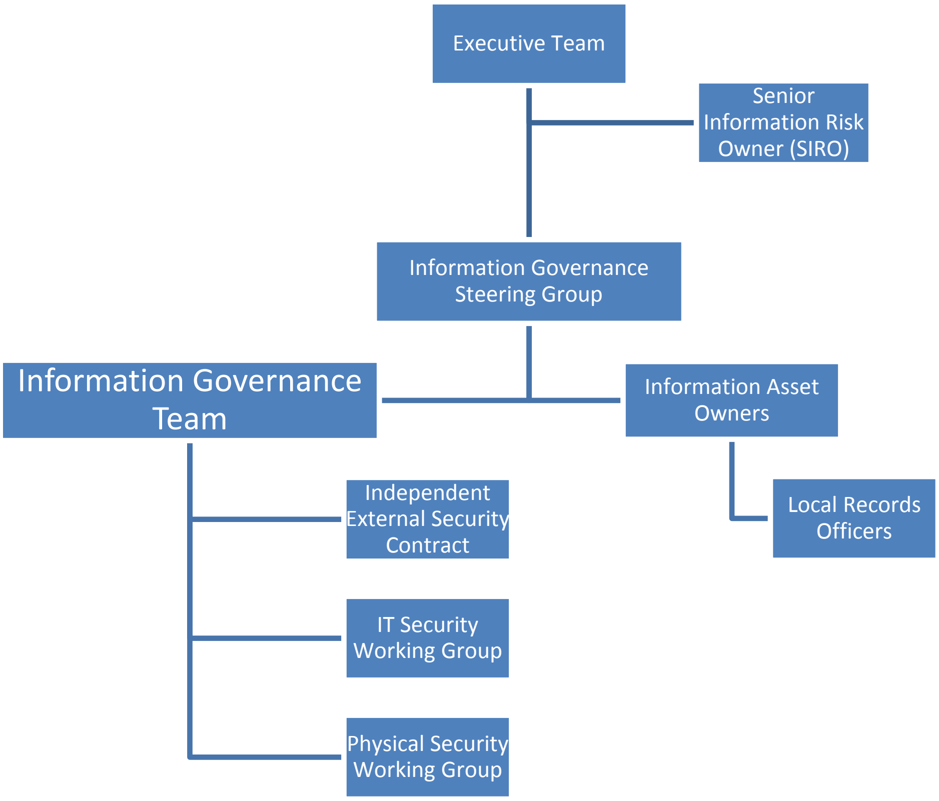
A physical security review of the off-site storage facility with any recommendations adopted	Satisfying the requirements of principle 7	Ensuring business continuity with information being available when required
A fully tested secure IT disaster recovery solution to ensure the continued availability of the ICO’s information in the event of an incident	Satisfying the requirements of principle 7	Ensures the continued availability of the ICO’s information in the event of an incident.
Successful annual PSN code of connection return and annual RMADS accreditation	Satisfying the requirements of principle 7 and the PSN code of connection	Continuity of external email and connection to the internet
Processes for ensuring that IT access is provided on a need to know basis are working effectively	Satisfying the requirements of principle 7	Licence costs could be reduced, opportunities for improved productivity if staff only have access to applications and software required to carry out their role.

7.6 Collection and use of personal information

	Delivering compliance	**Delivering business benefits**
Information governance requirements are considered in any new or changed IT systems, business processes or new initiatives which involve the collection and use of personal information and privacy impact assessments are carried out where necessary	Satisfying the requirements of principle 1	An opportunity to build in information governance considerations at an early stage saving time and costs and giving confidence to data subjects by ensuring that privacy impact assessments have been carried out where necessary
The ICO is clear about how it uses and manages the	Satisfying the requirements of	Gives confidence to individuals and third

personal information captured as a consequence of carrying out its statutory functions	principle 1	parties that the ICO is properly managing and protecting the personal information which it handles

8.0 Information governance roles and responsibilities


Executive Team
Senior Information Risk Owner (SIRO)
Information Governance Steering Group
Information Governance Team
Information Asset Owners
Independent External Security Contract
Local Records Officers
IT Security Working Group
Physical Security Working Group

8.1 Senior Information Risk Owner (SIRO)

The ICO's SIRO is the Director of Corporate Services who is a member of the ICO's Executive Team. The SIRO has responsibility for sponsoring and promoting information governance policy.

8.2 The Information Governance Steering Group (IGSG)

The IGSG is chaired by the SIRO. The responsibilities of the IGSG include:

- agreeing information governance policy;
- considering any lessons learned;
- monitoring progress on the delivery of the information governance strategy;

- identifying information governance risks and ensuring appropriate mitigation is in place;
- ensuring any issues relating to the regional offices are addressed; and
- identifying and discussing any new business initiatives which may have information governance impacts.

The membership of the group is the Director of Operations, the Head of Good Practice, the Head of IT, the Information Governance Group Manager and as agenda items dictate the Information Asset Owners, the Information Security Manager and the Lead Records Management Officer.

8.3 The Information Governance team

The Information Governance team is located within the Good Practice department under the leadership and direction of the Head of Good Practice. The team consists of the Information Governance Group Manager, the Information Security Manager, the Lead Records Management Officer and the Information Governance Officer providing support to the team.

The team is responsible for:

- the development and implementation of an effective strategy to deliver sound and compliant information governance practices across the ICO;
- the development and promotion of information governance policy;
- ensuring the ICO’s Information Asset Owners (IAO’s) are aware of and understand the information governance strategy and policies, and have a good understanding of their role and responsibilities;
- providing advice and assistance to the IAO’s to ensure that local procedures are in place to underpin and implement information governance policy;
- leading and coordinating the work on the ICO’s Integrated Assurance Framework which provides assurance relating to the effectiveness of the ICO’s information governance control framework and to mitigate corporate risk;
- to ensure there is awareness of the policy for managing security incidents, ensure any incidents are logged, investigated and recommendations implemented;
- maintaining positive relationships regarding information governance matters with relevant external bodies eg TNA, Cabinet Office, CESG; and

- providing input and feedback to Policy Delivery on emerging policy lines.

8.4 Information Asset Owners (IAO’s)

The ICO has twelve IAO’s who are heads of departments and who have responsibility for the information being created, received or obtained by their department. Their responsibilities include:

- ensuring that the ICO’s policy is implemented in the business processes for which they are responsible;
- ensuring that their staff are aware of the information governance policies that affect them and that they attend or complete training as required;
- fostering a culture of personal responsibility and commitment related to information governance matters in their department; and
- completing and submitting bi annual self-assessments which measure their levels of assurance against a range of control measures.

8.5 The ICO’s staff

All the ICO’s staff have a personal responsibility to:

- handle information in accordance with information governance policy;
- attend security induction training and continue to attend or complete training as required;
- understand that failure to comply with information governance policy is treated seriously and can lead to disciplinary action; and
- report security incidents or weaknesses.

8.6 Independent external security contract

The ICO has an independent security contract in place to provide independent assurance and validation of IT information security practice and controls.

This contract provides independent advice and challenge in relation to the security of our IT environment and the work of our IT suppliers.

8.7 IT Security Working Group (SWG)

The SWG manages security across the ICO IT platform with the aim of identifying, understanding and controlling any information risks in line with the ICO’s information risk appetite. The SWG is the forum where all IT security stakeholders meet and make decisions in line with HMG and the ICO’s policy. It is responsible for:

- approving and maintaining the ICO’s Accreditation Maintenance Plan;
- managing the ICO’s accreditation activities including the Risk Management Accreditation Document Set (RMADS) and compliance with the PSN Code of Connection;
- monitoring recorded information risks and the implementation and effectiveness of associated controls;
- monitoring IT security incidents;
- approving the ICO’s code of connection with third party suppliers; and
- advising on the ICO’s system and network developments and providing security input to projects and programmes.

8.8 Physical Security Working Group

The Facilities team are responsible for the implementation and management of physical security policy and controls at Wycliffe House. The information governance team are responsible for ensuring that the requirements of the ICO’s policy and any relevant standards are understood and inform the implementation of physical security controls. The Physical Security Group meets to discuss any physical security incidents and issues. The group’s responsibilities are:

- defining physical security controls;
- carrying out periodic security inspections;
- assessing the ICO’s current physical security controls and making any recommendations for change; and
- reviewing physical security incidents.