Home Office

STILL WANT TO KNOW MORE...?

Getting the most out of our knowledge and information

Contents

Foreword

Information is critical to every part of the Home Office business.

Managing and using it correctly, protecting it appropriately and making it available to both stakeholders and the public enables the department to fulfil its objectives, deliver improved services and increase our standing with the public.

When the Home Office first published its Information Management strategy in January 2010, one of the key themes was managing information risk and ensuring that adequate measures were put in place to protect information. Due to considerable efforts in every part of the Home Office Group, we have achieved major improvements in the way we handle information. It is essential that we sustain our focus on this important element of information management so that the public can maintain trust and confidence in the way the department operates.

But, increasing demands for the right to government data means the relationship between the citizen and the state is changing. We have entered a new era of transparency which will transform the way that public services are used and delivered.

In responding to this change, the Home Office is fully embracing the move towards greater openness – sharing our knowledge and information maximises its value to us, helps facilitate closer collaboration and better enables the public to hold the department to account.

This refreshed information management strategy sets out our approach to managing our knowledge and information to achieve the right balance between making information more widely available to the public, whilst ensuring that adequate protection is in place.

As both SIRO and Transparency Champion for the Home Office, this strategy has my full support and that of the Information, Systems & Technology Executive Board members.

Helen Kilpatrick

Helen Kilpatrick Director-General Financial and Commercial Group, Senior Information Risk Owner (SIRO) and Transparency Champion for the Home Office Group.

Why an information management strategy?

WHO IS THIS STRATEGY FOR?

All employees of the Home Office, its Agencies and Arm's Length Bodies (ALBs) need information every day in order to do their jobs – the office cannot function or meet its objectives without it. This strategy isn't just for those working in "information roles": it is for all Home Office group staff – for every role, every grade, in every part of the organisation. It outlines what 'we' as the department need to do to manage our information better and supports 'the Home Office we want to be' programme.

WHY DO WE NEED A STRATEGY?

Information comes in many forms – policy documents, research papers, minutes, statistics, operational data, personal data – and is held in a variety of printed and electronic formats. Across the department we use this information in our daily working lives as we work to achieve our own objectives and those of the Home Office Group – whether it be delivering services, formulating policy, drafting legislation, holding meetings or managing staff.

To maximise the potential benefit from our information we need to manage it effectively, re-use it where we can, share it appropriately and ensure that it is adequately protected. Past experience has shown us that this does not always happen – information that is not managed properly may be lost, shared with the wrong people or not found at all.

In addition, there is now more external scrutiny of how departments manage their information and a move towards greater openness and transparency around the information that we hold. Much activity has taken place in the Home Office Group, both at corporate level and in local business areas in response to these issues.

The Home Office is playing a leading role in making more data available to the public and has published over 200 datasets on **www.data.gov.uk**, such as the crime mapping portal at: **www.police.uk**.

The Information Management (IM) strategy aims to provide a framework around managing our information throughout its lifecycle and to give a focus which has hitherto been missing. It aligns with the Information Principles[1] published by the Cabinet Office in January 2012 and with the goals of the **Home Office Business Plan 2011-15** in supporting the Home Office Group Information and Technology Strategy Framework's[2] key principles of:

- sharing and re-using systems and technology;
- joining-up information flows and processes;
- exploiting and enabling re-use of information;
- compliance with legislation, regulations and government strategies.

The strategy recognises that local IM strategies and policies may exist within business areas but it is expected that these will be aligned with this over-arching IM strategy and with the Home Office IM Corporate Policy Framework.

[1] Information Principles for the UK Public Sector. Cabinet Office, January 2012

[2] Home Office Group Information and Technology Strategy Framework. Home Office, February 2012

WHAT'S IN IT FOR YOU?

Improving the way we manage our information brings a number of benefits both to the individual and to the department. Good information management provides the individual with the following benefits:

- finding the information you need quickly and easily;
- knowing what you need to keep and what you can dispose of – removing duplication and the "I'll keep it just in case" approach;
- knowing where to keep it and how to save it;
- working more efficiently, making best use of resources – re-using information created by you or others and not re-inventing the wheel;
- working more collaboratively – making best use of skills and knowledge;
- knowing what you can share and with whom;
- knowing what information needs to be protected and what should be made available to the public; and
- providing assurance that risks are reduced and that you are complying with your responsibilities under legal requirements.

The Information Team in OCIO is responsible for developing and supporting the strategy, the corporate approach to knowledge and information management, and works closely with Information Leads across the Home Office Group to achieve this.

WHAT'S IN IT FOR THE DEPARTMENT?

Good IM provides the department with the following benefits:

- enables us to provide a more effective service to stakeholders and the public with greater transparency around the information we hold;
- preserves our reputation with the public and enables us to meet expectations of how we will manage their information;
- builds trust in the quality of our information both for staff and the public;
- supports informed decision and policy making;

Good IM enables staff handling FOI requests to locate and retrieve information easily within the required timescales. Improving our response times helps to reduce the number of complaints made to the Information Commissioner's Office.

- ensures compliance with legal requirements;

- preserves for the public record decisions being made now which will become our history in the future;

- increases our efficiency by enabling us to get the most out of the information we hold and to re-use it, which prevents us having to start all over again each time;

- reduces levels of information-related risk and ensures that our information is protected and secure;

- provides confidence and assurance to Senior Information Risk Owners (SIROs) that we are managing information risk in the department; and

- through the role of Information Asset Owners (IAOs), ensures that we are aware of our information holdings.

The Home Office Senior Information Risk Owner (SIRO) is the member of the Home Office Supervisory and Executive Management Boards with responsibility for ensuring that information risks are managed appropriately, balancing this with the requirement to make public data open and re-usable. The SIRO is accountable to the Permanent Secretary and is required to submit an annual report providing an assessment of information risks in the Home Office.

WHAT'S IN IT FOR THE PUBLIC?

Good IM in the department provides the public with the following benefits:

- delivery of more efficient, cost effective services;

- ensures that we make the best use of information;

- increases the transparency of our data, enabling the public to participate in decision making;

- increases understanding of what the Home Office does;

- enables the public to engage and collaborate with the Home Office in achieving its aims;

- enables the public to hold the government to account.

WHAT DOES GOOD INFORMATION MANAGEMENT LOOK LIKE?

Every member of staff in the Home Office Group can say:

‘I know what information we’ve got and where it’s stored’
‘I collaborate with others to share knowledge and information”
‘I know how to protect information and manage it appropriately’
‘I have the skills I need to manage information’
‘I know what’s expected of me when creating and using information’
‘I have the IT that I need to manage information’
‘I know why all of this matters because I am part of an organisation which values knowledge and information’

HOW DO WE MAKE IT HAPPEN?

We will publish a Delivery Plan outlining how the strategy will be implemented across the Department, its Agencies and ALBs. This will ensure a consistent approach to managing information and knowledge across the Home Office group. It supports the ambitions of the ‘Home Office we want to be’ programme, helping to build a flexible and joined up department through greater collaboration and knowledge sharing.

‘I know what information we’ve got and where it’s stored’

Providing staff with the right tools for managing information and training them in their use will help everyone to know what information is available to them, why it’s being held and where it’s stored.

We will:

- reduce the volumes of information that we hold, only keeping information where there is a business need to do so, and in line with statutory requirements, such as the Data Protection Act (DPA);
- increase staff awareness of the information that they create, e.g. avoiding unnecessary emails and re-using information to avoid duplication;
- increase the use of shared corporate repositories enabling quicker responses to Freedom of Information (FOI) requests and improving our understanding of what we hold and what can be made available to the public. This increases our ability to be open and transparent;
- maintain our knowledge of the information held by the department through continued use of the Information Asset Register (IAR);
- improve Shared Services solutions and promote their adoption in order to facilitate a consistent and joined up approach;
- ensure that appropriate retention schedules are applied and followed. We will securely dispose of information when we no longer require it;
- work to identify vital records and ensure they are managed effectively in order to facilitate re-use and comply with requirements;
- find effective solutions for managing our paper holdings as well as our electronic information. Many areas of the department continue to hold some information on paper and certain parts of the business rely heavily on paper files, such as UK Border Agency case files; and
- recognise that websites and other online systems form part of our information resource and so also need to be effectively managed.

The immigration casework programme (ICW) in UK Border Agency will help the business move online and move away from paper and old computer systems. This will provide a greatly improved experience for caseworkers and customers alike. The goal is to deliver a single, end-to-end, electronic caseworking system and a set of simplified processes by 2014.

‘I collaborate with others to share knowledge and information’

In line with wider government Transparency[3] initiatives and the Home Office value to “work openly and collaboratively”, we need to share information and knowledge[4] with colleagues, business partners, stakeholders and the public as appropriate – and understand the benefits that this brings. We must recognise that sharing and protecting are complementary activities, and are not mutually exclusive.

Information and knowledge are key corporate assets and we all have a responsibility to share and re-use them to release their value and maximise benefits to the business and the public. Data held by the government should be open to re-use unless there is a good reason not to.

Lessons learned from within the public protection network have highlighted the necessity of sharing information to ensure public safety. We must make the most of the knowledge and information we already have rather than reinventing the wheel.

Good information management and sharing between the police, UK Border Agency, local authorities and the core Home Office, among others, has led to many notable successes. For example, knowledge sharing through photographs and intelligence led to the arrest of many suspects in the August 2011 London riots.

We will advocate:

- a risk-based approach to sharing to ensure information and knowledge are shared responsibly;
- active sharing and re-use of information to meet the business need;
- sharing of appropriate information with the public to meet government commitments on transparency and accountability, facilitating the re-use of data to increase economic and social value.

We need to have a clear picture of information sharing activities. We must:

- maintain common data sharing principles and agreements, and work to embed these across the department;
- maintain a clear picture of who we need to share information with, such as stakeholders and suppliers, and manage this in a responsible way;
- develop a clear picture of where information and knowledge resides across the organisation, as well as the interdependencies.

[3] Transparency is all about making government open and accountable to everyone by making key information and datasets available for release so that people can hold politicians and public bodies to account.

[4] Information is produced through processing, manipulating and organising data to answer questions, adding to the knowledge of the receiver. Knowledge is what is known by a person or persons. It involves interpreting information received, adding relevance and context to clarify the insights the information contains.

We will:

- encourage sharing and re-use by knowing what information we have and where it is stored. We will give staff tools which support secure sharing and collaboration – increasing access to information through common repositories and by improving search facilities;

- enable learning from each others' experience, sharing best practice and lessons learned in a meaningful way;

A Home Office knowledge sharing tool kit has been developed which includes guidance on:

- Peer Assists – A method of sharing knowledge and experience at the start of a project;

- After Action Reviews – Looking back at a project or activity – what happened, why it happened and what lessons can be learned;

- Knowledge Exchange Interviews – A way of capturing knowledge about what it takes to do a job when someone leaves a post or changes role.

- identify and work to remove barriers to sharing, enabling secure sharing across system and organisational boundaries, such as other government departments (OGDs) or law enforcement agencies;

- maximise the opportunities provided by the introduction of a common IT infrastructure to increase sharing, collaboration and re-use; and

- ensure that, where appropriate, public data is made available in re-usable form following the five star standard for open data adopted by the Transparency Board[5].

Following a data migration exercise the Serious Organised Crime Agency (SOCA) identified a number of lessons learned:

- It's better to clean records in the old system than the new system;

- When planning data cleansing, remember to take account of existing expertise and the capability to use the tools efficiently;

- Be aware of the amount of time it takes to learn the new system and how this might impact on the data cleansing programme.

[5] The Transparency Board will drive forward the government's transparency agenda, making it a core part of all government business and ensuring that all Whitehall departments meet the new tight deadlines set for releasing key public datasets. The five star standard for open data rates how easy the data is to manipulate and use by the public on a one to five star basis.

‘I know how to protect information and manage it appropriately’

By adopting a more strategic approach to information assurance we are now more aware than ever of the associated risks of managing information. However, there is still much to do and we must continue to build upon our achievements.

Going forward we need to maintain a proactive, planned, proportionate approach to risk and security. Our response to managing risk should be appropriate and balanced with business need, enabling staff to do their jobs whilst safeguarding information.

We must work to achieve an environment where staff are risk aware and have the confidence to share information. Whilst ensuring that information is properly protected, we will appropriately and effectively share information in order to protect and inform the public. It is essential that we communicate to staff that the protection and sharing of information are not opposing principles.

‘All managers, especially Senior Civil Servants, shall model the behaviours and culture that ensures information is valued, protected and used for the public good. Managers shall encourage their staff and stakeholders to identify risks.’

Home Office Information Risk Management Policy and Guidance

We need to:

- monitor compliance with security policies, ensuring that procedures for handling breaches are strictly adhered to, and lessons learnt are incorporated into policies and ways of working;
- understand the protective marking scheme and how it impacts on the way we manage information. The Cabinet Office review of the scheme is likely to reduce the number of security markings, simplifying the scheme and ensuring that it better supports the business and our public facing work;
- support secure information sharing across the Home Office Group and external boundaries, such as supporting our work with external reviewers on projects and programmes, whilst ensuring that we adopt a proportionate approach to sharing between trusted domains;
- explore secure ways of working with new technologies, such as social media and collaborative work spaces, ensuring that staff are informed about their responsibilities when using them, both at work and at home, and are held to account;
- continue to develop those solutions which are already in place for protecting information, e.g. supporting the approach on encryption;
- build information requirements into business continuity procedures, by identifying those information assets which are business critical and protecting them accordingly;

- continue to ensure that each information asset has an Information Asset Owner (IAO) and that they are adequately trained;
- ensure ongoing access and usability of information through and after data migration and business change;
- ensure alignment with government strategy on cyber security[6].

We need to give staff the tools and skills to protect information and manage it appropriately.

We need to ensure that staff have access to tools which:

- protect information and provide secure storage;
- enforce security protocols such as access controls, and help them follow the rules;
- enable secure sharing and collaboration.

Through training and communication we will ensure that staff:

- know why managing risk is crucial and that they understand the potential impact of not adopting this approach – both on the department and the public;
- know that they have a personal responsibility to manage information-related risk;
- know that our responsibility for managing risk extends to external partners, e.g. commercial suppliers, local authorities and charities;
- understand the current and revised protective markings scheme and the different handling controls required for different types of information;
- are confident in storing information securely, applying access controls appropriately to information held in the department's systems.

[6] http://www.cabinetoffice.gov.uk/content/cyber-security

‘I have the skills I need to manage information’

We will ensure that all staff have the knowledge, skills and support they need to manage information and use it appropriately. We will build IM capability:

- **Through a range of development opportunities**
- **Through a culture which recognises IM skills**
- **Through a network of information management experts**
- **Through strengthening the Knowledge and Information Management (KIM) profession**

THROUGH A RANGE OF DEVELOPMENT OPPORTUNITIES

We will:

- ensure that IM awareness is reflected in the development needs of everyone in the Home Office Group throughout their career;

- ensure that staff have the skills to use new technology, such as collaboration tools, to their maximum potential;

- ensure that staff develop the IM skills appropriate for their roles – through training and guidance which is relevant to their responsibilities and focuses on priorities: what they need to know, and not on what they don’t;

- ensure staff are aware of sources of KIM training and development, such as Civil Service Learning;

- ensure that all staff complete the Level 1 Protecting Information mandatory e-learning training on an annual basis;

- provide staff with a clearer, holistic picture of their responsibilities, e.g. combining elements of information assurance, the need for transparency and information management;

- monitor and evaluate the effectiveness of training material and guidance on an ongoing basis;

- ensure that staff are aware of the handling requirements for different types of information, e.g. personal data and statistics;

- ensure managers lead in cultivating good IM behaviours and knowledge sharing activity which staff can emulate;

- increase managers’ awareness of their responsibility to encourage take-up of development opportunities and to ensure that what is learnt is put into practice; and

- encourage champions in each business area to promote good IM and knowledge sharing practices.

THROUGH A CULTURE WHICH RECOGNISES IM SKILLS

We will:

- work to create an environment where IM skills are recognised and valued – in the same way that management, communication, project management and financial skills are;
- work towards a position where good IM skills are seen as core skills required by all Home Office staff; and
- work towards recognising IM skills and behaviours in the performance management process. Similarly poor IM skills or behaviours will be addressed and training needs identified.

THROUGH A NETWORK OF INFORMATION MANAGEMENT EXPERTS

We will:

- ensure that staff know who to contact when they require advice or guidance on IM and ensure that help is readily available. This support may be a local unit expert or a specialist in a central team;
- work to identify the essential skills and experience required for IM roles;
- build on the skills and knowledge of staff working in IM-related roles, providing opportunities for sharing knowledge and expertise;
- work with business areas to ensure that the importance of essential IM roles, such as Records Advisers and Information Asset Owners, is understood;
- ensure that our network of Information Asset Owners have the tools needed to support them and have completed the necessary training;
- raise awareness and usage of existing sources of support and guidance e.g. available from Information Management Shared Services, through increased promotion; and
- encourage staff to consult and involve experts early when managing specific types of information so that it is used appropriately, e.g. specialists working in research and analysis.

THROUGH STRENGTHENING THE KNOWLEDGE AND INFORMATION MANAGEMENT (KIM) PROFESSION

The KIM community in the Home Office Group is part of the cross-government professional KIM function which comprises staff working in a range of information management and information assurance roles in both strategic and operational environments. Those roles include: information rights officers; records managers; librarians and knowledge managers.

As part of our work to strengthen the KIM profession across the Home Office Group, we will:

OCIO organises Lunchtime Learning events for the Home Office KIM community and produces a quarterly newsletter, Inside Knowledge.

- build a coherent, visible professional community with a clear purpose under the leadership of the Head of KIM Profession (Head of Information within OCIO);
- ensure that IM-related roles and responsibilities are clearly defined and standardised where appropriate;
- value professionals working in knowledge and information management;
- work to embed the Knowledge Council's[7] **KIM Competency Framework**[8] across the department, ensuring that it is used in the recruitment and management of staff filling information management roles;
- ensure that KIM staff have access to tools which enable them to assess and develop their KIM professional skills;
- develop a clear picture of KIM capability across the department, identifying skills gaps and putting in place a mid- to long-term skills development plan for the profession to ensure that it continues to meet the needs of the business;
- share professional knowledge and best practice within the department;
- contribute to work being lead by the Knowledge Council to support KIM capability across government; and
- identify opportunities for closer working with other professions across the HO group.

[7] The Knowledge Council is the lead body within government for knowledge and information management issues.

[8] **A professional competency Framework for the government KIM function which focuses on KIM-specific skills.** To be used in conjunction with departmental Core Competency Frameworks.

‘I am part of an organisation which values information and knowledge’

We will develop an organisational culture which values information and works to remove barriers to managing information effectively. We will communicate our vision and culture to all staff and stakeholders, resulting in a high level of awareness due to effective messages around IM.

- **Through a culture which values information and knowledge**
- **Through effective communication of messages around IM**

THROUGH A CULTURE WHICH VALUES INFORMATION AND KNOWLEDGE

Changing culture and behaviours is a long process but we will continue building a culture:

- which values sharing information and knowledge and recognises the consequences of not sharing;
- where staff have confidence and trust in the quality of our information and in making it available to the public, unless there are reasons for not doing so, such as privacy or security;
- which values protecting information appropriately;
- where good IM is everyone’s responsibility and part of how people do their jobs every day;
- where managing information is an enabler to our business and not an additional responsibility;
- where we anticipate future IM requirements, planning proactively to improve our efficiency and effectiveness and not just react when things go wrong;
- which builds on previous IM activity and learns from experiences;
- where policies are accessible, understood and followed by staff;
- which encourages collaborative working and prevents silo working;
- where staff apply the same information management principles in projects or programmes as they would to their business as usual work; and
- which values corporate benefits over individual benefits thus encouraging the retention of knowledge within the department.

THROUGH EFFECTIVE COMMUNICATION OF MESSAGES AROUND IM

We will increase awareness among staff of the importance of information and raise the profile of IM within the department.

We will communicate:

- the benefits of good IM both to the individual and the department;
- the risks and potential impact of poor IM; and
- our culture to staff and to our partners, such as commercial suppliers.

We will do this by:

- simplifying complex information into more accessible practical guidance using clear and consistent language;
- developing and maintaining a **glossary of KIM terms** as they are used in the Home Office;
- using a range of communication channels appropriate to different audiences and targeted to particular roles and functions;
- using stories and case studies of best practice in our communications to illustrate the power of IM in improving delivery and enabling the business;
- building messages about IM into general communications and activities; and
- dispelling myths about IM, such as around the functionality of IM systems.

The 'Information Management' area on the Home Office intranet, Horizon, provides easy access to policies, guidance and tools to support staff in managing knowledge and information and includes a **Glossary** of KIM terms.

‘I know what’s expected of me when creating and using information’

We will ensure that staff know what is expected of them when creating and using information:

- **Through comprehensive IM policies and guidance**
- **Through development of an IM maturity model**
- **Through establishing a picture of compliance; and**
- **Through an accessible corporate IM Policy Framework.**

A crucial part of using and managing information effectively, is our understanding of how and why we need to manage it.

IM is governed by legislation, policies and codes of practice that govern our creation, use and storage of information. Knowing when a policy or standard applies to an activity should be part of the general understanding of a role. Finding out what compliance means in this context will be achieved:

THROUGH COMPREHENSIVE IM POLICIES AND GUIDANCE

Much of the information we hold and use has legal restrictions or guidelines covering its use. It is important that we understand how we can use and re-use our information within these guidelines and that we do re-use it where possible.

We will:

- ensure IM policies and guidance are easily accessible and show when and where they need to be applied so that you can easily see what is necessary;
- ensure IM policies and guidance are focussed towards Home Office business and the relevant standards so that we comply where it is necessary and in a way that is beneficial and cost-effective to the department;
- ensure requirements reflect our changing business and make full use of our IT infrastructure;
- proactively disseminate IM policies, promoting awareness and ensuring they are followed.

THROUGH DEVELOPMENT OF AN IM MATURITY MODEL

The way we manage information changes and develops over time as requirements alter. Information security, information assurance and cyber security all have an effect on how we should manage and make best use of the information we hold and collect.

As we move towards a common IT infrastructure, managing our information in a unified way becomes more necessary and increasingly possible.

We will produce a maturity model for Information Management to map the path that we, and our partners, need to travel both to improve our individual handling of information and establish the basic requirements for information management compliance. This will set out the standards and policies we use, providing a single development path, a unified approach, and producing in effect a single IM policy for the Home Office family. The Model will tie in directly with the IM Strategy delivery plan and culture change work, leading towards a greater maturity and consistency in the way we manage our information.

Knowing the level of compliance that currently applies, and what the next stage will be, will help imbed IM practice into everyday processes and help staff become aware of what is expected of them.

Did you know that there are rules governing national and official statistics? These are set down in a **Code of Practice for Official Statistics** established by the UK Statistics Authority, which must be followed by everyone – not just staff working in statistics. The Authority monitors compliance with the Code to ensure that our statistics are produced, managed and disseminated to high professional standards.

THROUGH ESTABLISHING A PICTURE OF COMPLIANCE

We will:

- use the IM and IA maturity models and audit processes to establish an accurate and complete picture of compliance levels;

- align KIM auditing and reporting processes and, where possible, re-use the data for external reporting requirements, such as The National Archives' **Information Management Assessments**[9]; and

- ensure that we are clear about who is responsible and accountable for compliance, for example, all staff are required to comply with the DPA.

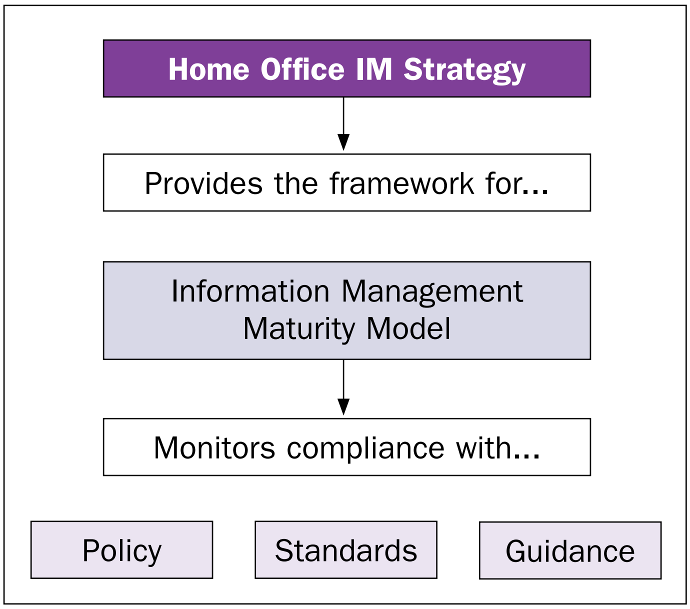
[9] Provides independent validation of the standards and integrity of information management processes and capability within departments by assessing areas such as governance and leadership, access, compliance and culture.

THROUGH AN ACCESSIBLE CORPORATE IM POLICY FRAMEWORK

We have an agreed **suite of corporate IM policies** which reflect the high level requirements for managing information from creation to deletion/archiving. This policy framework will continue to be developed in support of this strategy and our compliance requirements.

We will:

- ensure that staff can access IM policies and guidance;
- that IM policies and standards are linked;
- proactively disseminate IM policies, promoting awareness and ensuring they are followed;
- establish monitoring processes to ensure that policies are implemented and complied with. Work has begun on measuring levels of compliance with the high level policies across the office; and
- work to embed our IM policies into everyday processes.


Home Office IM Strategy
Provides the framework for...
Information Management Maturity Model
Monitors compliance with...
Policy
Standards
Guidance

‘I have the IT that I need to manage information’

We will ensure that all staff have the technology they need to support the IM good practice and behaviours set out in this strategy.

- **Through moving the department to a common IT infrastructure**
- **Through ensuring that IM requirements are key to IT decision making**
- **Through giving staff access to appropriate IT**
- **Through the use of a corporate repository which meets the needs of the business and the user**

THROUGH MOVING THE DEPARTMENT TO A COMMON IT INFRASTRUCTURE

The core Home Office, the delivery Agencies and ALBs will, over time, converge onto a common IT infrastructure. The Home Office is working towards delivery of this vision by 2016, bringing together a user group of approximately 25,000 employees. The planned convergence promises enormous benefits to staff and the organisation:

- a common IT infrastructure will make it easier for staff to access, re-use and share information across organisational or network boundaries where there is a business need to do so;
- it will enhance security, providing increased protection for information;
- it will facilitate collaborative working, support remote working and also provide significant cost savings; and
- it will provide greater opportunities for the take up of Shared Services.

THROUGH ENSURING THAT IM REQUIREMENTS ARE KEY TO IT DECISION MAKING

To achieve the aims of this strategy, we need to ensure that our IM and IT requirements are aligned and that IM needs are a key factor in the making of IT decisions. This will cover: the business specification and design of new systems; the implementation and management of systems; the management of legacy systems and data migration; and the secure disposal of information and IT equipment. New approaches to technology, such as cloud, will have implications for how we manage and protect our information. In working to address these, we must focus on the information and content within systems and not the technology alone.

THROUGH GIVING STAFF ACCESS TO APPROPRIATE IT

All of our IT should:

- enable staff to manage, use and share information and knowledge;
- support effective search, retrieval and re-use;
- support the needs of the business and adapt to changing requirements;
- support the department's approach to cloud, open standards and open source as set out in the department's ICT Strategy;
- enable us to embrace the opportunities presented by using new technologies, such as social media, securely for business purposes;
- support flexible, remote and collaborative working;
- incorporate information assurance and cyber security requirements enabling us to protect our information;
- support compliance with standards, policies and legislation such as the Public Records Act;
- provide continued access to digital information; and
- provide reliable management information to inform decision making.

THROUGH USE OF A CORPORATE REPOSITORY WHICH MEETS THE NEEDS OF THE BUSINESS

We are working towards a situation where our business information is held in an appropriate corporate repository – and not stored in a multitude of inboxes and personal drives.

Use of shared corporate repositories has a number of benefits for the individual, the department and the public;

- staff know what information we have and where it is stored;
- information can be shared where appropriate and re-used;
- it supports us in being more transparent to the public;
- it reduces the risk of duplication – a single copy of a document is held centrally, rather than multiple copies held locally;
- the latest version of a document is easily identifiable;

- appropriate retention and disposal rules can be applied;
- information is stored securely and protected via permissions settings;
- information is not lost during data migration or when a member of staff moves on; and
- using an appropriate corporate repository means less money is spent on individual business-specific solutions.

Who will make this happen?

OCIO, in collaboration with stakeholders, will establish an effective governance model for IM to take forward implementation of this strategy:

- **Through a clear picture of IM governance**
- **Through a streamlined governance model**

THROUGH A CLEAR PICTURE OF IM GOVERNANCE[10]

It is essential that the department understands who is responsible for its IM systems, IM strategy and policies, and information holdings. The governance structure will support KIM activities across the department, recognising the needs of Agencies and ALBs, while ensuring alignment with the agreed strategic direction set out in this document. Further work has been undertaken in OCIO to expand the current IM governance landscape to incorporate cyber security.

THROUGH A STREAMLINED GOVERNANCE MODEL

We are seeking to achieve a simplified IM governance model for the department which will provide increased clarity of function and accountabilities and reduce duplication of work.

We will:

- ensure that relationships between different governance bodies and roles are clearly laid out and logical;
- ensure that the governance model is agile enough to reflect changing organisational needs;
- formalise and document the authority, responsibilities and Terms of Reference (TORs) of different roles, bodies, groups and communities of interest, recognising that these will evolve over time;
- ensure that policies are linked to delivery outcomes;
- ensure that statutory duties are enforced through mandated roles, such as Records Advisors;
- ensure that business units, Agencies and ALBs are appropriately represented through membership of governance bodies and decision-making groups or by consultation with them; and
- ensure that the agreed governance model is communicated, understood and reviewed on an ongoing basis.

The SIRO role has been expanded to include that of Transparency Champion, emphasising that Transparency and Information Assurance are ‘two sides of the same coin’. The ToRs and associated standards and guidance for this role have been revised to reflect this change.

[10] Sets out the process for decision making – providing clarity around individual roles and responsibilities so that staff are clear on where decisions are made and why.

What we did

CONSULTATIONS TOOK PLACE WITH THE FOLLOWING STAKEHOLDERS

HO BUSINESS UNITS:

Communication Directorate (CD)

Crime and Policing Group (CPG)

Departmental Security Unit (DSU)

Home Office IT (HOIT)

Human Resources (HR)

Information Management Service (IMS)

Office of the Chief Information Officer (OCIO)

Office for Security and Counter-Terrorism (OSCT)

Home Office Science

DELIVERY PARTNERS:

Criminal Records Bureau (CRB)

Independent Police Complaints Commission (IPCC)

Identity and Passport Service (IPS)

National Policing Improvement Agency (NPIA)

Serious Organised Crime Agency (SOCA)

UK Border Agency (UKBA)

EXTERNAL:

The National Archives (TNA)

CONSIDERATION WAS GIVEN TO THE FOLLOWING DOCUMENTS

Agency / ALBs IM Strategies and Policy Documents [Various]

Bichard Inquiry Report. HC 653. Sir Michael Bichard, June 2004

Data Handling Procedures in Government – Final Report. Robert Hannigan, Cabinet Office, June 2008

Data Principles, Cabinet Office, 2011

Data Sharing Review Report. Richard Thomas and Mark Walport, July 2008

Digital Britain – Final Report. CM 7650. Department for Culture, Media and Sport and Department for Business, Innovation and Skills, June 2009

Five Star Standard for Transparency. Transparency Board, Cabinet Office, 2011

Government ICT Strategy. Cabinet Office, March 2011

Government Knowledge and Information Management (KIM) Professional Skills Framework. Knowledge Council, 2009

Government Shared Services, A Strategic Vision, Cabinet Office, July 2011

Home Office Business Plan 2011-15. Home Office, May 2011

Home Office Communication Strategy. Home Office, 2010

Home Office Information Risk Management Policy and Guidance. Home Office, July 2008

Information and Communication Technology (ICT) Strategy. Home Office, February 2012

Information Principles for the UK Public Sector. Cabinet Office, January 2012

Information Matters: Building Government's Capability in Managing Knowledge and Information. HM Government, November 2008

Information and Technology Strategy Framework. Home Office, February 2012

Making Open Data Real: A Public Consultation. Cabinet Office, August 2011

The Power of Information: an independent review. Ed Mayo and Tom Steinberg. June 2007

Review of Criminality Information. Sir Ian Magee, July 2008

Science and Innovation Strategy 2009-12: Using Science, Research and Analysis to Protect the Public. Home Office, February 2009

Staying Safe Online.

Strategic Direction for the Improvement of Criminality Information Management.
HM Government, 2009

'If people put data on the web – government data, scientific data, community data, whatever it is – it will be used by other people to do wonderful things in ways they would never have imagined. The cry of 'raw data now' has spread around the world.'

Sir Tim Berners-Lee

Home Office

ISBN: 978-1-84987-690-2
Published by the Home Office

© Crown Copyright 2012

Any enquiries relating to the information management strategy should be addressed to:

The Office of the Chief Information Officer
Home Office
4th Floor, Seacole Building
2 Marsham Street
London
SW1P 4DF

Email: OCIO@homeoffice.gsi.gov.uk

In preparing this document, consideration has been given to the Public Sector Equality Duty.