

## News release

11 May 2011

### UK code of practice on data sharing launched

A new statutory code of practice designed to help businesses and public sector bodies share people's personal information appropriately has been published today by the Information Commissioner's Office (ICO).

The ICO's [data sharing code of practice](#) covers both routine and one-off instances of data sharing. It includes good practice advice that will be helpful to all organisations that share personal information – for example when local authorities share information with the health service or when building societies provide information to a credit reference agency. The code gives advice on when and how personal information can be shared as well as how to keep it secure.

The ICO consulted on a draft code last October. A number of changes and improvements have been made, including the addition of more public and private sector case studies to explain practically how the Data Protection Act applies to data sharing.

Along with the full code of practice, the ICO has also published a summary checklist that can be used as a quick reference guide to sharing information.

By following the code, organisations should find they have:

- a better understanding of when, whether, and how personal information should be shared;
- improved trust and a better relationship with the people whose information they want to share;
- reduced risk of the inappropriate or insecure sharing of personal data; and
- minimised risk of breaking the law and consequent enforcement action by the ICO or other regulators.

Information Commissioner, Christopher Graham, said:

“Few would argue that sharing data can play an important role in providing an efficient service to consumers in both the public and private sector. More and more transactions are done online - from shopping and banking to managing tax and health records. People now have an expectation that, where appropriate and necessary, their personal details may be shared. However, this does not mean that companies or public bodies can do this just as they see fit. The public rightly want to remain in control of who is using their information and why, and they need to feel confident that it is being kept safe.

“The code of practice we’ve issued today offers a best practice approach that can be applied in all sectors. It reflects the constructive comments we received during the consultation period, meaning that we can be confident that it not only makes sense on paper but will also work in the real world too. I’d encourage all businesses and public bodies that share personal data to get to grips with the code without delay so they can be sure they are getting it right.”

**ENDS**

If you need more information, please contact the ICO press office on 0303 123 9070 or visit the website at: [www.ico.gov.uk](http://www.ico.gov.uk).

## Notes to Editors

1. The data sharing code of practice is available on the ICO website here:  
[http://www.ico.gov.uk/~media/documents/library/Data\\_Protection/Detailed\\_specialist\\_guides/data\\_sharing\\_code\\_of\\_practice.pdf](http://www.ico.gov.uk/~media/documents/library/Data_Protection/Detailed_specialist_guides/data_sharing_code_of_practice.pdf)
2. The summary checklist is available on the ICO website here:  
[http://www.ico.gov.uk/~media/documents/library/Data\\_Protection/Practical\\_application/data\\_sharing\\_checklists.pdf](http://www.ico.gov.uk/~media/documents/library/Data_Protection/Practical_application/data_sharing_checklists.pdf)
3. The Information Commissioner's Office upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals.
4. The ICO has specific responsibilities set out in the Data Protection Act 1998, the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Privacy and Electronic Communications Regulations 2003.
5. The ICO is on [Twitter](#), [Facebook](#) and [LinkedIn](#), and produces a monthly [e-newsletter](#). Our [For the media](#) page provides more information for journalists.
6. Anyone who processes personal information must comply with eight principles of the Data Protection Act, which make sure that personal information is:
  - Fairly and lawfully processed
  - Processed for limited purposes
  - Adequate, relevant and not excessive
  - Accurate and up to date
  - Not kept for longer than is necessary
  - Processed in line with your rights
  - Secure
  - Not transferred to other countries without adequate protection