

Annual Report 2006/07





Information Commissioner's Office

Annual Report 2006/07

Presented by the Information Commissioner to Parliament pursuant to Section 52(1) of the Data Protection Act 1998 and Section 49(1) of the Freedom of Information Act 2000 and Schedule 5 paragraph 10(2) of the Data Protection Act 1998.

Ordered by the House of Commons to be printed 10 July 2007

HC646

London: The Stationery Office

Price: £18.00

© Crown Copyright 2007

The text in this document (excluding any Royal Arms and departmental logos) may be reproduced free of charge in any format or medium providing that it is reproduced accurately and not used in a misleading context. The material must be acknowledged as Crown copyright and the title of the document specified.

Any queries relating to the copyright in this document should be addressed to
The Licensing Division, HMSO, St Clements House, 2-16 Colegate, Norwich, NR3 1BQ.
Fax: 01603 723000 or e-mail: licensing@cabinet-office.x.gsi.gov.uk.

Contents

1. Information Commissioner's foreword	5
2. Your information rights	9
3. Our year at a glance	11
4. Protecting your personal information	20
5. Your right to know	32
6. Our regional offices	42
7. Improving our communications	46
8. Our people	49
9. ICO infrastructure	51
10. Corporate governance	54
11. Prosecutions	56
Accounts	59



What we do

Promoting public access to official information and protecting your personal information

The Information Commissioner's Office (ICO) is the UK's independent public body set up to promote access to official information and to protect personal information. We enforce the Data Protection Act, the Freedom of Information Act, the Privacy and Electronic Communications Regulations and the Environmental Information Regulations, regulating the organisations that come within our remits.

We provide guidance to organisations and individuals to promote awareness of information rights and obligations, ensure compliance with the law and encourage good practice.

We rule on eligible complaints and can take action when the law is broken. The Commissioner, who reports directly to Parliament, has the power to order compliance, using enforcement and decision notices, and prosecution.



1

Information Commissioner's foreword



Information rights matter

There has been a sea-change. Information rights have never been taken more seriously – by politicians and the public sector, by business leaders, by the media and, crucially, by private individuals. The two strands of our work have repeatedly set the news agenda over the last year and featured heavily in Parliament and in public discussion. Data protection and freedom of information impact on almost every aspect of life. Both involve delicate balancing acts. Both make a real difference in shaping the nature of society.

Data protection protects people – providing essential safeguards for private life and for the integrity of personal information. Freedom of information brings the transparency and accountability which any democracy demands – reminding everyone that government serves the people, not the other way round.

At the ICO, we are proud of a very successful year. We have handled unprecedented caseloads. We have exceeded our targets, with some dramatic improvements in performance. Although the current level of funding means that some cases are taking longer than we want, we have issued a steady stream of well-respected freedom of information decision notices and resolved many thousands of cases informally. Information on a huge variety of topics has come into the public domain. We have shown our regulatory teeth with successful prosecutions and enforcement action. Our hard hitting reports on the pernicious illegal trade in personal information are producing tangible results. We have started a national debate about surveillance issues and this has inspired two select committee inquiries. We hosted the two main international conferences for privacy and for freedom of information commissioners. We have launched a brand new and well-received website and created a new intranet. Individuals' awareness of data protection rights has risen to 82% (from 76% last year) and their awareness of freedom of information rights has reached 73% – astonishingly high for a new law.

We aim to be robust and responsible in ensuring that the law is doing what it was set up to do: protecting privacy and promoting openness. It is not easy to promote openness of public bodies while respecting the privacy of individuals. There are real tensions between securing greater transparency and preserving the private space needed for good policy-making. Public security and safety demand greater access to information about our private activities. Both sets of law are based on a strong foundation of information rights. Both promote good information-handling. Both depend upon high standards of records management. Both cry out for clear rules for

countless situations, often requiring difficult balancing acts. And, as the daily demands of our work demonstrate, both are now an essential part of the modern world.

Introducing freedom of information, and parallel access to environmental information, has involved a steep learning curve for all concerned. A constitutional reform of such magnitude, calling for cultural change at the heart of public administration, was bound to involve some initial discomfort. But – as in other countries – this will subside as the benefits of open government become ever more apparent. The surprise is why so much was previously kept secret. After two years, it is remarkable how much progress has been made. Over 200,000 requests for information from public authorities – most of them successful – have demonstrated the appetite for openness. With members of the public as the biggest group of users, information has been requested on topics as broad as toxic waste, speed cameras, the performance of surgeons, MPs' travel expenses, local authority pension investments, prostitution zones and ministerial advice on angling.

Every complaint about a refused request throws up new, and often highly complex, factual and legal issues. At the ICO we have to apply the law to many different types of case, setting the boundaries for public sector transparency. Each case involves considering the competing arguments of the public authority and of the requester and (in numerous cases) identifying and weighing the competing public interest considerations. Cases where publication is ordered hit the headlines, but decisions upholding non-disclosure are just as important. With so many high profile cases, it is a source of pride that – despite the ease of going to the Tribunal – three-quarters of our decisions are accepted by both sides without appeal.

As freedom of information settles down, its cousin, data protection, has never been more necessary nor faced greater tests.

Personal information is now used in previously unimaginable ways. In the world of cheap and almost limitless processing and storage capacity, commercial and political pressures to escalate the use of the electronic footprints we leave many times a day become almost irresistible. The benefits of using personal information are undeniable. But so are the risks for individuals and society where use goes beyond reasonable expectations or where things go wrong. The purposeful, routine and systematic recording of everyone's movements, activities and transactions in public and private spaces – a surveillance society – is fast becoming a reality. The dangers are graver still as one system is linked to another. The risks – such as mistaken identity, inaccurate or out of date information, judgmental profiling – magnify as information is shared ever-wider.

Only data protection and self-interest stand in the way. Although many of the detailed rules are too bureaucratic, the underlying principles of data protection have successfully stood the test of time. They provide a sound framework to minimise the risks and promote acceptable and beneficial handling of personal information. But legal regulation is insufficient by itself. The consequences of getting it wrong can now be seen instantly – domestically and across the globe – causing great short-term damage to political and commercial reputations and long-term damage to society. It is ministers, permanent secretaries, chairs and chief executives who must ensure their organisations guarantee safeguards and exercise the necessary self-restraint. This is simple self-interest which must come from the top.

Recent security breaches – permitting the wrong people to access confidential information – provide a powerful illustration of the need to ensure that safeguards are achieved in practice. The roll call of banks, retailers, government departments, public bodies and other organisations which have admitted serious security lapses is frankly horrifying. How can laptops holding details of customer accounts be used away from the office without strong encryption? How can millions of store card transactions fall into the wrong hands? How can online recruitment allow applicants to see each others' forms? How can any chief executive of a bank face customers and shareholders and admit that loan rejections, health insurance applications, credit cards and bank statements can be found, unsecured, in non-confidential waste bags?

Security breaches are just one example. Customer, employee, stock market and voter expectations are high for all aspects of data protection. My office is committed to making it easier for those organisations who seek to handle personal information well – and tougher for those who do not. My message to those at the top of organisations is to respect the privacy of individuals and the integrity of the information held about them, to embrace data protection positively and to be sure you are not the business or political leader who failed to take information rights seriously.

To sum up, freedom of information and data protection are now inescapable features of the landscape. Secret government is unhealthy government – freedom of information brings official information into the open and gives power to the people. Equally, too much private information held by the state or by commercial organisations can be unhealthy, and is dangerous if organisations do not handle it with the utmost care.

A thriving democracy needs both freedom of information and data protection. Our intention is to ensure that the public and private sectors take them ever more seriously.

A handwritten signature in blue ink that reads "Richard Thomas". The signature is stylized with a large, looped 'R' and a long horizontal stroke underlining the name.

Richard Thomas, Information Commissioner

2 Your information rights

The **Freedom of Information Act 2000** gives people a general right of access to information held by most public authorities. Aimed at promoting a culture of openness and accountability across the public sector, it enables a better understanding of how public authorities carry out their duties, why they make the decisions they do and how they spend public money.

The **Environmental Information Regulations 2004** provide an additional means of access for people who want environmental information. The Regulations cover more organisations than the Freedom of Information Act, including some private sector bodies, and have fewer exceptions.

The **Data Protection Act 1998** gives people important rights including the right to know what information is held about them and the right to correct information that is wrong. The Data Protection Act protects the interests of individuals by obliging organisations to manage personal information responsibly.

The **Privacy and Electronic Communications Regulations 2003** support the Data Protection Act by regulating the use of electronic communications for unsolicited marketing to individuals and organisations.



Data protection – the 30 second expert

- The Data Protection Act protects your personal information.
- The Act ensures your personal information is fairly and lawfully processed, for specified purposes only.
- It ensures the information held about you is adequate, relevant and not excessive.
- It ensures the information is accurate and up to date, and kept no longer than necessary.
- It also ensures your information is kept securely.
- The Act gives you the right to see the personal information held about you, and to correct it if it is wrong. It also gives you the right to stop unwanted direct marketing materials being sent to you.
- If you feel your rights have been breached, you can ask the ICO to help.

Freedom of information – the 30 second expert

- The Freedom of Information Act gives you the right to know – you can request information held by public authorities.
- Information must be disclosed unless there is a good reason not to.
- The public interest is usually considered when deciding whether or not to release the information.
- The Act covers around 115,000 public bodies.
- It encourages open government, challenges unnecessary official secrecy, improves the quality of decision-making and increases accountability for public duties and spending of public money.
- It improves understanding of and trust in public authorities.
- If you feel your rights to public information have been breached, you can ask the ICO to help.

3 Our year at a glance

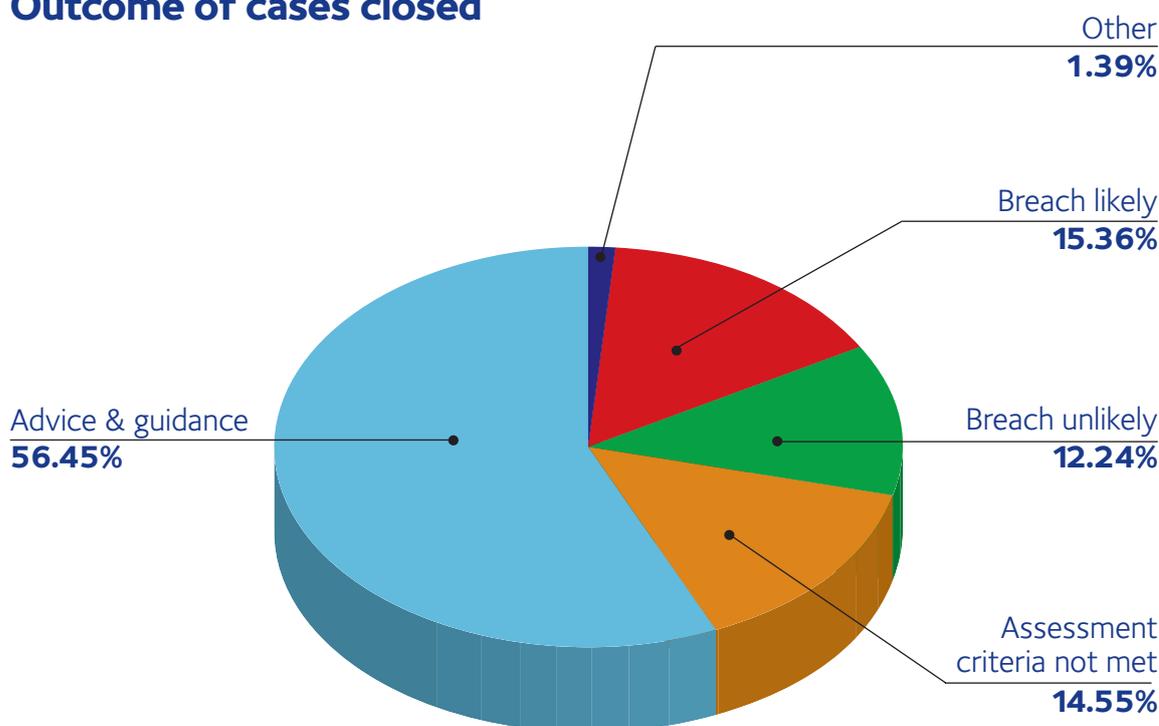


Data protection casework

More than half of data protection cases required us to simply provide advice and guidance. In some cases this advice was relatively straightforward, in others extremely complex. In the remainder of cases, we considered whether a breach of the Data Protection Act or Privacy and Electronic Communications Regulations was likely to have occurred.

In one third (35.28%) of these cases we decided a breach was likely to have occurred and the organisation took remedial action in three quarters (77.49%) of these cases. Such remedial actions may include a data controller correcting an individual's record, implementing a data protection policy or training staff.

Outcome of cases closed

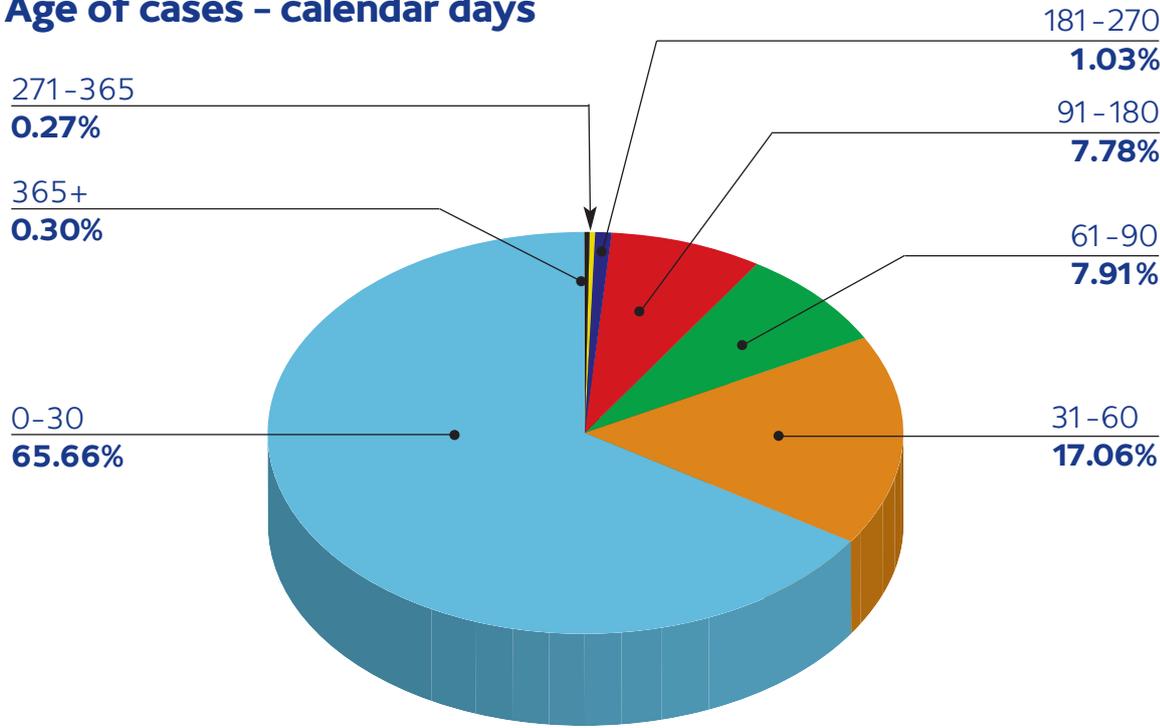


Performance against targets

Time to close cases	Target	Actual
30 days or less	40%	66%
90 days or less	90%	91%
180 days or less	98%	98%

Received	Closed	Work in progress
23,988	24,084	1,978

Age of cases - calendar days



Nature of complaints

The business areas generating the most complaints are as follows:

Internet	13.32%
Lenders	12.12%
Direct marketing	10.32%
Telecoms	7.15%

The most frequent reasons for complaining are as follows:

Subject access	28.94%
Inaccurate data	17.55%
Unwanted telesales calls	15.51%
Disclosure of personal data	10.05%
Unwanted sales faxes	6.33%
Unwanted sales email	5.94%

Freedom of information casework

Over half of cases were resolved within a month. Over 45% were resolved informally, where the ICO brokers an agreement between the two parties. In 13% of cases, we served a decision notice. During 2006/07 we served 339 decision notices. This is a 82% increase on 2005/06 when 186 decision notices were served.

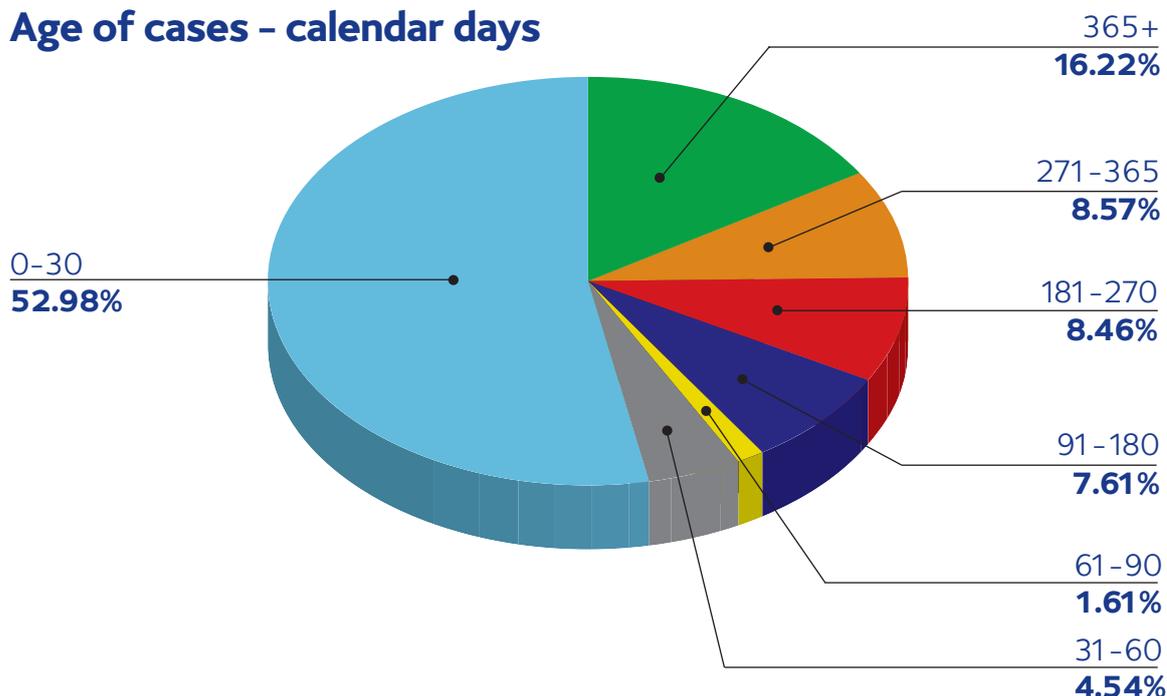
Performance against targets

Time to close cases	Target	Actual
30 days or less	35%	52.98%
90 days or less	40%	59.13%
180 days or less	50%	66.74%
365 days or less	80%	83.78%

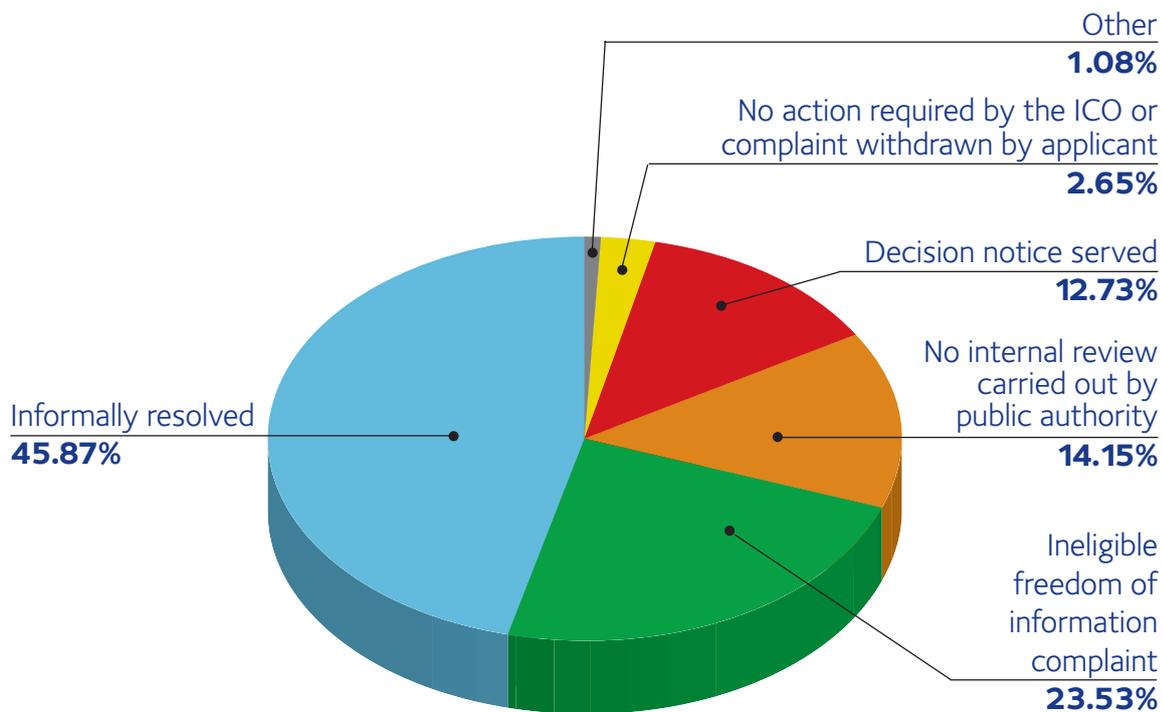
Received	Closed	Work in progress*
2,592	2,601	1,371

* Data cleansing exercises have taken place throughout the financial year which resulted in a revised carry forward figure from 2005/06 of 1,380.

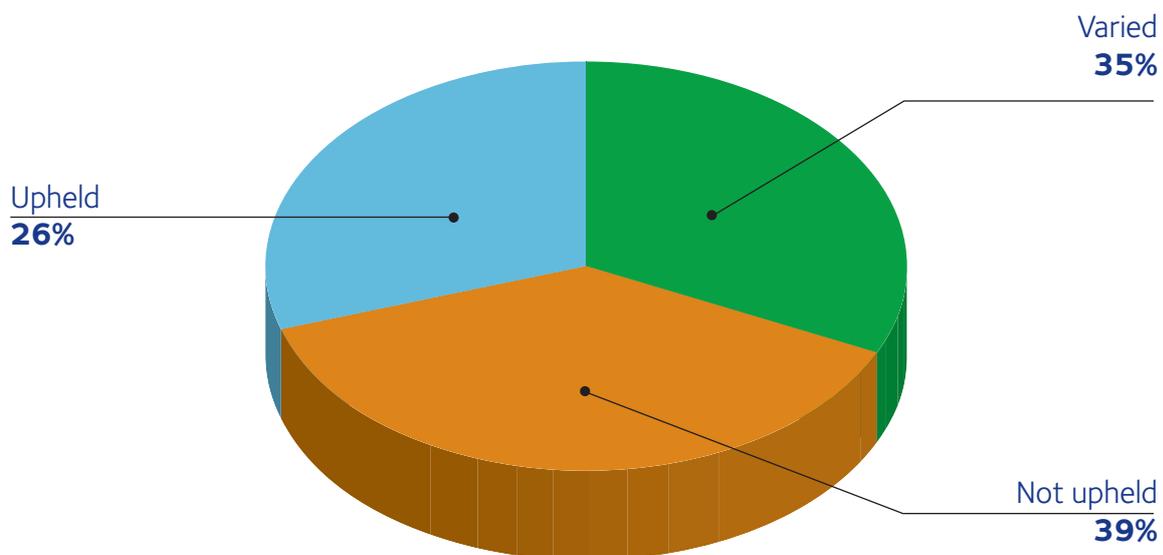
Age of cases - calendar days



Outcome of cases closed



Outcome of decision notices



92 appeals against ICO decisions were lodged with the Information Tribunal during 2006/07.

Customer satisfaction June 2006

Data protection

How do data controllers rate the quality of service overall? (base: 128)					
Excellent	Very good	Good	Fair	Poor	Don't know
9%	23%	34%	20%	15%	0%

How do individuals rate the quality of service overall? (base: 202)					
Excellent	Very good	Good	Fair	Poor	Don't know
14%	22%	20%	12%	28%	3%

Freedom of information

How do Freedom of Information practitioners rate the quality of service overall? (base: 74)					
Excellent	Very good	Good	Fair	Poor	Don't know
18%	22%	35%	12%	12%	1%

How do individuals rate the quality of service overall? (base: 26) Number giving each response					
Excellent	Very good	Good	Fair	Poor	Don't know
3	9	3	2	7	2

Requests for information received by the Information Commissioner's Office under the Freedom of Information Act 2000

The Information Commissioner is a public authority for the purposes of the Freedom of Information Act 2000. He receives requests for information held by us. An Information Requests Team administers our responses to these. Request handlers are advised by the Information Requests Board, chaired by the Director of Legal Services. In 2006/07 the ICO received 297 requests, 28% more than in the previous financial year.

A disclosure log is available on the Information Commissioner's Office website which provides access to responses to requests that are of wider public interest.

	2006/07	2005/06
Total requests received	297	232
Average number of working days taken to deal with a request	15	15
Number of internal reviews requested	24	11
Average number of working days taken to deal with a review*	18	36
Outcome of reviews		
Upheld	16	9
Overtaken	4	2
Hybrid	4	0

*The ICO's time period for responding to requests for internal reviews was 40 working days during 2005/06. This time period was reduced to 20 working days for 2006/07.

Our highlights of 2006/07

April 2006:	we hired a new HR director, Vicky Best, with the brief to modernise the ICO's HR practices.
May 2006:	we launched the campaign for custodial sentences for the illegal buying and selling of personal information, with our "What Price Privacy?" report.
May 2006:	our view that the Scottish National Party's marketing telephone calls are in breach of electronic privacy regulations is upheld by the Information Tribunal.
May 2006:	we issued our first enforcement notices under the Freedom of Information Act, requiring the government to release information on the legality of the Iraq war.
May 2006:	we hosted an international conference on freedom of information that attracted 140 delegates.
June 2006:	we issued a new policy to simplify freedom of information publication schemes, with proactive release of information as the focus of the initiative.
July 2006:	we found the B4U website in breach of the Data Protection Act and issued an enforcement notice against its use of electoral register information.
July 2006:	we issued new guidance on the transfer of personal information overseas.
July 2006:	we prosecuted a bogus caller for breaching the Data Protection Act; he is found guilty and fined £600 plus costs.
July 2006:	we prosecuted a finance company for failing to notify under the Data Protection Act. The directors were found guilty and fined £300 each plus costs.
July 2006:	we ordered the Health Protection Agency to release information about a case of Legionnaire's disease in a Malta hotel.
August 2006:	we launched our new website. www.ico.gov.uk
August 2006:	we issued new data protection guidance on direct marketing.
September 2006:	we published research which showed eight out of 10 organisations said data protection is needed.
September 2006:	we ordered the disclosure of MPs' travel expenses.
September 2006:	we ruled that Ofcom must release data on mobile phone base stations.
September 2006:	we issued new guidance on Radio Frequency Identification Tags.
October 2006:	we investigated allegations that customers' data is not properly protected in some overseas call centres.
October 2006:	we issued guidance on personal information and equality monitoring in Northern Ireland.
October 2006:	the courts ordered two men to pay back money they gained by posing as a bogus data protection agency.
November 2006:	we hosted an international conference on the "Surveillance Society". Held in London, the conference attracted 300 delegates from 30 countries, and gained national and international media coverage.
November 2006:	David Smith, our deputy commissioner for data protection, is appointed chair of Europol's data protection joint supervisory body.

November 2006:	we launched our new data protection training DVD.
November 2006:	we prosecuted a husband and wife team for the illegal obtaining of personal information. They were found guilty of 25 cases and fined over £7000 plus costs.
December 2006:	we served enforcement notices against five companies for making illegal telesales calls.
December 2006:	a man who illegally obtained and sold personal information was sentenced to 150 hours community service.
December 2006:	we ordered Derry Council to release information about an agreement with Ryanair under the Freedom of Information Act.
December 2006:	we issued our follow up report "What Price Privacy Now?" on the illegal buying and selling of information, calling for a custodial sentence for the offence.
January 2007:	we marked European Data Protection Day with the release of a series of public information films warning against identity theft.
January 2007:	we successfully prosecuted Liverpool City Council for failing to respond to an Information Notice under the Data Protection Act.
January 2007:	we required DEFRA to issue ministerial advice on salmon fishing.
January 2007:	we ordered Braintree District Council to release information on the properties it owns, and Liverpool City Council to release information relating to managed zones for prostitutes.
January 2007:	we released data protection guidance for people working with violent members of the public.
January 2007:	we released new guidance on local authorities' use of council tax information.
January 2007:	we issued guidance explaining that young people have the right to see information held about them by their school.
January 2007:	we published research showing that a fifth of the UK population believes they had been a victim of identity crime.
January 2007:	we launched our new Personal information toolkit.
January 2007:	four men sentenced to jail for their involvement in bogus data protection agencies.
February 2007:	we issued data protection guidance for political party marketing in Wales and Scotland.
February 2007:	we ruled that West Midlands Passenger Transport Executive was right to treat multiple information requests as vexatious.
February 2007:	we ordered the London Borough of Camden to release information on ASBOs.
March 2007:	the Information Commissioner spoke at the International Association of Privacy Professionals' Summit in Washington, USA.
March 2007:	we were hailed as the best data protection communicator in Europe.
March 2007:	we found 11 banks in breach of the Data Protection Act.
March 2007:	demand for our publications continued to rise – requests were up 38% over the previous year.

4 Protecting your personal information: data protection and privacy and electronic communications



The Data Protection Act and the Privacy and Electronic Communications Regulations were put in place with the aim of protecting the privacy of our personal information. This aim has solid foundations. It stems directly from the right to respect for private life enshrined in the European Convention on Human Rights. But its roots go even deeper – they are in the need we all have, to varying degrees, for a private space which we control and which is free from unwarranted intrusion.

The collection of biometrics and other personal information as a weapon in the fight against terrorism and serious crime, the increased sharing of our personal information to improve public services, and ever more inventive forms of electronic marketing, are all examples of ways in which this private space is under challenge. Legitimate aims are, for the most part, being pursued but protecting the privacy of our personal information in a measured and responsible way has never been of more importance.

The existence of a law is not, on its own, enough to achieve this. The law must be applied in practice. Effective risk-based enforcement is important but we have to go further. Delivering protection of personal information is dependent on public confidence in the law and in us. This is why we work hard to explain and apply the law in a way that is simple, sensible, easily understood and consistent with good business practice. Educating and advising individuals and businesses about their rights and responsibilities is one of our key roles. We encourage individuals to make direct use of their own legal rights and we support them in this with our complaints handling service.

Generating public confidence in the law, and a public that is confident in using its rights, is at the heart of how we approach our data protection work. We need to be influential and imaginative. This is why we also work hard to persuade those whose role impacts on data protection, whether as law makers, policy makers or business leaders, that a reduction in data protection risk is a meaningful and valid objective in its own right. It is also why we place great emphasis on our regional offices, enabling us to become increasingly influential with the devolved administrations and with our regional stakeholders.

Our Corporate Plan translates this approach into specific data protection aims. We have delivered and continue to deliver against those aims.

Resolving complaints

Through 2006/07 we provided an efficient casework and public advice service that:

- dealt with more than 23,000 written data protection enquiries and complaints from individuals and organisations throughout the UK;
- answered more than 115,000 telephone enquiries, of which more than 80% were about data protection;
- resolved complaints in high profile, high volume cases such as subject access requests to banks and web-based look-up services.

Running an efficient and helpful Notification service

During 2006/07 we increased the numbers on the register of data controllers to over 287,000 and achieved a significant increase in renewals from automatic chase-up letters.

On 18 August 2006 a Yorkshire businessman was found guilty at Bingley Magistrates Court for failing to notify as a data controller. Despite requests from the ICO, he didn't notify and was subsequently prosecuted. He was fined £300 and was ordered to pay costs of £500.

Getting tough

We are committed to using legal and other regulatory sanctions against those organisations who refuse to accept their obligations. We have adopted an approach that we believe to be firm but fair.

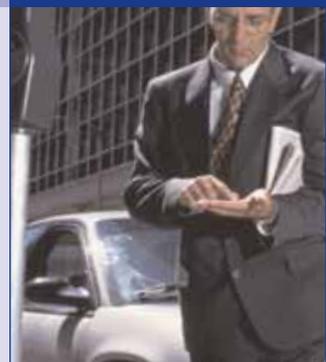
Making a difference - how we've helped

Mr X disputed Criminal Records Bureau (CRB) records that showed him having a conviction for driving with excess alcohol, even though he had proved in court that another man was using his driving licence, which he had lost. Mr X claimed that this had cost him jobs.

The CRB said that the police force concerned maintained that the record was accurate. Mr X then complained to the ICO.

He supplied official documents proving that he did not have such a conviction, and the CRB sent him a copy of its record with the inaccurate information removed.

Case study



What price privacy?

It has become increasingly clear that there is a thriving and lucrative market for personal information which has been illegally obtained. The Investigations Unit of the ICO looks into complaints about the unlawful obtaining of personal data. Section 55 of the Data Protection Act 1998 makes it an offence to unlawfully obtain, disclose or procure the disclosure of personal information knowingly or recklessly without the consent of the organisation holding the data.

One of the ICO's largest investigations was Operation Motorman, which began in November 2002. It uncovered an organised and large scale trade in personal information involving private investigators and corrupt officials who had access to personal information held by the DVLA and the police.

Those of us concerned about the rise in data collection by the state can hardly be dismissive of the Information Commissioner's determination to root out the illegal gathering and sale of personal information.

The Independent on Sunday, Sunday 17 December 2006

In May 2006, the Information Commissioner, using special powers under the Act, presented the report 'What price privacy?' to Parliament. The report called for the government to introduce a custodial sentence for individuals convicted under the Data Protection Act for unlawful obtaining, buying and selling of personal information.

The Commissioner also made proposals to organisations representing the media and the finance industry, as well as the Security Industry Authority and the Association of British Investigators. Progress with these was catalogued in a second report presented in December 2006, 'What price privacy now?'

In January 2007 the Department for Constitutional Affairs (DCA) announced the government's intention to introduce legislation bringing in a custodial sentence for individuals convicted of illegally buying or selling personal information.

Since the publication of 'What price privacy?' the Investigations Unit has concluded a number of cases where individuals have been prosecuted for unlawfully obtaining personal information:

- In July 2006 a private investigator was found guilty and fined £1,750 with £600 costs at Salisbury Magistrates Court for unlawfully obtaining personal data. The private investigator had been making telephone calls to British Telecom purporting to be a BT employee and attempted to obtain personal data of BT customers.
- In November 2006 a married couple pleaded guilty to 25 offences of unlawfully obtaining personal data following an ICO investigation. The couple asked the court to take into consideration a further 65 offences. They had obtained personal information from a number of organisations by 'blagging' the information. They also had purported to be employees of various organisations to enable them to unlawfully obtain the personal information. They were fined a total of £7,500 and ordered to pay £3,694 costs.
- In December 2006, a private investigator was sentenced to community service at Kingston upon Thames Magistrates Court after pleading guilty to the unlawful obtaining of personal data. He impersonated individuals to obtain information such as bank account details and ex-directory telephone numbers which he later sold to interested parties.

“**Businesses and government organisations were warned by the Information Commissioner yesterday that they will be pursued if they use private detective agencies to acquire financial and other personal information about individuals illegally.**”

*Financial Times,
Thursday 14 December 2006*

Making a difference – how we've helped

Mrs W asked a cosmetic surgery clinic for a copy of her treatment notes and any other documents held about her. Despite many requests she did not receive a response. The Act requires data controllers to respond promptly – definitely within a maximum 40 days of receiving the request.

After our intervention Mrs W got the information she had requested and the clinic agreed to review and update its procedures.

Case study



Protecting personal information on electoral registers

In July 2006, the ICO issued an enforcement notice against B4U Business Media Limited, operators of the B4usearch website. The notice ordered the company to stop using personal information from electoral registers published before 2002. This action resulted from many hundreds of complaints made to the ICO.

Before 2002, people had no choice over whether their personal details from the electoral register were sold on to other organisations. After that date individuals could opt out of the public register. The ICO received complaints from people who had subsequently opted out of the public register but whose details were freely available on the website.

B4U allowed people to search pre-2002 electoral registers to obtain the names and addresses of some individuals who had subsequently chosen not to be included on the public register. As a result of the ICO's intervention, information from pre-2002 electoral registers was removed from B4U's website.

Protecting the right to see information held about you

A former employee of Liverpool City Council asked the council to see some personal information they held about her. Liverpool City Council provided some information but not all so the former employee complained to the ICO.

The ICO started an investigation. Liverpool City Council failed to respond to written requests for information. As a result the ICO issued an information notice requiring the council to provide us with specified information. Again no response was received so the ICO brought a prosecution against the council.

Liverpool City Council pleaded guilty at Liverpool City Magistrate's Court on 14 December 2006. When sentencing, the District Judge said the Council had shown an "appalling breakdown of communication" and "a clear lack of compliance with the Data Protection Act 1998". The Council was fined £300 and agreed to allow the ICO to audit its data protection processes.

The importance of responding to information requests made under the Data Protection Act was highlighted last month after Liverpool City Council became the first organisation to be prosecuted for failing to comply with an information notice from the Information Commissioner's Office.

IT Week, Monday 8 January 2007

Only last month, high street banks were criticised by data protection watchdog, the Information Commissioner, for dumping documents containing customers' personal details in rubbish bags left on the street.

*Mail on Sunday,
Sunday 5 November 2006*

Protecting bank details

Following an ICO investigation into complaints concerning the disposal of customer information, 11 banks and other financial institutions were found to be in breach of the Data Protection Act.

As a result formal undertakings were signed by Alliance & Leicester, Barclays Bank, Clydesdale Bank, Co-operative Bank, HBOS, HFC Bank, Nationwide Building Society, Natwest, Royal Bank of Scotland, Scarborough Building Society, The Post Office and United National Bank. They were found to have discarded personal information in waste bins outside their premises. The Immigration Advisory Service was also found to have disposed of personal information in similar circumstances.

Stopping spam and junk mail

Individuals and organisations who do not want to receive marketing calls can register with the Telephone Preference Service – the TPS. The Privacy and Electronic Communications Regulations ban unsolicited marketing calls to people who have registered with the TPS.

The TPS and the ICO receive many complaints from individuals who have received unsolicited marketing telephone calls even though they have indicated that they do not wish to receive them.

On 5 December 2006, we issued enforcement notices against five companies who had been making unsolicited marketing calls to individuals without their consent, or to individuals who were registered with the Telephone Preference Service. The notices ordered the companies to stop telephoning individuals who had objected.

“The privacy watchdog has rapped five companies for making unwanted cold calls to householders. The ICO described the practice as ‘unacceptable’.”

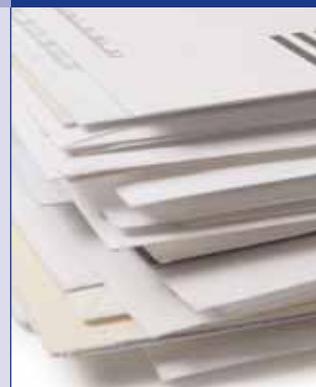
*PA Newswire,
Wednesday 6 December 2006*

Making a difference – how we’ve helped

An insurance company was sending magazines to its customers that contained direct marketing. This led to a number of complaints from customers who had previously opted out of receiving such marketing. In response the insurance company argued the magazine contained ‘service messages’ and not marketing. The matter was then referred to our remedies unit.

Case officers from the remedies unit reviewed the magazines and found the material clearly fell under the Act’s definition of direct marketing. Following discussions the company agreed to stop sending the magazine to any new customers who had opted out of marketing.

Case study



Data protection health checks

During the year we conducted eight data protection audits to assess the processing of personal data. The organisations involved, all public authorities, co-operated fully in the exercise and recognised the mutual benefits.

Our audit team, in conjunction with other EU data protection authorities, also undertook a survey of medical health insurance companies with the objective of taking a pan-European view of compliance across a single sector.

The audit programme provides us with a chance to examine, at first hand, policies and working practices and an understanding of how compliance is approached on a day to day basis. Whilst at the most simplistic level the audits raise awareness of data protection in the participating organisations, they also afford the opportunity to highlight non-compliance and make recommendations on how data protection responsibilities might better be managed.

Audit is seen as an increasingly important function of ours. In consequence we are not only looking to expand the audit unit and number of audits conducted but also to increase our powers in this area.

“Public authorities were today warned that they face prosecution if they wrongly deny people access to personal information held about them... the Information Commissioner’s Office has said it would back any individual who is struggling to obtain data from either public or private sector organisations.”

*PA News Wire,
Tuesday 9 January 2007*

Appeals to the Information Tribunal

The Information Tribunal, to whom complainants and public authorities can appeal if they are unhappy with our decision, continues to make rulings which provide useful commentary and interpretation.

TRIBUNAL RULING May 2006 – The Information Tribunal delivered a ruling which affects the way political parties canvass support. In dismissing an appeal by the Scottish National Party the Tribunal upheld the view of the Information Commissioner that the Privacy and Electronic Communications Regulations 2003 apply to political parties making appeals for funds or support.

Influencing to protect personal information

The Identity Cards Act has now passed into law. Electronic health records are on the horizon. The development of databases of children's personal information, biometric passports and the National Identity Register has stimulated substantial public debate. Transformational government is high on the public policy agenda. The protection of personal information remains a key concern for individuals as the implications of a surveillance society become more widely understood.

We have worked closely with government and others to ensure that respect for personal privacy remains a key part of policy delivery. If society is to gain the benefits of more effective use of personal information, the public's trust, participation and understanding must be maintained. Data protection

compliance ensures that this is the case. It ensures that society's use of personal information develops in a fair and transparent way, one that respects the people the information is about.

Mr Thomas is to be commended for ringing the alarm bells. While conceding that much official snooping is well-intentioned and can bring benefits, he warns that unseen, uncontrolled or excessive surveillance can foster a climate of suspicion and undermine trust.

*Daily Telegraph,
Thursday 2 November 2006*

Waking up to a surveillance society

In November we hosted the 28th International Conference of Data Protection and Privacy Commissioners in London. In a departure from previous tradition the conference focused on a single issue, the Surveillance Society. We commissioned a well-received research report on the nature of the surveillance society. This provoked much interest in the media and amongst parliamentarians. We have now developed a surveillance society action plan. This will

Making a difference - how we've helped

Mr R complained that, because of an inaccurate record on the Police National Computer, details of an historic conviction had not been deleted at the appropriate time. Mr R and his family were planning to emigrate and this error potentially impacted on his emigration application. The case was further complicated because of the introduction of new rules governing conviction details under which the convictions would be retained for policing purposes.

Following intervention by the ICO and the acknowledgement of the specific circumstances of this case the conviction details were removed.

Case study



help us to co-ordinate our efforts in relation to surveillance society issues over the forthcoming year. It will also help us to develop a consistent and concerted approach to dealing with the challenging issues that we face. The international conference provided an opportunity for Commissioners to agree on approaches and initiatives at an international level. What has become known as the 'London Initiative' was adopted. This signals a commitment by data protection authorities to focus on pragmatic effectiveness and improved communication.

Sharing personal information

Over the last year the transformation of government services through the use of technology has been high on the public policy agenda. A key component of this is the sharing of personal information. We have provided our views to Misc. 31, a Cabinet Committee on data sharing. Its aim is to develop the government's strategy on data sharing across the public sector. In particular, Misc. 31 seeks to identify barriers to sensible information sharing.

We continue to receive enquiries from public bodies and members of the public about the application of data protection law in the context of information sharing. We have met representatives of several government departments to ensure that their initiatives are carried out in a way that respects personal privacy. We have responded to consultation exercises about issues such as serious and organised crime and an index for sharing information about children.

The sharing of personal information can benefit individuals and society, for example by making services simpler to access, or by protecting the public purse more rigorously. Our approach has enabled organisations to obtain the benefits of sharing personal information whilst protecting the people the information is about. Data protection law helps organisations to strike this balance correctly. Our primary concern is to safeguard the privacy and integrity of personal information. We recognise, though, that an overly restrictive application of data protection law can lead to organisations failing to make sensible use of the information they hold. Increasingly, respect for personal privacy is being seen as an essential component of effective information sharing, not as a barrier to it.

Making a difference - how we've helped

Ms X contacted us after she discovered that her bank statements, cheque book and debit card had been posted by her bank to her ex-husband's address.

The bank had changed the contact details on his current account and in doing so altered details of all other accounts that he had, including a joint one with Ms X.

After hearing from us the bank developed a new change of address form, which asks customers whether the changes should apply to all their accounts.

Case study



ID Cards and the National Identity Register

We have been working to ensure that the practical arrangements for establishing the National Identity Register and issuing ID cards facilitate compliance with the Data Protection Act. We have been consulted by the Identity and Passport Service as their plans have developed. The Home Office has

published its National Identity Scheme Strategic Action Plan. The new plan involves biographical data gleaned from the Department for Work and Pensions National Insurance database and biometric data held by the Home Office and the Identity and Passport Service. These new arrangements pose some challenges in terms of the quality of these existing information resources, and in ensuring that the safeguards set down in the Identity Cards Act remain effective.



Safeguarding children's information

Safeguarding our children from harm and ensuring they receive proper care and support are matters of considerable public policy interest. The efforts of government and others to achieve these important objectives involve the recording of more and more information about children. This opens up the possibility of the information being shared more widely. We commissioned research into the growth of such databases, the information flows that take place and the practical use of the information. This has helped us to identify a number of areas worthy of further exploration, such as the use of information to identify children perceived as being at risk of growing up to be criminals, and arrangements for obtaining consent from children for the use of their information. This research has informed our wider work on surveillance society issues. It has helped us develop a Children Database Action Plan. This will help us to ensure that those involved in the compilation and use of information about children are fully aware of, and comply with, their data protection obligations.

Connecting for Health

Plans for the creation of a national health care record system for England has provoked debate involving health professionals and patients. It has also engaged the concerns of parliamentarians. We were pleased to provide evidence to the House of Commons Health Committee as part of its scrutiny of these new developments. Connecting for Health's intention is to create an electronic summary care record of patients' basic medical details. This will be available to those treating a patient wherever in England the treatment takes place. This has led to concerns about the quality of the information to be loaded onto the new records, and who will have access to them. We have worked closely with Connecting for Health to insist that such concerns are fully addressed. Connecting for Health are aware of the need to take patient privacy seriously. An example of this is the development of the 'sealed envelope'. This allows patients to restrict access to certain parts of their health record. Another example is the provision of an opportunity for patients to opt out.

We are continuing to work with Connecting for Health on the practical arrangements for establishing a national health care record. We want to ensure that appropriate mechanisms are in place for helping patients to exercise the choices they have, for giving them online access to their records through Health Space and for ensuring that security arrangements are effective. We will be working closely with Connecting for Health on their 'early adopter' sites to ensure that a comprehensive system of data protection safeguards is in place before the system is rolled out nationally.

Protecting information across international borders

We continue to play our role as the national supervisory authority, and as part of the joint supervisory authorities, for Europol, Customs Information System and Eurojust. We were pleased that David Smith, Deputy Commissioner, was elected for a two year term as Chair of the Europol Joint Supervisory Body. We also co-operate with our European colleagues on the supervision of Eurodac, a database of asylum seekers' fingerprints. We attend the Schengen Information System Joint Supervisory Authority as observers.

Participation in these supervisory bodies helps us to ensure that there are proper safeguards in place. However, the experience gained here, and in our other European Union co-operative activities, also helps us to provide evidence as part of parliamentary scrutiny of the proposed Data Protection Framework Decision, the United States/Europe Passenger Name Records agreement and the Treaty of Prum. The Treaty provides for greater criminal justice co-operation, including the sharing of DNA profiles.

We continue to work closely with our international colleagues, particularly at European level through our membership of the Article 29 Working Party. The Working Party has continued its efforts to bring about a harmonised approach to implementation of the European Union Data Protection Directive at national level.

Society for Worldwide Interbank Telecommunication

In June 2006 we, along with several data protection authorities in the EU and worldwide, received a complaint about alleged covert disclosure of information relating to European Union nationals by the Society for Worldwide Interbank Telecommunication (SWIFT). SWIFT is an international financial messaging service which connects institutions engaged in international financial transfers. The messages include information such as names and account numbers. The messaging process involves a transfer of information to the United States. According to the complainant, the United States Treasury had issued a number of administrative subpoenas to access this information as part of investigations into terrorist activity. The possibility that United States authorities had been given access to information about UK citizens generated a great deal of media coverage.

To investigate the complaint, we have maintained close contact with other data protection authorities. In November 2006, the Article 29 Working Party issued an opinion saying that the transfer of information to the US authorities had been undertaken in a manner contrary to fundamental data protection principles. It called for steps to be taken to ensure that even when investigating matters as serious as terrorism, the fundamental rights of citizens were respected. We continue to work with our European colleagues, as well as with SWIFT, to achieve this aim. We have asked United Kingdom financial institutions to consider what steps are needed to make sure they comply with data protection legislation.

It is reassuring to learn that Richard Thomas, the Information Commissioner, is fighting on the side of the angels against the 'surveillance society.'

*Sunday Times,
Sunday 29 October 2006*

Information, advice and guidance

We have been particularly active this year in producing advice and guidance for individuals and organisations. A pragmatic regulatory approach has focused on individuals' real concerns and has given organisations the clear, simple guidance they need to comply with data protection law.

It's your information

This year we introduced a new type of guidance for the public, called 'It's your information'. This guidance gives individuals straightforward, practical advice, particularly about exercising their legal rights.

The topics we have covered so far are:

- Stopping unwanted marketing
- Gaining access to police information
- Claiming compensation
- The use of radio frequency identification tags



Good practice notes

We have continued to publish practical and easy to understand good practice notes. They explain to organisations what they need to do to comply with the law. We have issued guidance on the following:

- Handling requests for access to personal information.
- Outsourcing data processing activities for small and medium sized businesses. This includes advice on using a company that is based abroad.
- Releasing information to prevent or detect crime.
- Automatic renewals of policies or membership using a credit or debit card.
- Advice for tied agents and independent financial advisers.
- Using the Corporate Telephone Preference Service.
- The use of violent warning markers.
- Monitoring under section 75 of the Northern Ireland Act.
- Disclosures of personal information under the Taxes Management Act.

Technical and legal guidance

Sometimes organisations want a more detailed explanation of the requirements of the law. Our technical guidance meets this need. Although technical in nature, it uses clear, plain English. This year technical guidance has been produced on:

- Privacy enhancing technologies.
- Access to pupils' information held by schools in England, Wales and Northern Ireland.
- Disclosures to members of Parliament carrying out constituency casework.
- Subject access and third party information.
- Radio frequency identification tags.
- Guidance for marketers on the Privacy and Electronic Communications (EC Directive) Regulations 2003.
- Guidance for subscribers on the Privacy and Electronic Communications (EC Directive) Regulations 2003.
- Guidance on Part 2 of the Privacy and Electronic Communications (EC Directive) Regulations 2003.
- The use of personal information held for collecting and administering council tax.
- Legal guidance on international transfers of personal information.

5 Your right to know: freedom of information and environmental information



The Information Commissioner's responsibilities under the Freedom of Information Act and Environmental Information Regulations include:

- promoting good practice by public authorities;
- informing the public about the law;
- considering complaints about any alleged breach of the law;
- issuing decision notices and exercising enforcement powers to ensure compliance with the law; and
- approving publication schemes.

The Commissioner's approach is to be independent, responsible and robust, recognising that increased transparency and accountability will encourage more effective government.

Complaints to the Commissioner

During 2005 and 2006 – the first two years' full operation of the Freedom of Information Act – the ICO received over 5,000 complaints. When we prepared our plans for 2006/07, indications were that complaints would settle at around 190 per month. However, volumes have risen, and we actually received a monthly average of 216 cases, a total of 2,592 complaints. We closed 2,601 cases, thereby preventing a rise in our caseload.

We introduced significant process and structural changes in June 2006 which enabled us to make improvements in complaints resolution. We measure the age of cases at closure against published targets. During 2006/07 we met all these targets. In particular, over 50% of all the cases we closed were dealt with in less than 30 days (the target was 35%) with 59% of all cases closed within 90 days of receipt.

Our greatest challenge continues to be the high number of complex complaints that we receive. Once accepted, these are evaluated by team leaders and then placed in a queue ready for allocation to a caseworker. We may prioritise some cases, where the complaint might be time-critical or represent a path-finder case, resolution of which could close a number of others, or give direction on a particular topic. Cases can also be grouped if there are similarities with the parties involved or the issues raised. However, individuals bringing complex cases which do not fit into these categories are still waiting too long before we can begin to consider their complaint in detail.

Whilst improvements in complaint handling have reduced the backlog of complaints, our current level of funding for this work will restrict our ability to deliver further significant improvement.

As predicted in our October 2006 progress report, during the second half of 2006/07 we closed an increased number of older cases. During

Information cannot be withheld from the public just because it might be misunderstood or risk damage to a business, the information commissioner has ruled.

*Local Government Chronicle,
Thursday 25 January 2007*

2006/07, 16% of cases closed were over one year old. As we make inroads into the older caseload, we expect this trend to continue.

The closure figures for the first half of 2006/07 were in line with the closures for the final quarter of the previous year, which showed a steep rise in output as we dealt with our backlog of more straightforward cases. By the middle of the year, these cases were cleared. This led to a reduction in total cases closed each month leaving a core of complex cases awaiting resolution. Our caseload as at 31 March 2007 stands at 1,371.

The Commissioner has signalled his intention to be tougher with public authorities now that they have had time to become familiar with the legislation. We have started using information notices and have issued our first practice recommendation, and our more robust approach will also extend to the way in which we handle investigations.

In particular, we will be more demanding of public authorities, expecting them to be able to set out full and final arguments for withholding information in one clear submission and to respond quickly to requests for information.

Many cases continue to be resolved by informal resolution, where processes of discussion, persuasion and negotiation have produced positive results.

Where we have been unable to secure a satisfactory outcome informally, we issue a decision notice. During 2006/07 we served 339 formal decision notices, an increase of over 82% from the previous year. Many of these have brought about the disclosure of important information; others have upheld the position of the public authority.



Speeding up the process

In our October freedom of information progress report to Parliament we set out the changes in process and structure that we were implementing to deal with complaints more quickly and effectively. We are now reaping the benefits of those changes.

The establishment of the case reception unit, which carries out an initial assessment of freedom of information and environmental information regulations complaints made to the office, has streamlined our processes and case handling timescales.

The establishment of sectoral teams in our complaints division has ensured greater consistency in our approach to case handling and most importantly has created an environment which lends itself to the development of expertise within the ICO in relation to specific sectors. Teams are better able to identify related cases, enabling them to investigate a lead case where the legislation hasn't yet been tested.

Our newly created policy team works closely with caseworkers and senior officers to establish policy lines and determine how to progress the new, novel and complex cases and issues which arise.

We have adopted a much more robust approach in relation to both our enforcement activity and the types of case which we will follow through to a decision notice. Our new approach is not to take up, or continue with, any Freedom of Information Act or Environmental Information Regulations case where no useful purpose would be served if we were to proceed to an adverse decision notice. For example, where the initial response was delayed from the public authority but has now been provided, or where a public authority has failed to respond, they provide the information following our intervention. In our opinion pursuing a complaint in this situation would mean that the request is frivolous or vexatious. Such cases will be closed, or dealt with in other ways if they appear to raise enforcement or similar issues. This was done on the basis that public authorities should now have a good understanding of the interpretation of the legislation, the application of the exemptions and the consideration and weighing of public interest arguments. They should also know and fully understand how to deal with requests and what they need to do in order to conform to the codes of practice. This more robust approach also makes sense in terms of making the most effective use of our resources and acting responsibly and proportionately as a regulator.

Monitoring performance

We post our service standards on our website every month. These are a statement of our commitment to improvement and a measure of our performance against those commitments.

We have agreed key performance indicators for complaint handling, and a comprehensive performance dashboard – a single sheet which summarises our performance against all the key performance indicators.



Better staff training

We have a comprehensive induction programme in place. Following a successful pilot in July 2006, new starters have received a mixture of desk and classroom training. They are all now supported with a comprehensive procedures manual and improved knowledge management tools.

Informal resolution

Many cases have been resolved by informal resolution, where a great deal of discussion, persuasion and negotiation between complainants and public authorities, have produced positive results.

For example, the ICO received a complaint after a council refused to provide the names of streets where 'safe houses' for vulnerable people (such as those who had been the victims of domestic violence) were situated. The council refused saying that to provide the relatively small number of street names could compromise the safety of those in the safe houses.

The case officer considered other similar cases and asked the council for more details of the exemption and the relevant public interest factors. After considering this information, the Commissioner agreed the information should not be disclosed. The case officer then explained his reasons to the complainant who agreed to withdraw the complaint.

In another case, a complaint was received by the ICO after a parish council refused to disclose information about the parish clerk's salary and employment.

The complaint was then withdrawn after the Commissioner proposed, and the parish agreed, to publish the pay scale rather than the precise salary.

Making a difference - how we've helped

Ms X asked a NHS Trust for a copy of a report written about her stay in hospital. The Trust said it was being looked at for official purposes and passing it to her would hinder its work.

We contacted the Trust and, after discussing this, it was agreed that providing a copy would not after all cause a problem. The Trust sent Ms X the report - and reviewed its procedures based on our advice.

Case study



Decision notices

As part of the ICO's work to improve the quality of decision notices, the newly-established policy team checks notices for consistency against our established policy lines, noting any development of existing policy or novel point addressed in the decision.

We have acted on feedback from practitioners and have now improved the standard of drafting. We have also developed a decision notice template to give a clearer structure to more complex decisions, where there are often multiple issues of fact and law to explain. This enables the parties to better understand our reasoning and make a more informed decision whether to accept or appeal our ruling.

The layout of decision notices has also been improved following user feedback, so it is easier to pick out the key issues and the decision itself. This enhances the value of the decision notice as an educative tool for public authorities and other users of freedom of information.

Following feedback from users, we designed a decision notices database for inclusion in our new website, which was launched in August 2006. The database allows swift retrieval of the notices, which are searchable by case reference number, name of public authority, section of the Act, date (month and year) and status (upheld or not).

July 2006 DECISION NOTICE	The Information Commissioner ordered the Department for Trade and Industry (DTI) to release information relating to its four year investigation into allegations that British American Tobacco has been involved in smuggling in the third world.
September 2006 DECISION NOTICE	The Information Commissioner served a decision notice under the Environmental Information Regulations ordering Ofcom to provide all data on mobile phone base stations held within its Sitefinder database.
September 2006 DECISION NOTICE	The Information Commissioner upheld two complaints under the Freedom of Information Act following information requests to the Treasury and the Office of Government Commerce for the Gateway Reviews of the identity cards programme and the programme's traffic light status.
October 2006 DECISION NOTICE	The Information Commissioner ruled, in the circumstances, that Epsom and St Helier University Hospitals NHS Trust were right to refuse access to a deceased patient's records under freedom of information.
November 2006 DECISION NOTICE	Under the Environmental Information Regulations 2004 the Information Commissioner has ordered Doncaster Metropolitan Borough Council to release specified details of aircraft noise levels for November 2005 resulting from aircraft movements at Robin Hood Airport.
November 2006 DECISION NOTICE	The Information Commissioner decided that the Department of Health incorrectly applied exemptions and ordered that the Wells report into the National Health Service University be released within 35 days
December 2006 DECISION NOTICE	The Information Commissioner decided that the BBC was wrong to argue the Act did not apply to them when a complainant asked how much its staging of the Children in Need charity appeal programme cost in 2005 - and how much individual presenters including Terry Wogan, Eamonn Holmes and Natasha Kaplinsky were paid.
December 2006 DECISION NOTICE	The Information Commissioner upheld a Freedom of Information complaint against The National Archives relating to the 1911 census. The Commissioner stressed that this decision must be confined to the circumstances relating to the information requested in this case. It was not a decision that the entirety of the 1911 census must now be disclosed, nor did it create a precedent for other requests for information within the 1911 or other census schedules.
January 2007 DECISION NOTICE	The Information Commissioner ordered Defra to release ministerial advice concerning salmon fishing on the River Teign in Devon. The Commissioner considered the arguments put forward by Defra but also found that there were strong public interest arguments in favour of releasing the information. For instance, making the information public would help demystify the process by which a minister is informed of, and arrives at, a decision on an environmental issue. It would also promote greater transparency and accountability of decision making in government. Furthermore, the material may well be of interest to people in the local area, especially as any change in the use of the river could affect the local economy.
February 2007 DECISION NOTICE	The Information Commissioner published two decision notices ordering two local authorities to disclose how pension funds are being invested. The Commissioner concluded the information should be disclosed because, in these instances, the public interest in knowing that public funds are being invested wisely overrides the public interest in protecting confidentiality.
March 2007 DECISION NOTICE	The Information Commissioner ordered the London Borough of Camden to release details of the identities of some residents who have been made the subject of Anti-Social Behavioural Orders (ASBOs).

Handling vexatious requests

While giving full support to individuals seeking to exercise the right to know responsibly, we are sympathetic towards public authorities receiving specific requests which impose a heavy burden on their resources, particularly where the public interest in the disclosure of the information is limited. The Freedom of Information Act recognises that there are limits to compliance beyond which public authorities are not obliged to go and we encourage the appropriate use of these provisions by public authorities. We will shortly be developing further guidance on vexatious requests.

In March 2007 the Information Commissioner ruled that the BBC was justified in refusing requests for information under the Freedom of Information Act on the grounds that the requests were vexatious. Following the introduction of the right to know in January 2005, the BBC received

approximately 90 requests relating to the authority's hospitality expenditure and employee expenses claims during a short period of time.

In February 2007 the Information Commissioner concluded that the West Midlands Passenger Transport Executive (Centro) was entitled to refuse to answer a request for information on the grounds that it was vexatious. Between January and November 2005 the same person made 15 requests concerning the authority's financial relationship with four bus companies.

The Information Commissioner has concluded that Centro, the West Midlands Passenger Transport Executive, was entitled to refuse a freedom of information request on the grounds that it was 'vexatious'.

*Coach & Bus Week,
28 February 2007*

Cost limits

From a total of over 500 Decision Notices we have issued since January 2005, 20 related to complaints where the cost limit was an issue. Several of these cases also involved a failure by the public authority to give appropriate advice and assistance to the requester to enable the request to be modified, so as to bring it within the cost limit. In all but two of these cases the ICO was satisfied that there was evidence to support the estimate for compliance with the full request, so the decision that the cost limit would be exceeded was justified.

DECISION NOTICE **December 2006** - The complainant requested information concerning submissions made to the Scott Inquiry. The Ministry of Defence stated that it was not possible to confirm or deny whether information relevant to the request was held without exceeding the relevant cost limit of £600. The Commissioner accepted that to be the case.



Appeals to the Information Tribunal

The Information Tribunal, to whom complainants and public authorities can appeal if they are unhappy with our decision, continues to make rulings which provide useful commentary and interpretation.

Since 1 January 2005, 27% (127) of our decision notices have been appealed. Of those cases that have concluded, the outcomes were as follows:

Appeals withdrawn	32% (17 cases)
Appeal dismissed	47% (25 cases)
Appeal allowed/partially allowed	21% (11 cases)

The Tribunal has substituted the Commissioner's decision in seven of the cases it has ruled on. Public authorities brought 23% (29 cases) of the appeals and complainants 77% (98 cases).

TRIBUNAL RULING February 2007 – The Information Tribunal ordered the release of details of MPs' travel expenses. This upheld an earlier decision of the Information Commissioner.

In his original ruling the Commissioner recognised MPs are entitled to a private life, but as the information relates to individuals acting in an official, rather than a private, capacity it is clearly a matter of public interest.

TRIBUNAL RULING December 2006 – The Information Tribunal dismissed Derry City Council's freedom of information appeal and ruled that the council should disclose details of an agreement between Derry City Airport and Ryanair. The ruling upholds a decision made by the Information Commissioner's Office.

TRIBUNAL RULING January 2007 – The Information Tribunal ordered the BBC to release the minutes of their governors' meeting from 28 January 2004. These contained details of discussions concerning Greg Dyke's resignation from the BBC a few days earlier. The BBC had been resisting publication for two years, saying that its board would be inhibited in future discussions if members knew their comments would be published.

In overruling the BBC (and the ICO) the tribunal said there was a strong public interest in knowing why the governors had decided to press for Mr Dyke's resignation.



Making a difference - how we've helped

Mr X complained to the ICO after a local council had refused to disclose names and assessments of companies who had tendered for council work.

The ICO case officer proposed the council release a list of those who had tendered for the work and anonymised versions of the assessment forms.

The council accepted the idea and Mr X withdrew his complaint.

Case study



International conference



In May 2006 we hosted the fourth International Conference of Information Commissioners. Over 140 delegates attended from 40 countries, including Information Commissioners, non governmental organisations, and freedom of information academics and practitioners. Delegates heard from the Slovenian Information Commissioner, the New Zealand Ombudsman, the European Ombudsman and the Director at the Office of Information and Privacy in the US Department of Justice.

Promoting good practice

The Freedom of Information Act places a duty on the Commissioner to promote good practice among public authorities, and to promote observance of the Act and related codes of practice. These provisions also apply in relation to the Environmental Information Regulations.

The focus of the Good Practice team is to liaise with public authorities and key stakeholders. The new team concentrates on:

- using existing networks and establishing new ones;
- developing and approving publication schemes;
- encouraging good practice; and
- developing guidance and memoranda of understanding.

The team continues to contribute to relevant events and conferences, and to answer enquiries.

Modernising publication schemes

Following a review of publication schemes, work is already underway to improve and develop our model schemes with the aim of encouraging the pro-active, consistent, voluntary release of routine information.

MPs had claimed [to release] the information would be a breach of their privacy but were ordered to open their books by Information Commissioner Richard Thomas.

*Daily Mail,
Wednesday 14 February 2007*

Previously, our approval of publication schemes expired four years after the date of approval. We have now decided to extend that to 2008 and are using this time to help train public authorities to improve their schemes. Public authorities are being encouraged to provide uncomplicated and swift access to information they can routinely make available.

Sector-specific guides will be produced which will include lists of core information that should be released as well as notes on good practice.

Guidance

Throughout the year we have published a number of pieces of guidance to help public authorities and individuals including:

- using the procedural codes of practice
- lifecycle of a request
- time limits for consideration of the public interest test
- time limits for internal review
- basic guide to compliance for first tier councils
- access to information about the deceased

Enforcement

We are now adopting a stronger regulatory approach, particularly in relation to those authorities guilty of systemic or repeated breaches of the Freedom of Information Act or the Environmental Information Regulations.

We launched our freedom of information Enforcement Strategy in October 2006. This aims to achieve compliance with the legislation and observance of the Codes through a combination of advice, negotiation and formal action. We continue to monitor the performance of public authorities and non-compliance issues are normally dealt with informally in the first instance. We are increasingly using information notices where the public authority is reluctant to cooperate and these have resulted in the release of information needed to progress complaints resolution.

February 2007 – We issued our first practice recommendation to Nottingham City Council indicating the steps needed to achieve compliance.

6 Our regional offices

Through regional offices we are gaining a better understanding of the needs of the devolved administrations and our regional stakeholders



Scotland

The work of the ICO's Scotland office is largely focused on data protection, as most public authorities operating in Scotland are subject to separate Scottish freedom of information legislation. The period 2006/07 was the first full year in post for Ken Macdonald, the Assistant Commissioner for Scotland, and substantial effort was put towards the establishment of good working relationships with key stakeholders and promoting good data protection practice within organisations in all sectors.

The Scottish Parliament has legislative competence in a wide range of areas concerning personal privacy and a series of seminars was held in May and June which raised awareness of data protection to the billing and clerking teams at the Parliament. Submissions have been made to a range of Parliamentary consultations on issues such as DNA retention, the naming of child sex offenders and pre-employment disclosure checks to protect vulnerable groups. Our views were taken into account in the subsequent recommendations and the adopted legislation.

The approach to information sharing in the public sector in Scotland is being led by the Scottish Executive and co-ordinated through a National Data Sharing Forum which meets twice-yearly. The forum members include representatives from local authorities, health boards and other agencies; the ICO is represented at it by the Assistant Commissioner who attends with observer status. The Executive is also developing policies relating to the sharing of child protection and the ICO is working closely with it on the production of an associated Code of Practice.

The Scotland office continues to attend a number of sector-specific data protection groups, including ACPOS (police) and SOLAR (local government), where issues of mutual concern can be discussed and good practice promoted. In addition, over the past year, we delivered presentations at over 20 seminars and conferences, allowing us to pass our key messages to a wider audience.



Wales

The Wales office is headed by Assistant Commissioner Anne Jones. Freedom of information casework relating to Welsh public authorities forms much of the work undertaken by the office, as does the provision of advice on data protection and freedom of information issues. Three-quarters of all enquiries received relate to data protection, and slightly more enquiries were received from members of the public than from organisations.

The Wales office has continued its programme of raising awareness of information rights during the year, and has had input to several initiatives, including the Welsh Assembly's 'Making the Connections' strategy, which focuses on citizen-centred public sector services. Other significant involvement has been with 'Informing Healthcare', the Welsh electronic health records programme, WASPI (the Wales Accord on the Sharing of Personal Information), and umbrella bodies representing local and town councils. In total, Wales office staff have spoken at almost 50 conferences, seminars and meetings with local stakeholders over the year.

One of the main events of the year was the move to new premises in Cardiff Bay in mid-November. The new office represents a much improved resource, and is already providing new opportunities to work with local organizations and businesses. A reception was held just before Christmas to mark the event, which local stakeholders attended.

The new Government of Wales Act 2006 was implemented in May this year and will bring significant changes to the way the region is governed. It will also impact on the work of the Welsh regional office in that increasing levels of Wales-only legislation will require more partnership working with the Welsh Assembly Government.

The office continues to translate key guidance into the Welsh language in accordance with the requirements of the newly approved Welsh Language Scheme, with further implementation planned for the coming year.



Northern Ireland

The Northern Ireland regional office is headed by Assistant Commissioner Marie Anderson. Freedom of information casework relating to Northern Ireland public authorities forms much of the work undertaken by the office, as does also the provision of advice on information rights generally. In 2006/07 we dealt with 835 enquiries, with nearly two-thirds relating to data protection issues. Most of our enquiries came from the public, although we also provide advice and guidance to public authorities, the private sector and other groups.

We continued to promote information rights, and spoke at more than 60 events. In October 2006, the Northern Ireland regional office presented a review of our first fully operational year at a well attended stakeholder event in the Northern Ireland Assembly. We also launched much needed guidance for Northern Ireland public authorities on equality monitoring. In February 2007 we launched the ICO's "Personal information toolkit" in Northern Ireland to coincide with European Data Protection Day. Marie Anderson appeared on local radio to discuss data protection and identity theft, which led to an increase in enquiries and requests for the Personal information toolkit.

The Northern Ireland regional office continued to investigate Freedom of information complaints and we also saw our first challenge in the Information Tribunal, when Derry City Council appealed against a decision notice. The Commissioner had ordered disclosure of a contract between Derry City Airport and low cost airline, Ryanair. The Tribunal's ruling was especially significant because it clarified the application of the exemption for information provided in confidence in the context of public sector contracts. The office continues to deal with the more complex and politically sensitive cases arising locally. An example of this is the detailed investigation into a request for information about the Northern Bank robbery in December 2005. Some of this information was released as a result of the intervention of the Commissioner and he found that the public authority, the Northern Ireland Office, had properly withheld the more sensitive documents.



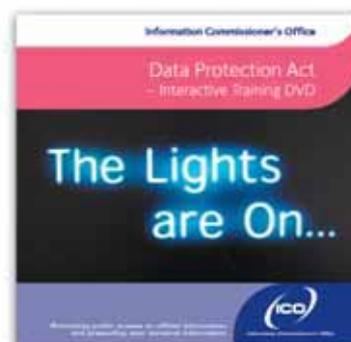
7 Improving our communications



The highlight of the year was launching our new website www.ico.gov.uk in August 2006. In response to user feedback, we produced material aimed more specifically at individuals or organisations, improved the navigation and provided more information about the ICO. The new site allows people to find out about data protection and freedom of information matters as they occur in real life, by following links on topics such as credit, health, housing, education and junk mail. Similarly, people with data protection and freedom of information responsibilities at work are able to follow links on the most frequent areas of need, such as employment, setting up a new business, and marketing.



This year also saw the start of a new programme of publications, designed to fill gaps in the information we provide, and to offer the right level of information for users' needs. Highlights for data controllers include a new training DVD, "The lights are on", to help people get data protection right in the workplace, as well as a new guide to notification. For individuals, the ICO launched a "Personal information toolkit" in January, to mark European Data Protection Day. The booklet was designed to help people protect their personal information,



and was promoted by a set of public information adverts. We also launched a new series of consumer fact sheets called "It's your information", which focus on data protection matters in everyday situations. This is a staplemate for the now established Good Practice Notes we produce for data controllers, which continue to attract the attention of trade and specialist media.



We distributed over 306,000 publications altogether, a rise of about 38% over last year. Our most popular leaflet remains “Credit explained”, a consumer guide to personal information and credit (we sent out over 72,000 copies). “Your guide to openness”, our guide to freedom of information, remained in the top five most requested publications, with around 40,000 being distributed. In response to customer requests for more information about the ICO, we launched a quarterly e-newsletter, as well as two leaflets on what the ICO does and the legislation we cover.

Wide-reaching media coverage of data protection and freedom of information stories demonstrates a high level of public interest in the issues. Freedom of information and environmental information decision notices continued to provide a steady source of media stories covering topics as broad as empty council properties, ministerial advice on salmon fishing, MPs’ expenses and aircraft noise. Our international data protection conference in London in November, which focused on the topic of the Surveillance Society, gave rise to significant national and international media coverage. Overall, the ICO generated over 1,500 media items in 2006/07 reaching a combined audience of over 356 million.

Efforts to improve our communications are paying off. More people are now aware of their data protection rights (82% of individuals compared to 76% last year). Awareness of freedom of information rights among individuals remains high at 73%. Awareness among practitioners is very high: 94% are aware of data protection rights (compared to 91% last year) and 97% are aware of freedom of information rights.

We have continued to improve our internal communications by launching a new internal communications strategy. Central to this was the development of an intranet, a corporate style guide and a corporate identity. Training has also started to help managers improve their role as communicators.

8 Our people



We have seen significant changes and improvements in our approach to Human Resources (HR) in the last year. In April 2006, Vicky Best, our new HR Director, joined the ICO, started a full review of the HR function and developed a comprehensive HR strategy. This strategy covers a range of initiatives to improve and develop the profile of the HR function and the ICO as a whole. The aim is to ensure that our approach to recruitment, leadership and development is professional. It emphasises our commitment to building, rewarding and retaining a diverse, highly skilled and motivated workforce. Another important theme has been the development of new ways of working in the context of moving away from the traditional personnel model to a strategic, performance-focused HR service.

New policies

We have already made substantial progress and have implemented new HR policies and procedures which cover areas such as dignity at work, managing sickness absence and performance management. We have established new ways of working which have improved our effectiveness in the way we attract and recruit new staff to the organisation. We have developed and implemented a competency framework which will be linked to recruitment, learning and development and the performance management process.

Developing leadership

We have started a significant leadership development programme which is predominantly aimed at senior managers in the organisation. This is a bespoke programme, developed from the results of a skills audit. The programme will focus on developing leadership and management skills such as coaching, managing performance and personal effectiveness.

Developing staff

The ICO is committed to providing effective and appropriate learning and development opportunities for all staff. This year, we have built upon successes of previous years and have provided a wide range of learning and development opportunities. As well as the leadership development programme, we have delivered training to managers on the new HR policies and health and safety, and provided job specific training to ensure that our staff have the right skills and knowledge. We have also developed a new staff induction programme because we recognise that a good induction for new staff is of fundamental importance to the success of the organisation. We have also supported a number of staff to gain professional qualifications through further education.

Unfortunately, we have not made as much progress as we had planned in the area of equality and diversity. We have developed a strategy and action plan and will focus next year on delivering our commitments in this area. The completion of the pay and grading review has also taken longer than was originally intended. This work is now complete and we will learn lessons from this experience.

9 ICO infrastructure



Information technology

The long term managed services agreement with Fujitsu expires in 2007 and cannot be renewed. As a result, the year has been dominated by a project to procure IT services. This was completed in May 2007 when the Commissioner agreed a new five year agreement with Alfred McAlpine Business Services Ltd.

The procurement has provided an opportunity to ensure services are well defined and meet our business needs now and in the immediate future. Considerable effort is being made to ensure our in-house team is well prepared to manage the new agreement.

During the year our work focused on developing the functionality and supporting infrastructure of our core applications and internet environment to meet current business priorities. For example, we developed online knowledge bases to support casework staff in the decision making process. In addition developments have taken account of lessons learned, particularly from the early experience of handling freedom of information cases. The changes improved our ability to produce detailed management information.

A further development in the year has been the decision to establish an in-house IT forensics unit to support the work of our investigations team.

A project was launched during the year with the objective of improving the ability of our staff to work remotely, but in a secure environment. It takes advantage of a new service offering from the Government Secure Intranet (GSI) framework agreement.



Records management software (Meridio) is an integral part of our casework management system. During the year the ICO assessed whether there are business benefits in exploiting the use of Meridio further and, in particular, using it for the management of the ICO's corporate documents and records. As a result of a successful pilot the ICO will be extending the use of this software in 2007/08.

Accommodation

The ICO has accommodation on seven different sites. During 2006/07, the Wales office moved to its new permanent location, we re-negotiated the lease on our storage facility and expanded our Northern Ireland estate to house additional staff.

The main office in Wilmslow required considerable imaginative space planning in order to meet business requirements and to accommodate new temporary and permanent staff. There is now no more room for additional staff.

Plans to take additional accommodation in Wilmslow were shelved due to financial constraints, but the ICO continues to seek a cost effective way of moving the main office to one site.

The environment

All used paper is confidentially shredded on site and recycled. This includes archive files for which four recycling days are held each year. Newspapers and cardboard are also recycled. In 2006/07 our recycling saved 162 trees, an increase of 25% over the previous year.

We use paper from well managed sustainable forests, controlled sources and recycled wood or fibre. Low energy light bulbs are used throughout our offices, and our vending machines contain Fair Trade tea & coffee.



10 Corporate governance



The Information Commissioner, Richard Thomas, reports directly to Parliament. As accounting officer he is directly responsible for safeguarding the public funds for which he has charge, for propriety and regularity in the handling of those public funds, and for the day to day operations and management of his office.

The Commissioner is supported by his Management Board which is responsible for providing strategic direction and corporate governance. The Board meets every quarter and comprises members of his Executive Team and four non-executive directors:

Dr Robert Chilton

David Clarke

Sir Alistair Graham

Clare Tickell

The Executive Team is responsible for office-wide leadership, articulation of policies and ensuring the office is effectively and efficiently well-managed. The Executive Team meets approximately every fortnight. In addition to the Commissioner its members are:

Vicky Best - Director of Human Resources

Simon Entwisle - Chief Operating Officer

Susan Fox - Director of Communications and External Relations

David Smith - Deputy Commissioner, data protection

Graham Smith - Deputy Commissioner, freedom of information

Nick Tyler - Director of Legal Services

The Commissioner is also supported by an Audit Committee which is responsible for scrutiny, oversight and assurance of risk control and governance procedures. The Committee comprises:

Dr Robert Chilton

David Clarke

Graham Smith

Key achievements and changes 2006/07

Richard Thomas was re-appointed as Information Commissioner for a further two years, until June 2009, providing continuity of leadership for his office.

The corporate governance arrangements, introduced in summer 2005, were reviewed during 2006/07 and were found to be working well. In addition, a business planning policy and procedure were agreed which resulted in a new more focused format for the ICO's 2007/08 business plan, in addition to the publication of the Corporate Plan 2007 – 2010.

Risk management policies and procedures were also reviewed during the year, resulting in a refreshed corporate risk register and the development of business unit risk registers.

11 Prosecutions

Defendant	Offence	Court	Date of Hearing	Plea	Result	Sentence	Costs
Ram Finance and Insurance Services Ltd	Section 17	Nottingham Magistrates Court	12 July 2006	Guilty	Convicted	Conditional discharge 3 yrs	Nil
Rosella Yaro	Section 17	Nottingham Magistrates Court	12 July 2006	Guilty	Convicted	Fine £300	£300
Yohanna Yaro	Section 17	Nottingham Magistrates Court	12 July 2006	Guilty	Convicted	Fine £300	£300
Asud Iqbal	Section 17	Leeds Magistrates Court	18 August 2006	Guilty	Convicted	Fine £200	£150
Yusuf Badat	Section 17	Leeds Magistrates Court	18 August 2006	Guilty	Convicted	Fine £200	£150
Ashfaq Anjum	Section 17	Leeds Magistrates Court	18 August 2006	Guilty	Convicted	Fine £200	£150
Acorn Accounting Company Ltd	Section 17	Leeds Magistrates Court	18 August 2006	Guilty	Convicted	Fine £300	£150
Stephen Anderson	Section 55 (unlawful obtaining etc of personal data) (obtaining & selling x 3, obtaining x 4, selling x 4) (plus a further 46 offences taken into consideration)	Huntingdon Magistrates Court	14 November 2006	Guilty	Convicted	Fine £300 x 11 = £3,300	£3,694
Sharon Anderson	Section 55 (obtaining & selling x 3, attempted obtaining x 3, disclosing x 4, obtaining x 4) (plus a further 51 offences taken into consideration)	Huntingdon Magistrates Court	14 November 2006	Guilty	Convicted	Fine £300 x 14 = £4,200	£3,694
Ishvarial Mistry	Section 17	Bradford Magistrates Court	7 December 2006	Guilty	Convicted	Fine £250	£1,059
Brian Grove	Section 17	Kidderminster Magistrates Court	12 December 2006	Guilty	Convicted	Fine £100	£75

Defendant	Offence	Court	Date of Hearing	Plea	Result	Sentence	Costs
Anthony Gerald Clifford	Section 55 x 16 Section 17 x 1	Kingston upon Thames Magistrates Court	12 December 2006	Guilty	Convicted	18 months probation + 150 hours community service	£2,000
Liverpool City Council	Section 47 (failed to comply with Information Notice)	Liverpool City Magistrates Court	14 December 2006	Guilty	Convicted	Fine £300	Nil
Abdul Ghafoor	Section 17	Bingley Magistrates Court	5 January 2007	Not Guilty	Convicted	Fine £350	£500

Number of premises search warrants applied for – 7
Number of cautions administered – 5

The Information Commissioner's Office

Accounts

for the year ended 31 March 2007

Foreword	60
Statement of the Information Commissioner's responsibilities	68
Statement on internal control	69
Certificate and report of the Comptroller and Auditor General to the Houses of Parliament	73
Income and expenditure account	76
Balance sheet	77
Cashflow statement	78
Notes to the accounts	79



Information Commissioner's Office



Foreword

History

On 12th June 2003 responsibility for the Information Commissioner passed to the newly created Department for Constitutional Affairs. Previously, responsibility for the Information Commissioner passed to the Lord Chancellor's Department from the Home Office following the Machinery of Government changes announced in June 2001.

Following implementation of the Data Protection Act 1998 on 1 March 2000, the corporation sole by the name of Data Protection Registrar, established by the Data Protection Act 1984, continued in existence but under the name Data Protection Commissioner.

The Freedom of Information Act 2000 received Royal Assent on 30 November 2000. The title of Data Protection Commissioner changed to Information Commissioner with effect from 30 January 2001.

The Information Commissioner is sponsored by the Ministry of Justice established on 9 May 2007, replacing the Department for Constitutional Affairs.

Statutory background

The Information Commissioner's main responsibilities and duties are under the Data Protection Act 1998, the Freedom of Information Act 2000, the Environmental Information Regulations 2004 and the Privacy and Electronic Communications (EC Directive) Regulations 2003.

The Information Commissioner is not a typical non-departmental public body. Such bodies usually have a relationship with Ministers which is based on the delegation of ministerial powers. The Commissioner is an independent body created by statute that reports directly to Parliament. The Commissioner is required to carry out those functions laid down in the Data Protection Act 1998 and Freedom of Information Act 2000, using only those powers which these Acts set out. The Commissioner's decisions are subject to the supervision of the Information Tribunal and the courts.

The Information Commissioner is responsible for setting the priorities for his Office, for deciding how they should be achieved, and is required annually to lay before each House of Parliament a general report on performance.

Annual accounts and audit

The annual accounts have been prepared in a form directed by the Secretary of State for Constitutional Affairs with the consent of the Treasury in accordance with paragraph (10)(1)(b) of Schedule 5 to the Data Protection Act 1998.

Under paragraph (10)(2) of Schedule 5 to the Data Protection Act 1998 the Comptroller and Auditor General is appointed auditor to the Information Commissioner. The cost of audit services in the year was £21,000 (2005/06: £20,000) and no other assurance or advisory services were provided.

So far as the Accounting Officer is aware, there is no relevant audit information of which the Comptroller and Auditor General is unaware, and the Accounting Officer has taken all the steps that he ought to have taken to make himself aware of relevant audit information and to establish that the Comptroller and Auditor General is aware of that information.

Senior management

A list of senior managers is set out in Section 10 of the published Annual Report.

Pension liabilities

The treatment of pension liabilities is set out in the Remuneration report on pages 64–67, and Note 4 to the Accounts.

Employee policies

The Commissioner's equal opportunities policy aims to ensure that no potential or actual employee receives more or less favourable treatments on the grounds of race, colour, ethnic or national origin, marital status, sex, sexual orientation, age, religious belief or disability. To further this policy the Information Commissioner's Office (ICO) promotes the observance of good employment practice particularly where relevant to disabled people.

The Commissioner has an Equality Scheme approved by the Northern Ireland Equality Commissioner, produced as part of his responsibilities under section 75 of the Northern Ireland Act 1999.

The Information Commissioner continues to place importance on ensuring priority is given to the provision of appropriate training so that staff can develop skills and understanding of their roles in line with the aims and objectives of the ICO. A full-time training officer has been in place throughout the year.

Maintenance of the provision of information to, and consultation with, employees continues to be managed through a newsletter, staff intranet and regular meetings with Trade Union representatives, and briefings for all staff were held to ensure staff were being kept up to date with the significant changes affecting the ICO. A formal Health and Safety Policy Manual is available to all members of staff and a Health and Safety Committee is in place to address health and safety issues.

Changes in fixed assets

During the year £572,836 was spent on information services upgrading the applications and infrastructure provided for the IT network. £51,403 was spent on the refurbishment of newly leased premises in Cardiff, and £79,032 was spent on office machinery and upgrading telephony.

Creditor payment policy

The Information Commissioner has adopted a policy on prompt payment of invoices which complies with the 'Better Payment Practice Code' as recommended by government. In the year ended 31 March 2007, 98.3% (31 March 2006: 97.8%) of invoices were paid within 30 days of receipt or, in the case of disputed invoices, within 30 days of the settlement of the dispute. The target percentage was 95%.

Management commentary

A detailed review of activities and performance for the year of the ICO is set out in sections 1 to 11 of the published Annual Report.

Financial performance

Grant-in-aid

Freedom of information expenditure continued to be financed by a grant-in-aid from the Department for Constitutional Affairs (DCA), and for 2006/07 £5,550,000 (2005/06: £5,100,000) was drawn down.

Under the conditions of the Framework Document between the Information Commissioner and the DCA up to 2% of the annual grant-in-aid can, with the prior consent of the DCA, be carried forward to the following financial year. At the end of the financial year an amount of £6 (2005/06: £97,576 1.9%) was carried forward for expenditure in 2007/08 with the permission of the DCA.

There are no fees collected in respect of freedom of information type activities.

Fees

Expenditure on data protection activities is financed through the retention of the fees collected from data controllers who notify their processing of personal data under the Data Protection Act 1998.

The annual notification fee is £35, and has been unchanged since it was introduced on 1 March 2000.

Fee income collected in the year was £10,204,761 (2005/06: £9,655,060) representing an increase of almost 5.7% over the previous year. This information is provided for fees and charges purposes, rather than compliance with SSAP 25.

Under the conditions of the Framework Document between the Information Commissioner and the DCA, fees 'cleared' through the banking system, up to an amount of 3% of the expenditure of data protection activities can be carried forward for expenditure to the following financial year. At the end of the financial year an amount of £301,467 (3%) (2005/06: £111,426 (1.2%)) was carried forward for expenditure in 2007/08, as was a further £159,236 (2005/06: £159,620) of 'un-cleared' fees.

Accruals outturn

There was a retained deficit for the year of £7,439,909. This result is largely brought about due to the change in the accounting policy for grant-in-aid which resulted in £5,550,000 of grant-in-aid received in the year being taken to the Income and Expenditure Reserve rather than the Income and Expenditure Account. In addition, accruals of both income and expenditure have contributed to the year-end position, although on a cash basis the ICO has stayed within target.

The accounts continue to be prepared on a going concern basis as a non-trading entity continuing to provide public sector services. Grant-in-aid has already been included in the DCA's estimate for 2007/08, which has been approved by Parliament, and there is no reason to believe that future sponsorship and future parliamentary approval will not be forthcoming.

Treasury management

Under the terms of the Framework Document between the Information Commissioner and the DCA, the Commissioner is unable to borrow or to invest funds speculatively.

Fee income is collected and banked into a separate bank account, and cleared funds are transferred weekly to the Information Commissioner's administration account to fund expenditure.

In accordance with Treasury guidance on the issue of grant-in-aid that precludes non-departmental public bodies from retaining more funds than are required for their immediate needs, grant-in-aid is drawn in quarterly tranches. In order not to benefit from holding surplus funds, all bank interest and sundry receipts received are appropriated in aid to the Secretary of State for Constitutional Affairs on a quarterly basis.



Richard Thomas, Information Commissioner

11 June 2007



Remuneration report

Remuneration policy

The remuneration of the Information Commissioner is set in accordance with a motion made pursuant to Standing Order 118(6) (Standing Committees on Delegated Legislation) and is increased annually on 1st April, by the average percentage by which the mid-points of the senior civil service pay bands increase.

The remuneration of senior civil servants is set by the Prime Minister following independent advice from the Review Body on Senior Salaries.

The salary of the Information Commissioner is paid directly from the Consolidated Fund in accordance with paragraph 3(5) of Schedule 5 to the Data Protection Act 1998.

The remuneration of staff and other officers is determined by the Information Commissioner with the approval of the Secretary of State for Constitutional Affairs.

In reaching the determination, the Information Commissioner and Secretary of State for Constitutional Affairs have regard to the following considerations:

- the need to recruit, retain and motivate suitably able and qualified people to exercise their different responsibilities;
- government policies for improving the public services;
- the funds available to the Information Commissioner;
- the government's inflation target and Treasury pay guidance.

Service contracts

Unless otherwise stated below, staff appointments are made on merit on the basis of fair and open competition, and are open-ended until the normal retiring age of 60. Early termination, other than for misconduct, would result in the individual receiving compensation as set out in the Civil Service Compensation Scheme.

Non-Executive Board Members are paid an annual salary of £12,000 and are appointed on fixed term contract periods expiring on 18 June 2009.

Directorships and other significant interests held by Board Members which may conflict with their management responsibilities

A Register of Interests is maintained for the Information Commissioner, his two Deputy Commissioners and his four Non-Executive Board Members, and is published on the Commissioner's website www.ico.gov.uk.

Salary and pension entitlements

The following sections provide details of the remuneration and pension interests of the Information Commissioner and the most senior officials employed by the Information Commissioner.

Remuneration

Salary	2006/07 £'000	2005/06 £'000
Richard Thomas, Information Commissioner	95-100	95-100
David Smith, Deputy Commissioner	60-65	25-30 (Full year equivalent 60-65)
Graham Smith, Deputy Commissioner	70-75	70-75

Salary

'Salary' comprises gross salary and any other allowance to the extent that it is subject to UK taxation.

Benefits in kind

None of the above received any benefits in kind during 2006/07.

Pension benefits

	Accrued Pension at age 60 as at 31 March 2007 and related lump sum £'000	Real increase in pension and related lump sum at age 60 £'000	CETV at 31 March 2007 £'000	CETV at 31 March 2006 £'000	Real increase in CETV £'000
Richard Thomas Commissioner	30-35	0-2.5	584	540	21
David Smith Deputy Commissioner	25-30 +lump sum 75-80	2.5-5 +lump sum 10-15	523	435	70
Graham Smith Deputy Commissioner	5-10 +lump sum 15-20	0-2.5 +lump sum 2.5-5	92	75	14

Partnership pensions

There were no employer contributions for the above executives to partnership pension accounts in the year.

Civil service pensions

Pension benefits are provided through the Civil Service pension arrangements. The scheme is a defined benefit scheme, which prepares its own scheme statements. From 1 October 2002, employees may be in one of three statutory based 'final salary' defined benefit schemes (classic, premium, and classic plus). The schemes are unfunded with the cost of benefits met by monies voted by Parliament each year. Pensions payable under classic, premium, and classic plus are increased annually in line with changes in the Retail Prices Index. New entrants after 1 October 2002 may choose between membership of premium or joining a 'money purchase' stakeholder arrangement with a significant employer contribution (partnership pension account).

Employee contributions are set at the rate of 1.5% of pensionable earnings for classic and 3.5% for premium and classic plus. Benefits in classic accrue at the rate of 1/80th of pensionable salary for each year of service. In addition, a lump sum equivalent to three years' pension is payable on retirement. For premium, benefits accrue at the rate of 1/60th of final pensionable earnings for each year of service. Unlike classic, there is no automatic lump sum (but members may give up (commute) some of their pension to provide a lump sum). Classic plus is essentially a variation of premium, but with benefits in respect of service before 1 October 2002 calculated broadly in the same way as classic.

The partnership pension account is a stakeholder pension arrangement. The employer makes a basic contribution of between 3% and 12.5% (depending on the age of the member) into a stakeholder pension product chosen by the employee from a selection of approved products. The employee does not have to contribute but where they do make contributions, the employer will match these up to a limit of 3% of pensionable salary (in addition to the employer's basic contribution). Employers also contribute a further 0.8% of pensionable salary to cover the cost of centrally-provided risk benefit cover (death in service and ill health retirement).

Further details about the Civil Service pension arrangements can be found at the website www.civil-service-pensions.gov.uk

Cash Equivalent Transfer Values

A Cash Equivalent Transfer Value (CETV) is the actuarially assessed capitalised value of the pension scheme benefits accrued by a member at a particular point in time. The benefits valued are the member's accrued benefits and any contingent spouse's pension payable from the scheme. A CETV is a payment made by a pension scheme or arrangement to

secure pension benefits in another pension scheme arrangement when the member leaves a scheme and chooses to transfer the benefits accrued in their former scheme. The pension figures shown relate to the benefits that the individual has accrued as a consequence of their total membership of the pension scheme, not just their service in a senior capacity to which disclosure applies. The CETV figures, and from 2003/04 the other pension details, include the value of any pension benefit in another scheme or arrangement which the individual has transferred to the Civil Service pension arrangements and for which the Civil Superannuation Vote has received a transfer payment commensurate with the additional pension liabilities being assumed. They also include any additional pension benefit accrued to the member as a result of their purchasing additional years of pension service in the scheme at their own cost. CETVs are calculated within the guidelines and framework prescribed by the Institute and Faculty of Actuaries.

Real increase in CETV

This reflects the increase in CETV effectively funded by the employer. It takes account of the increase in accrued pension due to inflation, contributions paid by the employee (including the value of any benefits transferred from another pension scheme or arrangement) and uses common market valuation factors for the start and end of the period.

A handwritten signature in blue ink that reads "Richard Thomas". The signature is written in a cursive style with a prominent horizontal line underlining the name.

Richard Thomas, Information Commissioner

11 June 2007

Statement of the Information Commissioner’s responsibilities

Under paragraph 10 (1) (b) of Schedule 5 to the Data Protection Act 1998 the Information Commissioner is required to prepare in respect of each financial year a statement of account in such form as the Secretary of State for Constitutional Affairs may direct. The accounts are prepared on an accruals basis and must give a true and fair view of the Information Commissioner’s state of affairs at the year end and of his income and expenditure, recognised gains and losses and cash flows for the financial year.

In preparing the accounts the Information Commissioner is required to:

- observe the Accounts Direction issued by the Secretary of State for Constitutional Affairs with the approval of the Treasury, including the relevant accounting and disclosure requirements, and apply suitable accounting policies on a consistent basis;
- make judgements and estimates on a reasonable basis;
- state whether applicable accounting standards have been followed, and disclose and explain any material departures in the financial statements;
- prepare the financial statements on the going concern basis, unless it is inappropriate to presume that the Information Commissioner will continue in operation.

As the senior full-time official, the Commissioner carries the responsibilities of an Accounting Officer. His relevant responsibilities as Accounting Officer, including his responsibility for the propriety and regularity of the public finances and for keeping of proper records, are set out in the Non-Departmental Public Bodies’ Accounting Officer Memorandum, issued by the Treasury and published in Government Accounting.



Statement on Internal Control

1. Scope of responsibility

As Information Commissioner and Accounting Officer, I have responsibility for maintaining a sound system of internal control that supports the achievement of the policies, aims and objectives of the ICO, whilst safeguarding the public funds and assets for which I am personally responsible, in accordance with the responsibilities assigned to me in Government Accounting.

As Accounting Officer, I work with my Executive Team of senior managers to develop and implement the plans of the ICO, allocate resources and delegate financial and managerial authority to senior staff and others as appropriate. The Management Board decides and advises on issues of strategic importance, makes decisions on matters involving significant expenditure and receives regular reports on financial and operational performance. The Management Board is also involved in the management of risk at a strategic level, considering major factors that could prevent the Office's objectives being achieved.

The ICO is funded from the vote of the Department for Constitutional Affairs, partly from grant-in-aid and partly from data protection fee income. I am designated as Accounting Officer by the Department's Principal Accounting Officer. I advise the Department on the discharge of my responsibilities in connection with income and expenditure in accordance with the terms of an agreed Framework Document. In addition there is a programme of formal liaison meetings with the Department for Constitutional Affairs and reports are circulated as appropriate.

2. The purpose of the system of internal control

The system of internal control is designed to manage risk to a reasonable level rather than to eliminate all risk of failure to achieve the policies, aims and objectives. It can therefore only provide reasonable and not absolute assurance of effectiveness. The system of internal control is based on an ongoing process designed to identify and prioritise the risks to the achievement of the policies, aims and objectives of the ICO, to evaluate the likelihood of those risks being realised and the impact should they be realised, and to manage them efficiently, effectively and economically. The system of internal control has been in place for the year ended 31 March 2007 and up to the date of approval of the annual report and accounts, and accords with Treasury Guidance.

3. Capacity to handle risk

As Accounting Officer I acknowledge my overall responsibility for the effective management of risk throughout the ICO.

Much work has been done during 2006/07 in updating and formalising the risk management policy, ensuring it links with the business planning process and refreshing corporate risks. This has meant that the content of the Corporate Risk Register was not regularly updated from July 2006 through to the end of March, but following facilitated sessions with the Executive Team and representatives of the senior leadership group, has now been refreshed with a more rigorous approach to the external and internal risks facing the ICO. At the close of the financial year registers that identify, assess and set out mitigating actions to significant risks are in place at a corporate level, and for specific projects. In addition various business units are developing individual risk registers.

The management and review of the risks identified are led at Executive Team level within each business area, in particular through the quarterly reviews of progress against the business plan. These reports compare performance with key performance indicators in the business plan and describe activities that have been completed. They also note any variances against the business plan and highlight planned significant activities for the next quarter.

Significant risks are considered by the Management Board and Audit Committee through the corporate risk register which covers the entire organisation.

4. The risk and control framework

The risk strategy utilises the following processes to identify, evaluate and control risk:

The continued development and maintenance of risk registers. This includes reviewing the major risks facing the organisation. Risks that threaten the achievement of the objectives for the ICO are identified and analysed in terms of impact and likelihood, and are reported on quarterly via the corporate risk register to the Management Board and the Audit Committee. Risk registers are also maintained for certain projects as a mechanism for identifying and controlling risks, and significant risks are channelled into the corporate risk register.

Ownership of each risk is assigned to a named individual responsible for the active management of that risk. Risk management is incorporated into the decision making processes.

The other key elements in the control system are regular management information, a comprehensive budgeting system with an annual budget which is approved at Board level, regular reviews by the Management Board and Executive Team of periodic and annual financial reports and a system of delegation and accountability. The ICO continues to embed risk management into key business processes such as business planning, performance and project management and policy making. The system of internal control continues to be supported by a Fraud Policy and a 'Whistle-Blowing' policy for confidential reporting of staff concerns.

5. Review of effectiveness

As Accounting Officer, I have responsibility for reviewing the effectiveness of the system of internal control. My review of the effectiveness of this system is on-going throughout the year and is informed by the work of the internal auditors (PricewaterhouseCoopers) and the executive managers within the ICO who have responsibility for the development and maintenance of the internal control framework, and comments made by external auditors in their management letter and other reports. I have been advised on the implications of the results of the review by the Board and the Audit Committee and plans are in place to address weaknesses and ensure continuous improvement of the system.

Although no significant systemic internal control issues were raised during the year, the effectiveness of the ICO's risk management and payroll arrangements were a concern. Risk management is referred to at section 3 of this statement. Payroll is dealt with below.

The Executive Team is conscious that salaries constitute the largest single item of expenditure for ICO. During 2006-07 it became clear that the service from the ICO's external pay provider was unacceptably poor and that arrangements for salary forecasting were in need of reform to ensure that forecasts were as accurate and reliable as possible. A new pay provider has been engaged with effect from April 2007 and clear lines of responsibility and improved working arrangements have been established for salary forecasting.

Other areas for potential improvement highlighted by the internal auditors included estates management, procurement and contracts, and demand and resource forecasting. The Executive Team is responding to the recommendations that have been made.

More generally:

The Management Board meets five times a year and on a quarterly basis its agenda includes the subject of risk management and internal control. The Board also looks at management information relating to key performance indicators for the ICO as a whole. These relate to operational performance in respect of both data protection and freedom of information casework as well as current and projected data protection fee income.

The Executive Team meets approximately every two weeks, and is responsible for office-wide leadership, articulation of operational policies and ensuring the office is efficiently and effectively managed. The Executive Team also consider performance against the ICO business plan. Formal reports are prepared by the Executive Team member responsible every quarter.

The Audit Committee is chaired by a Non-Executive Board Member and attended by internal auditors (PricewaterhouseCoopers) and external auditors (National Audit Office). It reports to me as the Accounting Officer on the adequacy of audit arrangements and on the implications of assurances provided in respect of risk and control. It considers all audit reports and recommendations and the formal management responses.

The internal auditors have a direct line of communication to me as the Accounting Officer. In addition the internal auditors regularly report to the Audit Committee in accordance with government internal audit standards, including their independent opinion on the adequacy and effectiveness of the ICO's system of internal control. The internal auditors also provide an annual statement which expressed the view that, in the areas they scrutinised this year, established procedures were broadly adequate to meet management's overall objectives, and that controls were generally operating satisfactorily with those areas of potential improvement highlighted. It is especially reassuring that the internal auditors were able to conclude that the ICO was well managed, keen to improve and took account of audit recommendations.

A handwritten signature in blue ink that reads "Richard Thomas". The signature is written in a cursive style with a prominent initial 'R' and a long horizontal stroke underlining the name.

Richard Thomas, Information Commissioner

11 June 2007



The Certificate and Report of the Comptroller and Auditor General to the Houses of Parliament

I certify that I have audited the financial statements of the Information Commissioner for the year ended 31 March 2007 under the Data Protection Act 1998. These comprise the Income and Expenditure Account, the Balance Sheet, the Cashflow Statement and Statement of Recognised Gains and Losses and the related notes. These financial statements have been prepared under the accounting policies set out within them. I have also audited the information in the Remuneration Report that is described in that report as having been audited.

Respective responsibilities of the Information Commissioner and Auditor

As described on page 68, The Information Commissioner is responsible for preparing the Annual Report, the Remuneration Report and the financial statements in accordance with the Data Protection Act 1998 and directions made thereunder by the Secretary of State for Constitutional Affairs with the approval of Treasury and for ensuring the regularity of financial transactions. These responsibilities are set out in the Statement of the Information Commissioner's Responsibilities.

My responsibility is to audit the financial statements and the part of the Remuneration Report to be audited in accordance with relevant legal and regulatory requirements, and with International Standards on Auditing (UK and Ireland).

I report to you my opinion as to whether the financial statements give a true and fair view and whether the financial statements and the part of the Remuneration Report to be audited have been properly prepared in accordance with the Data Protection Act 1998 and directions made thereunder by the Secretary of State for Constitutional Affairs with the Approval of Treasury. I report to you if, in my opinion, certain information given in the Annual Report is consistent with the financial statements. I also report whether in all material respects the expenditure and income have been applied to the purposes intended by Parliament and the financial transactions conform to the authorities which govern them. In addition, I report to you if the Information Commissioner has not kept proper accounting records, if I have not received all the information and explanations I require for my audit, or if information specified by HM Treasury regarding remuneration and other transactions is not disclosed.

I review whether the Statement on Internal Control reflects the Information Commissioner's compliance with HM Treasury's guidance, and I report if it does not. I am

not required to consider whether this statement covers all risks and controls, or form an opinion on the effectiveness of the Information Commissioner's corporate governance procedures or its risk and control procedures.

I read the other information contained in the Annual Report and consider whether it is consistent with the audited financial statements. I consider the implications for my report if I become aware of any apparent misstatements or material inconsistencies with the financial statements. My responsibilities do not extend to any other information.

Basis of audit opinions

I conducted my audit in accordance with International Standards on Auditing (UK and Ireland) issued by the Auditing Practices Board. My audit includes examination, on a test basis, of evidence relevant to the amounts, disclosures and regularity of financial transactions included in the financial statements and the part of the Remuneration Report to be audited. It also includes an assessment of the significant estimates and judgements made by the Information Commissioner in the preparation of the financial statements, and of whether the accounting policies are most appropriate to the Commissioner's circumstances, consistently applied and adequately disclosed.

I planned and performed my audit so as to obtain all the information and explanations which I considered necessary in order to provide me with sufficient evidence to give reasonable assurance that the financial statements and the part of the Remuneration Report to be audited are free from material misstatement, whether caused by fraud or error and that in all material respects the expenditure and income have been applied to the purposes intended by Parliament and the financial transactions conform to the authorities which govern them. In forming my opinion I also evaluated the overall adequacy of the presentation of information in the financial statements and the part of the Remuneration Report to be audited.

Opinions

Audit Opinion

In my opinion:

- the financial statements give a true and fair view, in accordance with the Data Protection Act 1998 and directions made thereunder by the Secretary of State for Constitutional Affairs with the approval of Treasury, of the state of the Information Commissioner's affairs as at 31 March 2007 and of its deficit for the year then ended;
- the financial statements and the part of the Remuneration Report to be audited have been properly prepared in accordance with the Data Protection Act 1998 and directions made thereunder by the Secretary of State for Constitutional Affairs with the approval of Treasury; and
- the information given within the Annual Report is consistent with the financial statements.

Audit Opinion on Regularity

In my opinion, in all material respects the expenditure and income have been applied to the purposes intended by Parliament and the financial transactions conform to the authorities which govern them.

I have no observations to make on these financial statements.



John Bourn,
Comptroller and Auditor General,
26 June 2007

National Audit Office,
157-197 Buckingham Palace Road,
Victoria London SW1W 9SP

Income and expenditure account for the year ended 31 March 2007

	Note	2006/07		2005/06 RE-STATEd	
		£	£	£	£
Income					
Operating income	2	9,898,052		9,421,325	
Other income	3	26,222		14,852	
			9,924,274		9,436,177
Staff costs	4	8,353,825		7,158,834	
Other operating costs	5	6,928,451		6,268,098	
Depreciation of tangible fixed assets	7	2,050,724		1,910,033	
Loss on disposal of fixed assets		-		6,410	
Unrealised loss on tangible fixed assets	11	4,961		555,778	
			(17,337,961)		(15,899,153)
Operating deficit			(7,413,687)		(6,462,976)
Interest receivable	6		53,115		50,250
Notional cost of capital	1.7		30,330		(107,188)
Deficit for the year before appropriations			(7,330,242)		(6,519,914)
Notional cost of capital	1.7		(30,330)		107,188
Appropriations due (total)	6		(79,337)		(5,038,368)
Retained deficit for the year			(7,439,909)		(11,451,094)

Comparatives have been re-stated as explained in note 18. The notes on pages 79 to 91 form part of these accounts.

Statement of recognised gains and losses

	Note	2006/07		2005/06 RE-STATEd	
		£	£	£	£
Net gain on revaluation of fixed assets	11		164,236		25,307

Comparatives have been re-stated as explained in note 18, though there is no cumulative effect to report arising from the prior year adjustment.

There were no material acquisitions or disposals in the year.

The notes on pages 79 to 91 form part of these accounts.

Balance Sheet as at 31 March 2007

		31 March 2007		31 March 2006 RE-STATED	
	Note		£		£
Fixed assets					
Tangible fixed assets	7		3,280,534		4,468,712
Current assets					
Debtors and prepayments	8	514,163		517,420	
Cash at bank and in hand	9	472,224		380,894	
		986,387		898,314	
Creditors—amounts falling due within one year	10	(5,929,871)		(5,437,212)	
Net current (liabilities)			(4,943,484)		(4,538,898)
Net (liabilities)			(1,662,950)		(70,186)
Reserves					
Income and expenditure reserve	11	(1,852,493)		(95,493)	
Revaluation reserve	11	189,543		25,307	
			(1,662,950)		(70,186)

Comparatives have been re-stated as explained in note 18.
The notes on pages 79 to 91 form part of these accounts.



Richard Thomas, Information Commissioner
11 June 2007

Cashflow Statement for the year ended 31 March 2007

		31 March 2007		31 March 2006 RE-STATEd	
	Note		£		£
Net cash outflow from operating activities	12		(4,729,177)		(3,796,026)
Returns on investment and servicing of finance					
Interest received			53,115		50,250
Capital expenditure and financial investment					
Payment to acquire tangible fixed assets	7		(703,271)		(1,010,519)
Net cash outflow before financing			(5,379,333)		(4,756,295)
Financing					
Grant-in-aid received	11	5,550,000		5,100,000	
Appropriations made	6	(79,337)		(193,903)	
			5,470,663		4,906,097
Increase in cash			91,330		149,802

Comparatives have been re-stated as explained in note 18

Notes to the Accounts

1 Statement of accounting policies

1.1 Accounting convention

These accounts have been prepared in accordance with an Accounts Direction issued by the Secretary of State for Constitutional Affairs, with the approval of the Treasury, in accordance with paragraph (10)(1)(b) of Schedule 5 to the Data Protection Act 1998

These accounts shall give a true and fair view of the income and expenditure, and cashflows, for the financial year, and state of affairs at the year-end. The accounts are prepared in accordance with The Government Financial Reporting Manual for 2006-07 and other guidance which the Treasury has issued in respect of accounts which are required to give a true and fair view, except where agreed otherwise with the Treasury, in which case the exception is described in the notes to the accounts.

These accounts have been prepared under the historical cost convention, as modified by the inclusion of fixed assets at current cost. The accounts meet the accounting and disclosure requirements of the Companies Act 1985 and the accounting standards issued or adopted by the Accounting Standards Board to the extent that those requirements are appropriate.

Going concern

These accounts have been prepared on a going concern basis. For non-trading entities in the public sector, the anticipated continuation of the provision of a service in the future, as evidenced by the inclusion of financial provision for that service in published documents is normally sufficient evidence of going concern. The Government Financial Reporting Manual states sponsored entities whose balance sheet show total net liabilities should prepare their financial statements on the going concern basis unless, after discussion with their sponsors, the going concern basis is deemed inappropriate.

1.2 Grant-in-aid

Grant-in-aid is received from the Department for Constitutional Affairs to fund expenditure on freedom of information responsibilities, and is credited to the income and expenditure reserve upon receipt.

The prior year adjustment (note 18) relates to a change in accounting policy for grant-in-aid under the Government Financial Reporting Manual (FReM), which now requires grant-in-aid to be taken direct to the Income and Expenditure Reserve rather than via the Income and Expenditure Account.

1.3 Fee income

Fee income is received from notifications made under the Data Protection Act 1998, and is retained as operating income.

The notification is paid in advance for a period of one year, and a proportion of this income is therefore deferred and released back to the Income and Expenditure Account over the fee period.

1.4 Tangible fixed assets

Assets are capitalised as fixed assets if they are intended for use on a continuous basis, and their original purchase cost, on an individual basis, is £2,000 or more. Fixed assets (excluding assets under construction) are valued at net current replacement cost by using appropriate indices published by National Statistics, when the effect of re-valuing assets over time is material.

1.5 Depreciation

Depreciation is provided on all fixed assets on a straight-line basis to write off the cost or valuation evenly over the asset's anticipated life. A full year's depreciation is charged in the year in which an asset is brought into use. No depreciation is charged in the year of disposal.

The principal rates adopted are:

Leasehold improvements over the remaining life of the lease

Equipment and furniture 5–10 years

Information technology 5 years

Assets under construction nil

1.6 Stock

Stocks of stationery and other consumable stores are not considered material and are written off to the Income and Expenditure Account as they are purchased.

1.7 Notional charges

A notional charge reflecting the cost of capital employed in the year is included in the Income and Expenditure Account along with an equivalent reversing notional income to finance the charge. The charge is calculated using the Treasury's discount rate of 3.5% applied to the mean value of capital employed during the year.

1.8 Salary of the Information Commissioner

The salary and pension entitlements of the Information Commissioner are paid directly from the Consolidated Fund as a standing charge, and is included within Staff costs and also as a credit to the Income and Expenditure reserve.

1.9 Pension contributions

Pension contributions are charged to the Income and Expenditure in the year of payment.

1.10 Operating leases

Amounts payable under operating leases are charged to the Income and Expenditure Account on a straight-line basis over the lease term, even if these payments are not made on such a basis.

1.11 Value added tax

Most activities of the Information Commissioner are outside of the scope of VAT. Irrecoverable VAT is charged to the relevant expenditure category, or included in the capitalised purchase cost of fixed assets. Where output tax is charged or input tax is recoverable the amounts are stated net of VAT.

2 Operating income

Fees collected under the Data Protection Act 1998

	2006/07 £	2005/06 RE-STATED £
Deferred income at 1 April 2006	5,207,000	4,973,265
Fee receipts	10,204,761	9,655,060
Deferred income at 31 March 2007	(5,513,709)	(5,207,000)
	<u>9,898,052</u>	<u>9,421,325</u>

Comparatives have been re-stated as explained in note 18

3 Other income

Other income is appropriated-in-aid to the Department for Constitutional Affairs

	2006/07 £	2005/06 £
Legal fees recovered	12,333	9,106
Travel expenses recovered	13,781	5,346
Other	108	400
	<u>26,222</u>	<u>14,852</u>

4 Staff costs

Staff costs were:

	2006/07 £	2005/06 £
Wages and salaries	6,816,118	5,834,519
Social security costs	440,767	390,374
Other pension costs	1,096,940	933,941
	<u>8,353,825</u>	<u>7,158,834</u>
	Number	Number
Staff with a permanent UK employment contract with the Information Commissioner	243	230
Other staff engaged on the objectives of the Information Commissioner	19	15
	<u>262</u>	<u>245</u>

The salary and pension entitlements of the Information Commissioner are paid directly from the Consolidated Fund as a standing charge. Included in staff costs above are costs of £132,909 (2005/06: £130,573).

The Principal Civil Service Pension Scheme (PCSPS) is an unfunded multi-employer defined benefit scheme. The Information Commissioner is unable to identify its share of the underlying assets and liabilities. The Scheme Actuary (Hewitt Bacon Woodrow) valued the scheme as at 31 March 2003. You can find details in the resource accounts of the Cabinet Office: Civil Superannuation (www.civil-service-pensions.gov.uk).

For 2006/07, employer contributions of £1,087,058 were payable to the PCSPS (2005/06: £927,103) at one of four rates in the range 17.1 to 25.5 per cent of pensionable pay, based on the salary bands (the rates in 2005/06 were between 16.2 and 24.6 per cent). The Scheme Actuary reviews employer contributions every four years following a full scheme valuation. From 2007/2008 salary bands will be revised; however the rates will remain the same.

The contribution rates are set to meet the cost of the benefits accruing during 2006/07 to be paid when the member retires, and not the benefits paid during this period to existing pensioners.

Employees can opt to open a partnership pension account, a stakeholder pension with an employer contribution. Employer's contributions of £9,213 (2005/06: £6,483) were paid to one or more of a panel of three appointed stakeholder pension providers. Employer's contributions are age-related and range from 3 to 12.5 per cent of pensionable pay. Employers also match employee contributions up to 3 per cent of pensionable pay. In addition, employer's contributions of £669 (2005/06: £355), 0.8 per cent of pensionable pay, were payable to the PCSPS to cover the cost of the future provision of lump sum benefits on death in service and ill health retirement of these employees.

No contributions were due or prepaid to partnership providers at the balance sheet date.

No individuals retired early on health grounds during the year.

5 Other operating costs

	2006/07	2005/06
	£	£
Accommodation (rent, rates and services)	1,126,717	1,085,000
Office supplies, printing and stationery	206,349	291,490
Carriage and telecommunications	107,231	115,388
Travel, subsistence and hospitality	435,968	416,213
Staff recruitment	142,799	183,671
Specialist assistance, consultancy and policy research	558,692	476,988
Communications and external relations	1,861,782	1,343,110
Legal costs	290,449	155,528
Staff training, health and safety	378,314	392,061
Information services	1,797,544	1,787,349
Vehicle expenses	1,606	1,300
Audit fee	21,000	20,000
	6,928,451	6,268,098

Included above are operating lease payments for land and buildings of £606,060 (2005/06: £573,141)

6 Appropriations

	2006/07	2005/06
	£	£
(accruals terms)		
Interest received	53,115	50,250
Other income	26,222	14,852
Prepaid appropriations at 31 March 2006	-	4,973,266
Appropriations due per Income and Expenditure account	<u>79,337</u>	<u>5,038,368</u>
(cash terms)		
Interest receivable	53,115	50,250
Other income	26,222	14,852
Fee receipts	-	128,801
Appropriations made per Cashflow Statement	<u>79,337</u>	<u>193,903</u>

7 Tangible fixed assets

	Leasehold improvements	Equipment & Furniture	Information technology	Total
	£	£	£	£
Cost or valuation				
At 1 April 2006	467,039	365,611	7,467,760	8,300,410
Additions	51,403	79,032	572,836	703,271
Revaluation	18,614	(16,786)	(472,652)	(470,824)
At 31 March 2007	<u>537,056</u>	<u>427,857</u>	<u>7,567,944</u>	<u>8,532,857</u>
Depreciation				
At 1 April 2006	116,758	242,205	3,472,735	3,831,698
Charged in year	59,241	68,157	1,923,326	2,050,724
Revaluation	11,261	(11,825)	(629,535)	(630,099)
At 31 March 2007	<u>187,260</u>	<u>298,537</u>	<u>4,766,526</u>	<u>5,252,323</u>
Net Book Value				
At 31 March 2007	<u>349,796</u>	<u>129,320</u>	<u>2,801,418</u>	<u>3,280,534</u>
At 31 March 2006	<u>350,281</u>	<u>123,406</u>	<u>3,995,025</u>	<u>4,468,712</u>

Tangible fixed assets of £13,649 (2005/06: £106,971) have not been capitalised and are included within 'Other operating costs', as the individual costs were below the capitalisation costs of £2,000. Information Services are outsourced through a managed service agreement. The current contract with Fujitsu Services Limited expires in July 2007. The title of hardware and software procured under the current agreement is owned by Fujitsu Services Limited. The Information Commissioner is entitled to purchase the title of such assets for a nominal sum on expiry of the contract. A new contract with Alfred McAlpine Business Services Limited, for a period of 5 years expiring in July 2012 has been signed.

Information technology includes software licences procured under the managed services agreement, and as such are not separately disclosed as intangible assets.

8 Debtors

	31 March 2007 £	31 March 2006 £
Other debtors	14,146	30,655
Prepayment	500,017	486,765
	514,163	517,420
Split:		
Other Central Government bodies	-	19,696
Bodies external to Government	514,163	497,724
	514,163	517,420

9 Cash at bank and in hand

	31 March 2007 £	31 March 2006 £
Balance at 1 April	380,894	231,092
Increase in cash	91,330	149,802
Balance 31 March	472,224	380,894
Split:		
Commercial banks	470,421	379,649
Cash in hand	1,803	1,245
	472,224	380,894

10 Creditors; amounts falling due within one year

	31 March 2007 £	31 March 2006 £
Other taxes and social security	2,611	2,005
Trade creditors	171,883	67,513
Other creditors	32,220	27,548
Accruals and deferred fee income	5,723,157	5,340,146
	5,929,871	5,437,212
Split:		
Other Central Government bodies	81,306	29,612
Bodies external to Government	5,848,565	5,407,600
	5,929,871	5,437,212

11 Reserves

	Income and Expenditure reserve £	Revaluation reserve £	Total £
Balance at 1 April 2006	(95,493)	25,307	(70,186)
Retained deficit for the year (excluding unrealised loss on revaluation of tangible fixed assets)	(7,434,948)	-	(7,434,948)
Grant-in-aid from the Department for Constitutional Affairs	5,550,000	-	5,550,000
Consolidated Fund standing charge – Information Commissioner’s salary	132,909	-	132,909
Net (loss)/gain on revaluation of fixed assets	(4,961)	164,236	159,275
Balance at 31 March 2007	(1,852,493)	189,543	(1,662,950)

Opening balances have been re-stated as explained in note 18.

12 Reconciliation of operating surplus to net cash inflow from operations

	2006/07 £	2005/06 £
Operating deficit for the year	(7,413,687)	(6,462,976)
Depreciation charged in the year	2,050,724	1,910,033
Loss on disposal of assets	-	6,410
Loss on revaluation of fixed assets	4,961	555,778
Consolidated fund standing charge - Information Commissioner's salary	132,909	130,573
Reduction/(Increase) in debtors relating to operating activities	3,257	(90,929)
Increase in creditors relating to operating activities	492,659	155,085
Net cash outflow from operating activities	(4,729,177)	(3,796,026)

13 Commitments under operating leases

	31 March 2007 £	31 March 2006 £
Land and buildings		
Expiry within 1 year	-	3,584
Expiry within 2 to 5 years	-	-
Expiry thereafter	530,381	502,364
	530,381	505,948

The leases of land and buildings are subject to periodic rent reviews.

14 Capital commitments

There were no capital commitments outstanding at 31 March 2007 (31 March 2006: £nil).

15 Related party transactions

The Information Commissioner confirms that he had no personal or business interests which conflict with his responsibilities as Information Commissioner.

The Department for Constitutional Affairs is a related party to the Information Commissioner. During the year no related party transactions were entered into, with the exception of providing the Information Commissioner with grant-in-aid and the appropriation-in-aid of sundry receipts.

In addition the Information Commissioner has had various material transactions with other Central Government bodies. These transactions have been with the Central Office of Information (COI) and the Home Office Pay and Pensions Service (HOPPS).

None of the key managerial staff or other related parties has undertaken any material transactions with the Information Commissioner during the year.

16 Financial instruments

Financial Reporting Standard 13, Derivative and other Financial Instruments: Disclosures, requires disclosure of the role which financial instruments have had during the year in creating or changing the risks an entity faces in undertaking its activities. Because of the non-trading nature of its activities and the way in which central government sector entities are financed, the Information Commissioner is not exposed to the degree of financial risk faced by business entities.

Moreover, financial instruments play a much more limited role in creating or changing risk than would be typical of the listed companies to which Financial Reporting Standard 13 mainly applies. The Information Commissioner has no powers to invest surplus funds and may only borrow with the prior approval of the Secretary of State for Constitutional Affairs.

Financial assets and liabilities are generated by day-to-day operational activities and are not held to change the risks facing the Information Commissioner in undertaking his activities.

As permitted by Financial Reporting Standard 13, debtors and creditors which mature or become payable within 12 months from the balance sheet date have been omitted from the currency profile.

Liquidity risk

The Information Commissioner's funding is provided by fee income and grant-in-aid voted annually by Parliament within the Supply Estimate of the Department for Constitutional Affairs. It is not, therefore, exposed to significant liquidity risks.

Interest rate risk

The Information Commissioner is not exposed to any interest rate risk.

Foreign currency risk

The Information Commissioner's foreign currency transactions are not significant.

17 Accountability

No exceptional kinds of expenditure such as losses and special payments that required separate disclosure because of their nature or amount were incurred.

18 Prior year adjustment

There has been a change in accounting treatment as a result of the revision of The Government Financial Reporting Manual for 2006/07 (the FReM).

Grant-in-aid received for revenue purposes should now be regarded as a financing flow, and no longer as income, and should thus be credited directly to the income and expenditure reserve.

Grant-in-aid is provided to finance the activities of the Information Commissioner and enable him to meet his freedom of information statutory and other obligations, including capital spending, and as such should now be credited directly to the income and expenditure reserve, and not released to the income and expenditure account.

This change of policy has necessitated a re-statement of the prior year. The effect of the prior year adjustment is:

Income and expenditure account

	2005/06 £
Operating income	
As previously reported	15,983,027
Prior year adjustment	(6,561,702)
As re-stated	<u>9,421,325</u>

Balance sheet

	Income and Expenditure Reserve £	Deferred Government Grant Reserve £	Revaluation Reserve £	2005/06 Total £
Reserves				
As previously reported	(4,538,898)	4,443,405	25,307	(70,186)
Prior year adjustment	4,443,405	(4,443,405)	-	-
As re-stated	<u>(95,493)</u>	<u>-</u>	<u>25,307</u>	<u>(70,186)</u>

Cashflow statement

	2005/06 £
Net cashflow from operating activities	
As previously reported	293,455
Prior year adjustment	(4,089,481)
As re-stated	<u>(3,796,026)</u>
Financing	
As previously reported	1,010,519
Prior year adjustment	4,089,481
As re-stated	<u>5,100,000</u>

19 Post balance sheet events

On the 9 May 2007 the responsibilities of the sponsoring body, the Department for Constitutional Affairs, were transferred to the new Ministry of Justice.

The Annual Report, including the financial statements was authorised for issue on 10 July 2007, by Richard Thomas, Information Commissioner.

20 Resources by function

Data protection

The Secretary of State for Constitutional Affairs has directed that the notification fees collected by the Information Commissioner under the Data Protection Act 1998 shall be retained by the Information Commissioner to fund his expenditure on data protection work.

The annual fee for notification is £35, and has remained unchanged since it was introduced on 1 March 2000.

The data protection notification fee is set by the Secretary of State, and in making any fee regulations under section 26 of the Data Protection Act 1998, as amended by paragraph 17 of Schedule 2 to the Freedom of Information Act 2000, he shall have regard to the desirability of securing that the fees payable to the Information Commissioner are sufficient to offset the expenses incurred by the Information Commissioner, the Information Tribunal and any expenses of the Secretary of State in respect of the Commissioner or the Tribunal, and any prior deficits incurred, so far as attributable to the functions under the Data Protection Act 1998.

These accounts do not include the expenses incurred by the Information Tribunal, or the expenses incurred by the Secretary of State in respect of the Information Commissioner, and therefore these accounts cannot be used to demonstrate that the data protection fees offset expenditure on data protection functions.

Freedom of information

The Secretary of State for Constitutional Affairs provides an annual grant-in-aid to the Information Commissioner to fund his expenditure on freedom of information work. Grant-in-aid issued to the Information Commissioner reflects a need for cash, and is not paid to match accruals based expenditure.

There are no fees collected by the Information Commissioner in respect of freedom of information.

Apportionment of costs

Staff costs and other running costs are apportioned between the data protection and freedom of information functions on the basis of costs recorded in the Information Commissioner's management accounting system. This system allocates expenditure to various cost centres across the organisation. A financial model is then applied to apportion expenditure between data protection and freedom of information on an actual basis, where possible, or by way of a reasoned estimate where costs are shared.

Accounting basis

Accruals accounting is an accounting concept under which income and expenditure are recognised in the accounts for the period in which they are earned or incurred. This is in contrast to cash accounting under which income and costs are recognised in the accounts as money is received or paid. Accruals accounting allows the income received from fees to be properly matched over the accounting period to the expenditure.

Controls

The apportioned splits between data protection and freedom of information activities is shown below, firstly on an accruals accounting basis to comply with the spirit of the Treasury Fees and Charges Guide.

To demonstrate compliance with the general framework controls agreed between the Department for Constitutional Affairs and the Information Commissioner, information is also presented on a cash accounting basis.

Under the terms of the agreed Framework Document between the Information Commissioner and the Department for Constitutional Affairs up to 2% of the annual grant-in-aid can, with prior consent, be carried forward for spending in the next financial year. Similarly, up to 3% of fees collected which have been cleared through the banking system and are available for spending in the year, can be carried forward to spend in the next financial year. Any fees not cleared at the end of the year are regarded as cash in transit and are available for expenditure in the next financial year.

The segmental information has not been disclosed for the purpose of Standard Statement of Accounting Practice 25: Segmental Reporting.

Accruals basis

	Freedom of Information £	Data Protection £	Total 2006/07 £	Freedom of Information £	Data Protection £	Total 2005/06 £
Income						
Operating income	-	9,898,052	9,898,052	-	9,421,325	9,421,325
Other income	-	26,222	26,222	-	14,852	14,852
	-	9,924,274	9,924,274	-	9,436,177	9,436,177
Expenditure						
Staff costs	3,460,800	4,893,025	8,353,825	2,639,086	4,519,748	7,158,834
Other operating costs	1,749,988	5,178,463	6,928,451	2,050,661	4,217,437	6,268,098
Depreciation and revaluation	568,860	1,486,825	2,055,685	707,774	1,764,448	2,472,222
	5,779,648	11,558,313	17,337,961	5,397,521	10,501,633	15,899,154
Operating deficit	(5,779,648)	(1,634,039)	(7,413,687)	(5,397,521)	(1,065,456)	(6,462,977)
Grant-in-aid credited to reserves	5,550,000	-	5,550,000	5,100,000	-	5,100,000
Consolidated fund standing charge	66,455	66,454	132,909	65,286	65,287	130,573
Appropriations for other income	-	(26,222)	(26,222)	-	(14,852)	(14,852)
Income and expenditure reserve b/f	511,335	(606,828)	(95,493)	743,570	408,193	1,151,763
Income and expenditure reserve c/f	348,142	(2,200,635)	(1,852,493)	511,335	(606,828)	(95,493)

Cash basis

	Freedom of Information £	Data Protection £	Total 2006/07 £	Freedom of Information £	Data Protection £	Total 2005/06 £
Receipts						
Grant-in-aid drawn to spend	5,550,000	-	5,550,000	5,100,000	-	5,100,000
Fees available to spend (cleared)	-	10,045,526	10,045,526	-	9,495,440	9,495,440
	5,550,000	10,045,526	15,595,526	5,100,000	9,495,440	14,595,440
Payments						
Staff costs	2,593,610	4,725,226	7,318,836	2,446,516	4,334,616	6,781,132
Other operating costs	2,847,102	4,794,153	7,641,255	2,222,214	4,372,455	6,594,669
Tangible fixed assets	206,858	496,413	703,271	333,694	676,825	1,010,519
	5,647,570	10,015,792	15,663,362	5,002,424	9,383,896	14,386,320
Surplus cash from the year	(97,570)	29,734	(67,836)	97,576	111,544	209,120
Surplus cash b/f	97,576	271,733	369,309	-	569	569
	6	301,467	301,473	97,576	112,113	209,689
Cash in transit	-	159,236	159,236	-	159,620	159,620
Fees held under direction	-	11,515	11,515	-	11,585	11,585
Surplus cash c/f	6	472,218	472,224	97,576	283,318	380,894
Percentage of Cleared funds c/f						
	0.0%	3.0%		1.9%	1.2%	

The year end outturn for all of the financial annuality 'cash' controls were met.



Contact us

Information Commissioner's Office
Wycliffe House, Water Lane
Wilmslow, Cheshire SK9 5AF

Publications Line

t: 08453 091 091

Helpline

t: 01625 545745

f: 01625 524510

e: mail@ico.gsi.gov.uk

w: ico.gov.uk





Published by TSO (The Stationery Office) and available from:

Online

www.tso.co.uk/bookshop

Mail, Telephone, Fax and E-mail

TSO

PO Box 29, Norwich NR3 1GN

Telephone orders/General enquiries: 0870 600 5522

Order through the Parliamentary Hotline Lo-call 0845 7 023474

Fax orders: 0870 600 5533

E-mail: book.orders@tso.co.uk

Textphone 0870 240 3701

TSO Shops

123 Kingsway, London WC2B 6PQ

020 7242 6393 Fax 020 7242 6394

16 Arthur Street, Belfast BT1 4GD

028 9023 8451 Fax 028 9023 5401

71 Lothian Road, Edinburgh EH3 9AZ

0870 606 5566 Fax 0870 606 5588

TSO Accredited Agents

(see Yellow Pages)

and through good booksellers

