Statutory Code of Practice on Data Sharing

Iain Bourne
Group Manager – Policy Delivery

21st July 2011

ICO approach to information sharing

- DPA is not a barrier where information sharing is justified, necessary and proportionate

- DPA provides a framework for sharing in a secure, lawful and reasonable way

- Limitations and safeguards are essential

ico.

Background to the CoP

- Government vision statement 2006
- ICO Framework Code of Practice 2007
- Thomas/Walport data sharing review 2008
- Coroners and Justice Act 2009

ico.

Consultation responses

- Over 100 responses from public, private & third sector, trade associations and individuals

As a result of this process we have:

- Clarified the the scope of the code
- Included a section on mergers & takeovers
- Included more examples from private sector
- Included checklists for one-off and systematic sharing
- Provided more detail on specific conditions for processing personal data
- Included a glossary of key terms

ico.

What 'statutory' means

- Required by law to produce it
- Approved by Secretary of State and parliament
- Admissible in court proceedings
- But code still provides 'good practice' advice
- Not following the code isn't necessarily a DPA breach

ico.

What does the code cover?

Applies to data controllers in all sectors

Data sharing includes the disclosure of data:

- from one data controller to another
- from a data controller to a data processor
- data controllers pooling information
- separate departments within an organisation

Data sharing can be:

- systematic, routine data sharing for an established purpose
- exceptional, one-off disclosures of data for any of a range of purposes

Chapter-by-chapter

1-3: Foreword, introductory stuff, definitions

4: Lawful basis for data sharing
- Powers, obligations, information gateways

5: Deciding to share
- Questions to consider before sharing
- Conditions for processing

6: Fairness and transparency
- What to include in a privacy notice
- Sharing without telling the individual
- Specific advice on mergers and emergency response planning

ico.

Chapter-by-chapter

7: Security
- Compliance with 7th principle

8: Governance
- Data sharing agreements
- Agreeing data standards before sharing
  - Compatibility, accuracy, retention periods, training

9: Individuals' rights
- Dealing with SARs and objections

10: Things to avoid
- Some examples of bad practice

ico.

Chapter-by-chapter

11: ICO powers and penalties

12: Notification

13: FoI

14: Data sharing agreements
- Guidance on drafting an agreement
- Template data sharing request and disclosure forms

15: Data sharing checklists
- Useful overview of questions. Also available separately.

ico.

Chapter-by-chapter

Annex 1: DPA principles
Annex 2: Glossary
Annex 3: Case studies
- Based on common examples of data sharing

ico.

Deciding to share

- Legal provisions for sharing
- What benefits are sought from the proposed sharing?
- What risks are there?
- What are the likely effects on individuals/society?
- Consider the consequences of **not** sharing.
- Consent? Choice? Transparency?
- Make the citizen/client/consumer the focus of the decision.

ico.

Issues to consider

- Do you have the power to share the information?
- What is the sharing intended to achieve?
- Do you need to share personal data?
- What information needs to be shared?
- When should it be shared?
- Who does it need to be shared with?
- How should it be shared?

Fairness and transparency

- Consent – not the only basis to share information and in some cases clearly not achievable
- Generally organisations will need to tell individuals **who** is processing their data and **how** it will be used to comply with the fair processing requirements in the DPA
- Should consider what you should tell individuals about how you intend to share their data and how you will provide them with this information

ico.

Managing the sharing

Security – crucial to consider appropriate arrangements for security of shared data

Data standards – Compatibility of format
Accuracy
Retention and deletion
Staff training
Reviewing arrangements
Individuals' rights
Notification

ico.

Data sharing agreement

Should include:

- The purpose or purposes of the sharing
- Who will have access
- What will be shared
- Quality issues – accuracy, relevance and usability
- Data security
- Retention and deletion
- Individuals' rights
- Review of effectiveness of sharing

ico.

How the code can help

- The code provides good practice advice that will be relevant to all organisations that share personal data

- The ICO has the power to take action against organisations that do not comply with the DPA when they are sharing an individual's data

- Following the advice in the code will help you to:
  - decide whether or not to share personal data; and
  - collect and share personal data in a way that is fair, transparent and in line with the rights and expectations of individuals

ico.

Other help from the ICO

- Guide to data protection
- Personal information online CoP
- Privacy Notices CoP
- Modern, accessible, realistic
- Guidance review

ico.

Subscribe to our e-newsletter
at www.ico.gov.uk

Follow us on Twitter
at www.twitter.com/iconews

ico.

Supporting the technical needs of the ICO: Investigations, complaints and policy

Simon Rice
Principal Policy Adviser (Technology)
13 July 2011

Thank you for the invitation to speak at this event and for the opportunity to meet with many of you in the audience over the past couple of days.

I was initially invited by Stewart to offer comments at some of the other sessions during the conference

Whilst we were discussing those he asked the question (paraphrasing) "so what exactly do you do at the ICO?"

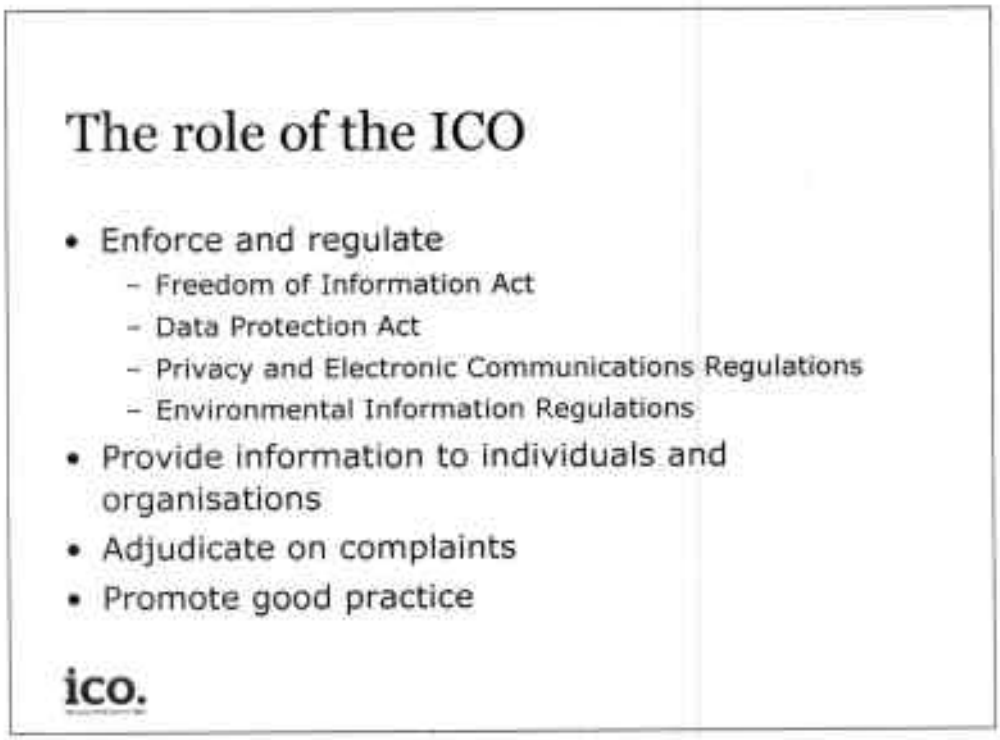
That is where the idea for next 30 minutes came from!

Before we put my job specification under the microscope I invite you to put the role of the ICO into context.

In the week that I was putting these slides together here is a list of the titles from a daily blog from a well known security firm.

CLICK(S)

The picture I am trying to present is that technology is a source of threats to information rights to UK citizens but also worldwide.



So how does this impact on the work of the ICO?

I am sure many of you may have seen this slide before,

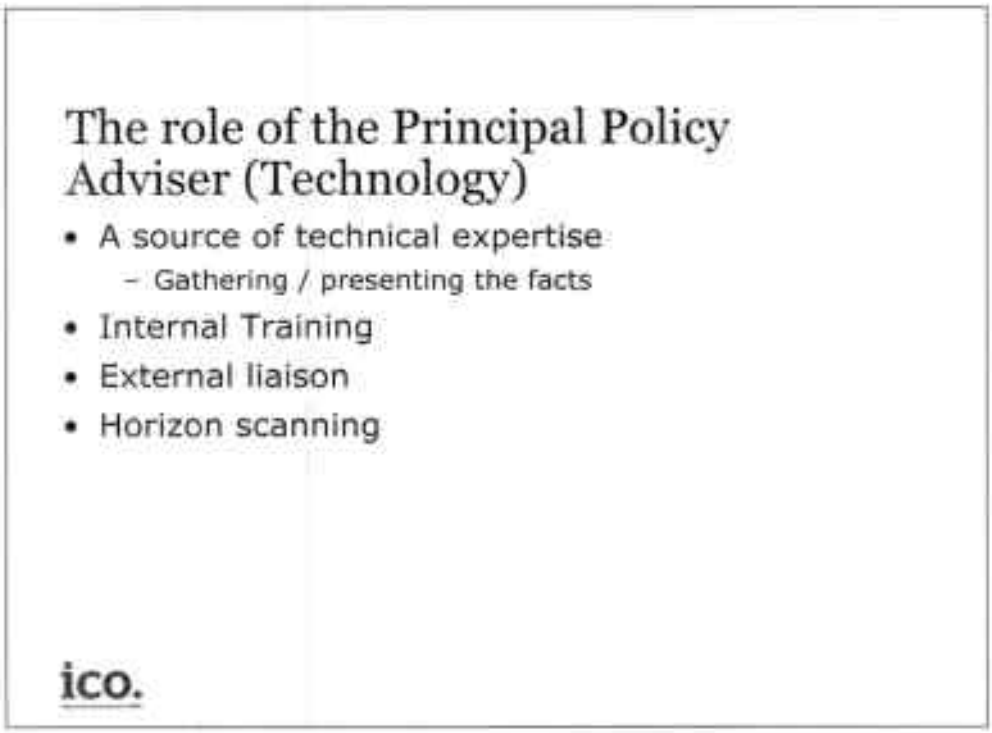
but I thought it worth reviewing it again specifically in the context of the types of headlines we have just seen as well as many others I am sure you can think of.

Freedom of Information Act

When the collation government came to power, David Cameron outlined the Government's Transparency agenda with the objective to become the most open government in the world. This has propelled the advancing demand from individuals to the data they have paid to be collected in addition to exercising their right to inspect public finances, decisions and information.

We have a wealth of information being published both proactively and in response to formal FOI requests. With all this data comes the ability for robust analysis. We can apply the power of social media, mash-ups and data mining being applied to publically available datasets, for example on data.gov.uk.

Importantly, we also have the computing power available to analyse it. A note published by the New York Times said that they used Amazon's Elastic Cloud computing to process a 4TB raw image file into 11 million finished PDFs in the space of 24 hours at a computation cost of about $240 (not including



Turning the attention to my role.

Essentially, to enable to ICO to deliver each of those bullet points where technology has an impact.

CLICK

This means as a source of technical expertise for each of the wide range of issues dealt with. Or to put is more simply, to gather and present the facts.

For example, a query could come through to the helpline about a topic that the call handler has never heard of before. This cannot reflect badly on the call handler because we cannot possibly expect them to know the ins and outs of every technology in existence.
What they can do, however, is take down the facts and contact me for further guidance and clarification. We can then together, formulate a response to the caller.

Rather than get spend time searching the internet, I can give them the important facts but also make it relevant to the particular circumstances. This means the call or complaint handler can spend more time dealing with the case rather than just trying to work out what it is all about!

If the query needs to go further, or it is a complaint, we can review the evidence and prepare a list of questions for the target of the complaint, and of course review their response.

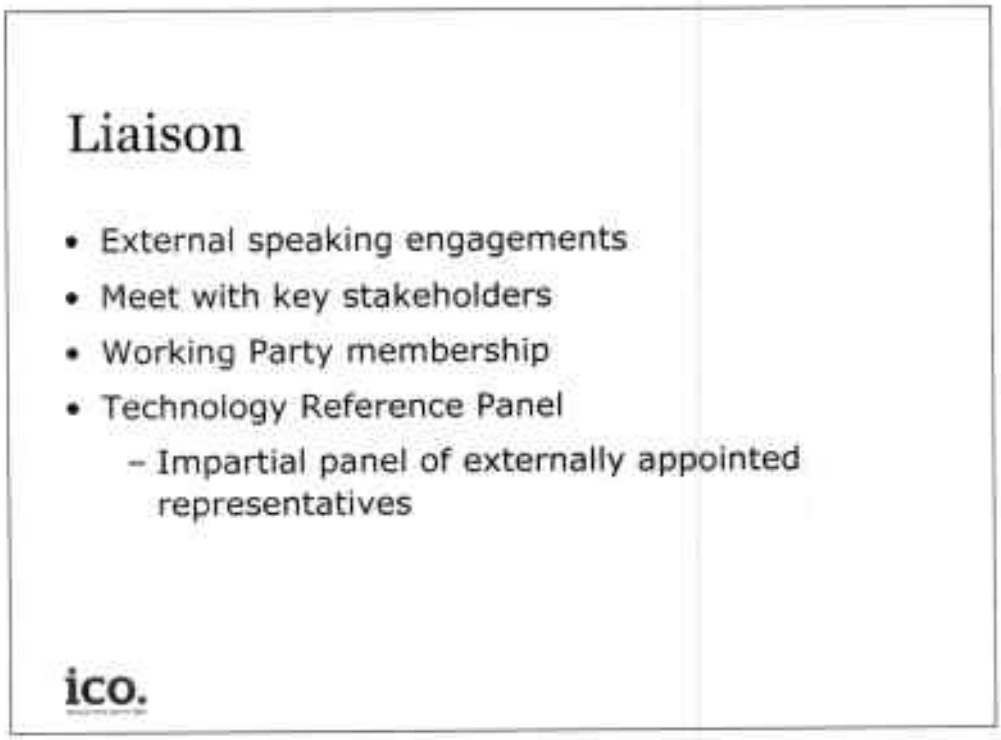
These types of queries also come from the policy delivery and strategic liaison teams. For example, since the revisions to PECR we have had a number of queries regarding strategies to comply with the legislation and also suggested solutions with regarding to getting consent for cookies. The legal experts are able to make the judgement as to whether or not the informed consent was achieved where as I was able to explore the underlying aspects and identify the possible loopholes or technical pitfalls.

CLICK

Again, we can never expect everyone within the office to know everything, we can expect most people to have a grasp of the basics.

So a second component of my role is to identify areas of weakness and deliver training to members of staff. For example, a 45 minutes session on "What is cloud computing?" or "The basics in IT security". Of course these will only touch on the basics but they can always be extended into a 1/2–day workshop for a small group or finding an appropriate external course.

CLICK



As I've already mentioned, a key role is engaging with "the outside world" in order to keep up to date with the topics and concerns being faced by organisations and individuals.

CLICK

Obviously one such way of achieving this is attending and speaking at external engagements such as this one. Not so much for the speaking component but the listening and dialogue with people such as yourselves during the coffee breaks.

CLICK

Outside of the formal conference arena, I am in regular discussions with individuals and technical organisations to discuss their data protection issues

CLICK

These can all be brought to working party groups to form a firm evidence base for any policy decision or review of a technical implementation. With this approach I can be sure that I am representing

For my final slide, I thought it would be interesting if I highlighted what I thought could be some of the key issues in the immediate and near future for the ICO.

Of course I don't have a crystal ball but here's a short list of topics on the agenda (and they are in no particular order)

CLICK

Cloud computing

Well, when I said in no particular order, lets get rid of the elephant in the room first!

You can't go near an IT magazine, blog or sales pitch without hearing the "C" word.

I am not going into definitions except to say that cloud means many things to many people.

The technology does indeed raise a number of DP issues but the majority are neither new nor specific to the cloud.

CLICK

If we think about the wide-scale adoption of public cloud services, by both individuals or organisations

The most obvious conflict with the Data Protection Act, is Principle 8 concerning the transfer of personal data, especially outside the EEA.

By its very nature, cloud computing is a distributed architecture and data is supposed to be spread out and moved across many locations. It is precisely this architecture which gives rise to the efficiencies found within the technology. As you may know, within the cloud, this makes it very difficult to know where you data is located at any one time. That works incredibly well for resilience and redundancy but not for compliance with the Data Protection Act.

Even signing up with a UK-based cloud provider may not provide you with a 100% guarantee that your data is held within these shores. That cloud service may well be layered on another cloud computing platform, for example using Microsoft's Azure platform or Amazon web services, which may be located elsewhere round the world.

A second concern is the security of the data. If you hand over your data to a third party this is now outside of your control. You have lost all governance and influence over the security measure applied. Only the largest businesses or government organisations will be able to request audits or other checks to ensure that the cloud provider has taken all appropriate steps to ensure that the service is secure. This might be a good thing because a large specialist cloud provider may be able to offer better security than a small business but how can you check?

We now have online backups, online accounting, online password managers, online email, online document editors, online spreadsheets. Almost every inch of the business process has a cloud based

Keep in touch

Subscribe to our e-newsletter at www.ico.gov.uk
or find us on...

facebook

twitter
www.twitter.com/iconews

YouTube

LinkedIn

ico.

Information rights in the balance: Where do transparency and accountability end and privacy and data protection start?

Christopher Graham, Information Commissioner

Privacy Laws & Business Conference
12 July 2011

Theme

- ICO: the authoritative arbiter
  - Mission
  - Performance
  - Information rights strategy
- Transparency and accountability
  - ICO approach
  - Saying yes
  - Saying no
- Projects
  - Data sharing
  - Crime mapping
  - Anonymisation

ico.

Our mission

The ICO's mission is to uphold information rights
in the public interest,
promoting openness by public bodies
and data privacy for individuals.

ico.

Our vision

By 2012 we will be recognised by our stakeholders
as the authoritative arbiter of information rights,
delivering high-quality, relevant and timely outcomes,
responsive and outward-looking in our approach,
and with committed and high-performing staff
-a model of good regulation,
and a great place to work and develop.

ico.

How's it going?

- Efficiency and effectiveness
  - 85% drop in DPA cases over six months old (cf 2009/10)
  - 73% drop in FOIA cases over nine months old (cf 2009/10)
- Civil Monetary Penalties
- Guidance
- Cookies
- Consensual audits by ICO – including Google

ico.

We want your views...

We are consulting on our draft information rights strategy.

This strategy is being introduced in light of our commitment to integrate our data protection and freedom of information activities wherever we can.

It replaces our former, separate data protection and freedom of information strategies.

The strategy describes the role of the ICO and explains how we go about our work and set priorities.

ico.

How to take part...

- Please visit the consultations page of the ICO website:

www.ico.gov.uk

Homepage > About the ICO > Consultations
> Current consultations

- Consultation closes 12 August

ico.

Context

- Transparency and Accountability agenda
  - Whitehall
  - Public services
- Open Data
- Data Sharing
- Crime mapping
- Big Society

ico.

What we're for

" Upholding information rights in the public interest, promoting openness by public bodies and data privacy for individuals"

- What we do is where it's at
- On the spot, in the spotlight
- At the centre of events
- The authoritative arbiter of information rights

ico.

Arbiter

ico.

Arbiter

ico.

ico.

Information Commissioner's Office

ico.

Statutory responsibilities

ico.

Information Commissioner's Office

Statutory responsibilities

ico.

Information Commissioner's Office

Public policy agendas

ico.

Statutory responsibilities

ico.

Information Commissioner's Office

Public policy agendas

- Transparency
- Accountability
- Open Data

ico.

Technology/
business

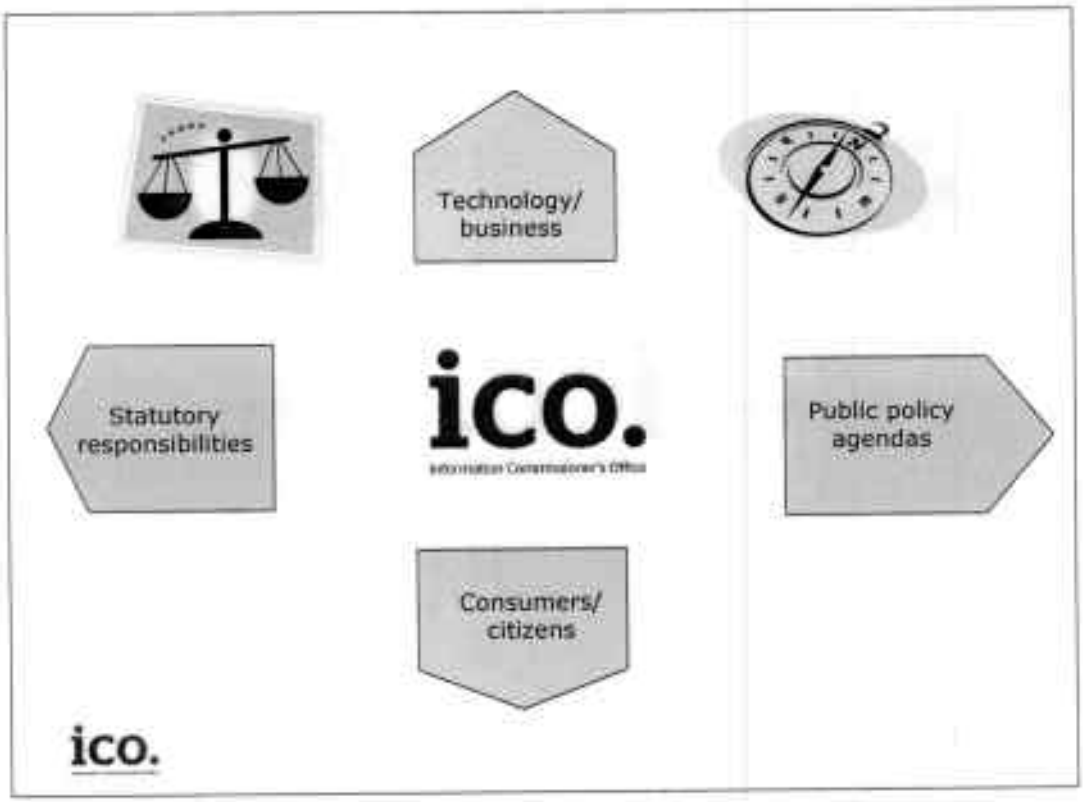
Statutory
responsibilities

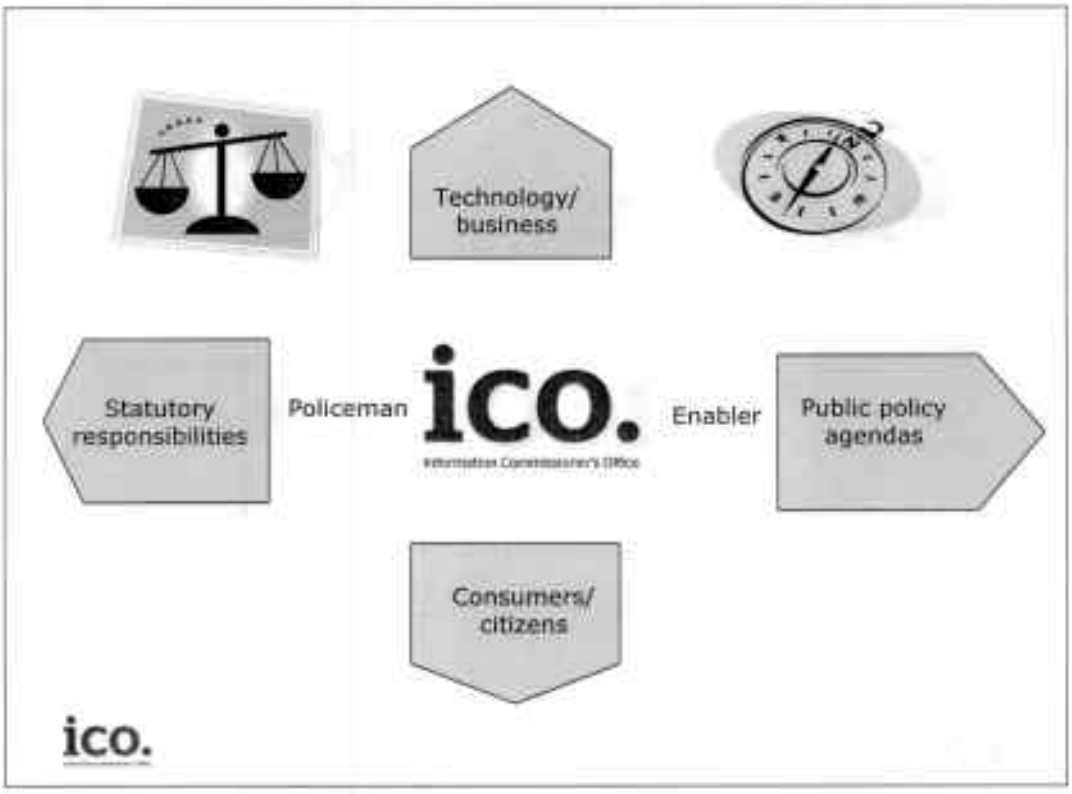
ico.

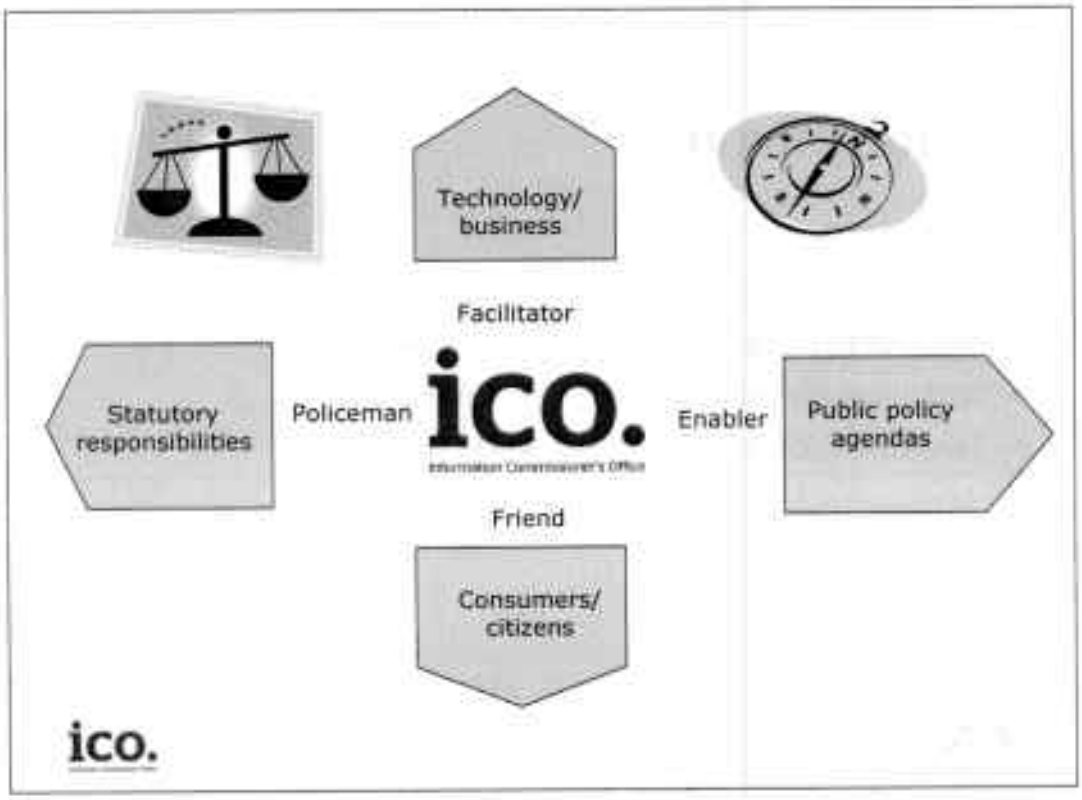
Information Commissioner's Office

Public policy
agendas

ico.


Technology/
business
Statutory
responsibilities
ico.
Public policy
agendas
Consumers/
citizens
ico.


Technology/
business
Statutory
responsibilities
Policeman
ico.
Enabler
Public policy
agendas
Consumers/
citizens
ico.


Technology/
business
Facilitator
Statutory
responsibilities
Policeman
ico.
Enabler
Public policy
agendas
Friend
Consumers/
citizens
ico.

Fit for purpose

- Statutory responsibilities
- Public policy agendas
- Technology/business
- Consumers/citizens

- Effective
- Independent
- On the ball
- On the case

ico.

How to strike the balance

- Technology drives possibilities, but 'because we can' is not justification in itself
- Data Protection Act and the DP Principles aren't suspended
- Proportionality judgement, not simply an equation balancing privacy against openness
- A key test is whether information relates more to the public life or the private life of an individual

ico.

Senior salaries

- Cabinet Office ordered to publish the salaries of 24 public servants earning more than £150k pa who were resisting publication
- Information Commissioner concluded that for public servants of this seniority there would be an expectation of publication
- Senior public responsibility will sometimes require the disclosure of personal information
- Cabinet Office accepts ruling

ico.

Bolton Council

- Ordered disclosure of certain sections of senior council officers' entries in the register of interests
- The register records the name of council officers and any personal interests they have, such as ownership of property, family associations, business interests, shareholdings and membership of organisations that could conflict with their decision-making role
- Information Commissioner acknowledged that releasing some of this information would intrude into the officers' private lives and might cause them distress
- Public interest favoured disclosure because the officers are responsible for decisions that affect the local community and involve spending public money

ico.

Cornwall Council

- An example of drawing the line and saying non disclosure was appropriate
- Case involved pension entitlements following early retirement of Chief Executives following local government reorganisation
- More about private life than public role

ico.

Data sharing

- Data protection myths – 'computer says no'
- Easiest/least risky approach is not to share
- More dangerous not to share than it is to share responsibly
- Privacy by design approach
- ICO Data Sharing Code of Practice

ico.

Crime mapping

- Conflict between utility and privacy
- First stage was fair compromise in terms of level of granularity
- Possible for some disclosures to go down to lower levels where risks are less eg antisocial behaviour in public places
- Offender outcomes with photographs on the maps or on the site?

ico.

Anonymisation

- ICO seminar at Wellcome Trust on 30 March
- Jigsaw identification by mashing datasets?
- What zealots want to believe
- Conference report shortly
- Further guidance will be produced

ico.

Next steps

- Transparency and privacy can be complementary concepts, eg transparency about how personal data is processed is vital
- Success of the government's transparency programme will be undermined if privacy of information in datasets is not protected
- Role of the Information Commissioner as referee builds confidence and acceptance

ico.

ICO as referee

- Enforce the rules – but let the game flow
- ICO as effective and engaged partner
- Enabler – from a position of credibility and respect
- ICO has to be independent – and be seen to be independent
- If not like the Ombudsman, then what?

ico.

Keep in touch

Subscribe to our e-newsletter at www.ico.gov.uk
or find us on...

facebook

twitter

www.twitter.com/iconews

YouTube

LinkedIn

ico.

Statutory Code of Practice on Data Sharing

Steve Wood
Head of Policy Delivery
Information Commissioner's Office

7th July 2011

ICO approach to information sharing

- DPA is not a barrier where information sharing is justified, necessary and proportionate

- DPA provides a framework for sharing in a secure, lawful and reasonable way

- Limitations and safeguards are essential

ico.

Background to the CoP

- Government vision statement 2006
- ICO Framework Code of Practice 2007
- Thomas/Walport data sharing review 2008
- Coroners and Justice Act 2009

ico.

Consultation responses

- Over 100 responses from public, private & third sector, trade associations and individuals

As a result of this process we have:

- Clarified the the scope of the code
- Included a section on mergers & takeovers
- Included more examples from private sector
- Included checklists for one-off and systematic sharing
- Provided more detail on specific conditions for processing personal data
- Included a glossary of key terms

ico.

What 'statutory' means

- Required by law to produce it
- Approved by Secretary of State and parliament
- Admissible in court proceedings
- But code still provides 'good practice' advice
- Not following the code isn't necessarily a DPA breach

ico.

What does the code cover?

Applies to data controllers in all sectors

Data sharing includes the disclosure of data:

- from one data controller to another
- from a data controller to a data processor
- data controllers pooling information
- separate departments within an organisation

Data sharing can be:

- systematic, routine data sharing for an established purpose
- exceptional, one-off disclosures of data for any of a range of purposes

ico.

Deciding to share

- Legal provisions for sharing
- What benefits are sought from the proposed sharing?
- What risks are there?
- What are the likely effects on individuals/society?
- Consider the consequences of **not** sharing.
- Consent? Choice? Transparency?
- Make the citizen/client/consumer the focus of the decision.

ico.

Issues to consider

- Do you have the power to share the information?
- What is the sharing intended to achieve?
- Do you need to share personal data?
- What information needs to be shared?
- When should it be shared?
- Who does it need to be shared with?
- How should it be shared?

Fairness and transparency

- Consent – not the only basis to share information and in some cases clearly not achievable
- Generally organisations will need to tell individuals **who** is processing their data and **how** it will be used to comply with the fair processing requirements in the DPA
- Should consider what you should tell individuals about how you intend to share their data and how you will provide them with this information

ico.

Managing the sharing

Security – crucial to consider appropriate arrangements for security of shared data

Data standards – Compatibility of format
Accuracy
Retention and deletion
Staff training
Reviewing arrangements
Individuals' rights
Notification

ico.

Data sharing agreement

Should include:

- The purpose or purposes of the sharing
- Who will have access
- What will be shared
- Quality issues – accuracy, relevance and usability
- Data security
- Retention and deletion
- Individuals' rights
- Review of effectiveness of sharing

ico.

How the code can help

- The code provides good practice advice that will be relevant to all organisations that share personal data

- The ICO has the power to take action against organisations that do not comply with the DPA when they are sharing an individual's data

- Following the advice in the code will help you to:
  - decide whether or not to share personal data; and
  - collect and share personal data in a way that is fair, transparent and in line with the rights and expectations of individuals

ico.

Other help from the ICO

- Guide to data protection
- Personal information online CoP
- Privacy Notices CoP
- Guidance review

ico.

We want your views...

We are consulting on our draft information rights strategy.

This strategy is being introduced in light of our commitment to integrate our data protection and freedom of information activities wherever we can.

It replaces our former, separate data protection and freedom of information strategies.

The strategy describes the purpose for which the ICO exists and explains how we go about achieving this purpose.

ico.

How to take part...

Please visit the consultations page of the ICO website:

www.ico.gov.uk

Homepage > About us > Consultations> Current consultations

ico.

Keep in touch

Subscribe to our e-newsletter at www.ico.gov.uk
or find us on...

facebook

twitter

www.twitter.com/iconews

YouTube

LinkedIn

ico.

Remaining compliant with Information Rights at a time of change

8th July

Dawn Monaghan, Group Manager Public Services

IG40

Myths and Legends

- DPA is a barrier to change
- Sharing personal data is bad
- DPA can be used as an excuse not to share and therefore not to change
- The data controller can transfer responsibilities to others

ico.

Myths and Legends

- Security issues are solely the domain of IT specialists
- Information Governance is solely the domain of information managers
- The Information Commissioner will not use his powers
- 'Right to data' means no more publication schemes

ico.

Information Rights in a Time of Change

- The Data Protection Act exists to safeguard personal information
- It's also an access regime – it gives people a right to access data held about them
- FOIA provides a right to official information proactively as well as reactively
- In a time of change these are essential rights
- DPA is not a barrier to change – It requires consideration of the principles, identification of risks and mitigating actions
- FOIA is not a threat a time of change but an opportunity to keep citizens informed and enable them to contribute.

ico.

DPA in a time of change

- It is no bigger barrier than any other consideration
- The legislation compels you to ensure that personal data is safeguarded and access rights upheld
- This requires you to consider in detail the impacts to information governance in relation to personal data when changing structures, systems, process and practices.
- Question why you are doing things, what risks does it pose and what safeguards need to be put in place.

ico.

Information Governance and Present perceptions

- Experienced and willing IG staff
- High percentage of reported breaches
- Security issues
- Lack of 'front line' staff awareness
- Lack of senior management 'buy in'
- IG seen as 'backroom' service
- Difficulties with storage
- Inconsistencies of policy, procedure and practices
- Concentration on Infrastructure rather than information
- Past difficulties with data management when organisations have merged leading to confusing relationships

ico.

Information Governance and Key Concerns for transition

New structures may mean;

- Changed or new responsibilities
- Sharing of data with new partners
- Acquisition of new data
- Decommissioning of data
- Changed purposes for processing
- Changes to organisations publication schemes 'guides to information'
- Requests for information, held now by someone else or not at all, or new information held by you!

ico.

What do we know?

- De creased Centralisation
- Lack of consistent frameworks
- Increased Data Sharing
- Increased release of data sets
- Changes to roles and responsibilities
- Changes to accountabilities
- IG could be the key to success or the Achilles heel depending upon how it is handled
- Less Resources
- New systems for information management

ico.

Threat or Opportunity?

If

- IG is centre stage it can enable smooth transition
- managed properly then an opportunity to get 'houses in order' and keep IG at the top of the agenda for the right reasons
- dealt with proactively then risks can be mitigated
- Opportunities are capitalised upon then in future greater data sharing and increased release of data can be envisaged.
- Seen as an opportunity rather than a threat than more chance than of it being so!

ico.

How can that be achieved?

- Going back to basics – Who is the Data Controller?
- Thinking and acting upon IG issues at the beginning rather than at the end
- Development of consistent frameworks
- Identification of what, why, who, when and how
- Checks for purpose and processing
- Protocols for sharing
- Gap analysis
- Being open and transparent with one another
- Ensuring staff at all levels treat data like any other important and valuable asset
- Being clear with everyone internally and externally what you are doing and why
- Being methodical and pragmatic

ico.

What can help?

- One another internally and network groups
- ICO Privacy Impact Assessment guidance
- ICO Data sharing Code of Practice
- Making IC aware of overarching concerns
- Going back to first principles
- Treating good Information governance as an enabler not a barrier

ico.

Subscribe to our e-newsletter
at www.ico.gov.uk

Follow us on Twitter
at www.twitter.com/iconews

ico.