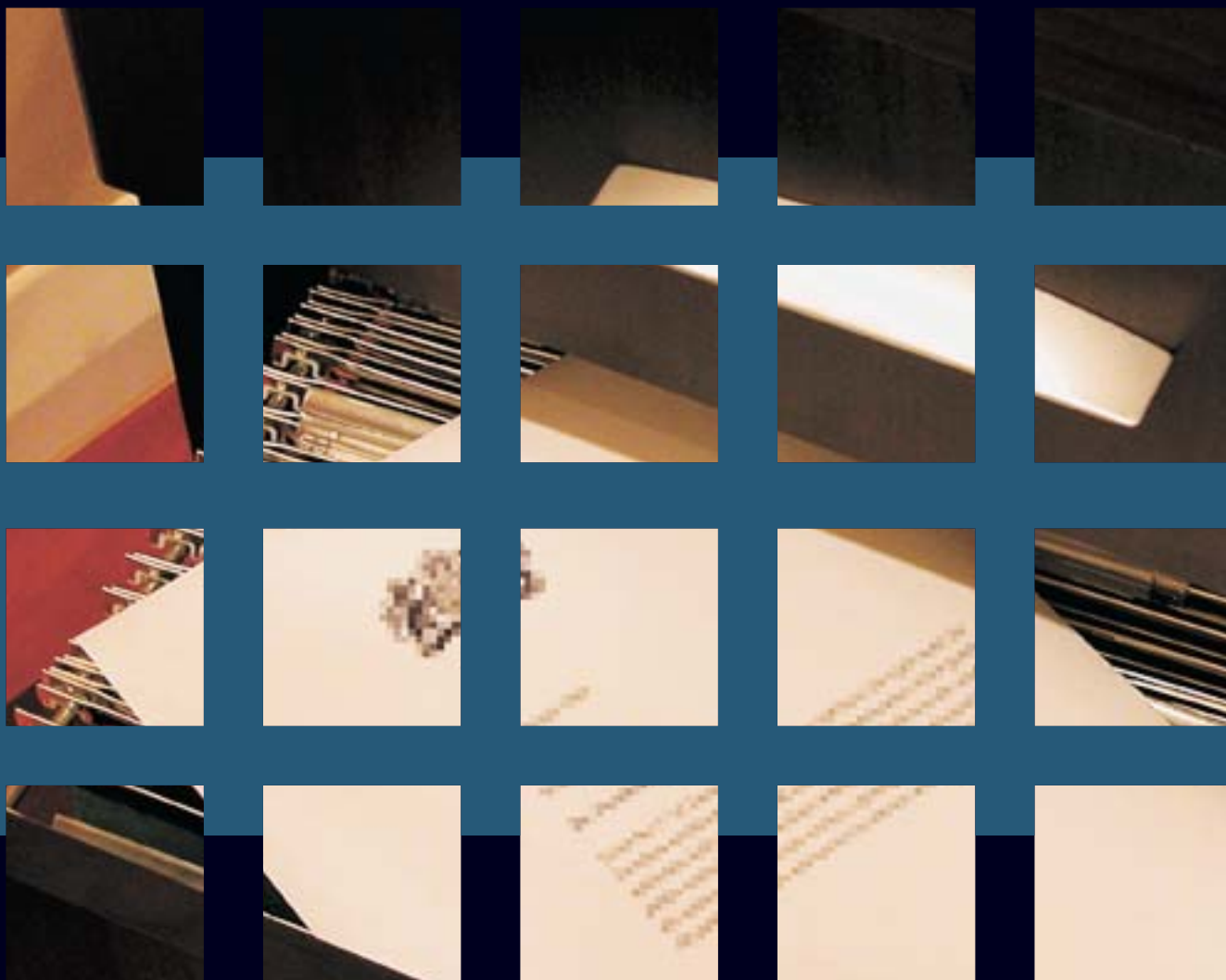


# ANNUAL REPORT

J U L Y 2 0 0 4







Information Commissioner Annual Report and Accounts for the year ending 31 March 2004

# ANNUAL REPORT

J U L Y 2 0 0 4



Information Commissioner

Presented 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 Schedules 5 paragraph 10(2) of the Data Protection Act 1998.

Ordered by the House of Commons to be printed  
13 July 2004

London: The Stationery Office

Price: £20.60

HC669



Information Commissioner



Information Commissioner

**© Crown Copyright 2004**

The text in this document (excluding the 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 enquiries 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](mailto:licensing@cabinet-office.x.gsi.gov.uk)

## contents

Commissioner's Foreword:	
Frequently Asked Questions	5
 The Year in Review:	
Developments in Freedom of Information and Data Protection	12
 Freedom of Information Act 2000: Countdown to The Right To Know	13
 Data Protection Act 1998: Privacy, Access, Standards	24
 A Growing Office	46
 Information Commissioner's Accounts for the Year Ended 31st March 2004	52
 Facts and Figures	87

---



## **Promoting public access to official information and protecting your personal information**

### **Information Commissioner's Office**

Wycliffe House  
Water Lane  
Wilmslow  
Cheshire SK9 5AF

To notify call: 01625 545740

Helpline: 01625 545745

Switchboard: 01625 545700

Fax: 01625 524510

DX: 20819 Wilmslow

Website: [www.informationcommissioner.gov.uk](http://www.informationcommissioner.gov.uk)

E-mail: [mail@ico.gsi.gov.uk](mailto:mail@ico.gsi.gov.uk)



Information Commissioner

## Management Board





### **Our Aims**

We have been created by Parliament as the independent body responsible for bringing about, on a UK-wide basis, the benefits of freedom of information, data protection and related laws. This translates into the following aims:

#### **For freedom of information**

- we will decide cases robustly and correctly where there is a dispute about access to information held by a public body;
- we will promote open government and bring about a culture where public bodies make as much official information available as possible.

#### **For data protection**

- we will promote good practice by organisations that handle personal information;
- we will run an efficient and helpful Notification and Case Reception service;
- we will provide remedies (where available to us) in cases where we are satisfied that individuals have legitimate grievances about the handling of their personal information;
- we will take purposeful regulatory action, where obligations are ignored, examples need to be set or issues need to be clarified.

#### **As an influential office**

- we will communicate helpful information and advice to targeted sections of the general public;
- we will influence domestic and international debates about access and privacy issues.

#### **As an effective office**

- we will deliver our responsibilities effectively and efficiently.





## Commissioner's Foreword – Frequently Asked Questions

During my first full year as Information Commissioner, people have Frequently Asked me Questions. Here are my end-of-year Answers.

### What do you do?

I am the champion of both open government and data protection. I do this by leading an independent office which regulates the handling of information. We are a wholly independent body, answerable to Parliament, given two basic tasks by law:

- promoting access to official information; and
- protecting personal information.

My office is small, but growing in size, profile and influence. I can do nothing without my committed, expert staff who recognise the importance of our responsibilities and who want to do a good job.

### What are your responsibilities?

Last year I announced a strategic review of our aims and objectives. This was carried out – under the banner of our Home Improvement Project (HIP) - over the second half of 2003. It involved extensive external and internal discussion, culminating in the work of six Task Forces looking at different aspects of our work. The most tangible outcome has been the Corporate Plan for 2004 – 2007 which was published in March 2004. This sets out re-defined Aims and Objectives, (see panel) summarising our responsibilities in terms of:

- **educator** – promoting good practice for organisations and communicating helpful information to the public
- **remedy provider** – providing solutions within our powers where there are legitimate grievances
- **enforcer** – taking firm, but fair, regulatory action where necessary.

The HIP Project confirmed the importance of clarifying and making sense of our various functions, identifying priorities and committing to the changes we need to make.

Richard Thomas, Information Commissioner



**To promote public access to official information and protect your personal information**



### **What are your top priorities?**

We need to be selective. We cannot do everything. I believe we will be seen as a successful and well-respected organisation if we focus on three priorities between now and 2007:

- top priority for our freedom of information responsibilities – deciding cases in ways which command public and organisational confidence and getting well down the road towards a genuine “open government” culture;
- taking a practical, down-to-earth approach to our data protection activities – simplifying and making it easier for the majority of organisations who seek to handle personal information well, and tougher for the minority who do not;
- aiming to be a “top-of-the class” office, with clear Values, of which we are all proud – influential, well-run, outward-looking and delivering real service to society.

### **What will all this mean in practice?**

We need to break our various responsibilities (new and existing) into manageable tasks, articulating what we can and cannot do and making sure we concentrate on important concerns where we are especially well-placed to make a real impact. This needs a new organisational structure, new policies and procedures and more active performance management. With greater clarity about “What and How?”, our plans spell out our intention to:

- become more proactive and maximise our influence, targeting issues and cases where detriment is greatest;
- become more customer-focused and better at communicating with target audiences and working with other organisations;
- shift attention away from those complaints where we cannot provide remedies in favour of activities which promote good practice;



- transform our internal working methods, especially to enable us to demonstrate success;
- ensure a reputation for helpfulness and effectiveness;
- ensure that we get the best from all those working here; and
- get the best out of new technology and our new regional structure.

We still have plenty to do to turn the plans into reality, but we are on track.

### Who leads the process?

As Commissioner, I must take ultimate responsibility for our activities. But staff at all levels deserve the credit for an astonishing range of work and achievements and must be heavily involved in the process of refreshment and modernisation. I reformed the corporate governance of the office during the year so that an Executive Team shares with me the internal leadership of the office. Strategic direction and leadership now come from a re-constituted Management Board. I was delighted that (from a very wide field) I was able to recruit four excellent non-executive members to this Board. All four new members arrived in January, but are already making significant contribution as objective and questioning supporters of the office.

### Why have you separated the freedom of information and data protection functions?

Parliament has superimposed the FoI responsibilities onto a mature data protection organisation. Both functions demand good information-handling practices and both are heavily concerned with access to information. But there are differences and sometimes tensions. These are best resolved inside the same organisation. Freedom of information will raise very sensitive, complex and high profile individual cases. The entire organisation will be judged on how well we handle these cases. We need the focus of a dedicated FoI team which can ensure that we develop the right organisational and cultural approach outside the shadow of on-going data protection activities.

### Non-executive Board Members

#### Dr Robert (Bob) Chilton

After a career in local government, Bob Chilton served as Director of Local Government Studies at the Audit Commission, and is currently Vice-Chairman of the National Consumer Council and undertakes project consultancy for the Audit Commission.

#### David Clarke

After a career in marketing including working for Scottish Power, David currently serves as a non-executive adviser to the think-tank Demos.

[continued next page](#)

## Non-executive Board Members

### Sir Alistair Graham

Previously Parades Commissioner for Northern Ireland and Chief Executive of two TEC's, Sir Alistair Graham is the Northern and Yorkshire Regional Commissioner for the NHS Appointments Commission, as well as being a member of the Employment Appeals Tribunal and Chairman of the Committee on Standards in Public Life.

### Clare Tickell

Is the Chief Executive of Stonham Housing Association, providing housing and care to some of the most socially excluded and disenfranchised, including homeless people, victims of violence, substance misusers and people with health problems.

## Will you be ready for freedom of information?

We have already approved Publication Schemes – setting out how information is made available without waiting for requests – for almost all public sector bodies. We are on course to complete the programme by July 2004. We have made good progress in implementing a project plan to make sure we are ready for the introduction of the Right to Know in January 2005. Our plan tackles such varied issues as casework systems, staff expansion, training and publishing guidance for public bodies. The National Audit Office has reviewed our preparations and we have benefited from their contribution. We know that we will receive difficult and demanding cases. The major unknown at the moment is the volume of casework. I also have serious concerns that – unless I am given freedom by the government to find ways to pay my staff in line with local market conditions – we will encounter increasing difficulty in recruiting and retaining staff of the right calibre to handle the FOI work.

## Will government be ready for freedom of information?

There has been a long waiting period since the law was passed in 2000. This should have allowed plenty of time for government departments and all other parts of the public sector to get ready, but the preparation time may have been used by some as a breathing space. Many public bodies are very well aware of what is coming; others are waking up late in the day. Some may get some unwelcome surprises when their first requests arrive – with only 20 working days to respond – because they have not thought ahead. I will not be able to accept “Not yet ready” as an excuse for failing to disclose information under the Act.

## Why is freedom of information important?

I see freedom of information as central to the democratic process. People are entitled to know what government – in the widest sense – is doing in their name and with their money. Freedom of information serves as a reminder that government should not be a secretive machine, locked away from the view of the citizens who elect those who govern us. Most



of the public sector delivers public services or provides public benefit. The rhetoric of recent years has been all about transparency and improved delivery. Fol is a means of demonstrating the reality. There are many exemptions to cover situations where there is a legitimate need for secrecy. The public interest test will cut both ways according to circumstance, but the presumption must be in favour of disclosure. I hope that Ministers will be very slow to use the so-called veto to over-rule public interest decisions in favour of disclosure. Whenever they do, I will need to explain the circumstances in a Special Report to Parliament.

### **Why is data protection important?**

Individuals need rights that they can rely on as a counter-balance to some of the excesses or risks of the information society. More generally, privacy is recognised as a fundamental human right and the protection of personal information is essential to our integrity as individuals. Our research shows how much people care about their privacy and the safeguarding of their information – especially after encountering a real threat. Businesses have taken these issues increasingly seriously in recent years, not least recognising the risks to corporate reputation if they get it wrong. This chimes well with my approach of promoting good data protection practice as enlightened self-interest, concentrating on aspects – such as mistaken identity - causing greatest actual or potential detriment.

### **What is your approach?**

The data protection principles are widely seen as sensible common sense. Sadly, some of the detailed requirements of the law, intended to bring these principles to life, are excessively complicated and perhaps unduly prescriptive. My task has to be to de-mystify the law, explaining things as clearly as possible and exploring the scope for simplification. We must make it as easy as possible for organisations and individuals to understand what to do and expect. There is still much to be done.

### **Does data protection do more harm than good?**

No, of course not. Data protection has a mixed reputation, not just for its complexity. Too often there are perceptions that it stops people doing sensible things – such as responsible information-sharing about vulnerable children and adults. These perceptions are nearly always mistaken, but they are real. It has become too easy to blame data protection. We need to show how data protection regulates flows of information in the interests of individuals, only stopping them altogether for good reason. This is a major challenge requiring more guidance, codes of practice and other initiatives. We must – and will – challenge the myths. Changes to the law are also needed, not least to make it clearer that privacy and data protection are not absolutes and that personal information can be processed or disclosed where that is necessary for public protection, rights and freedoms.

### **Was data protection responsible for the deletion of police records?**

Myths, misconceptions and misinformation rose to a crescendo when data protection was initially, and wrongly, blamed for the destruction of police records about previous contacts with Ian Huntley. It became clear during the subsequent Inquiry that deletion or loss of these records had nothing whatever to do with data protection law or any advice from my Offices. In his recent Report, Sir Michael Bichard explicitly rejected the suggestion that the legislation was the reason for the lack of searchable records. I entirely welcome the findings of the Inquiry; they will go a long way to restore public confidence in data protection. At the same time, I remain committed to a constructive relationship with the police and will contribute to a new Code of Practice in line with the Inquiry's recommendations.



### What have been your main achievements during the last year?

All achievements are those of my office as a whole. They are recorded in this report. Highlights include:

- Home Improvement Project, culminating in the new corporate plan for 2004 - 2007
- very positive response to our Employment Code, dealing with surveillance in the workplace;
- innovative advertising campaign to communicate rights to target groups;
- Make Data Protection Simpler Initiative;
- strong articulation of the need for maximum safeguards if and when ID cards are introduced;
- successful implementation, with well-received guidance, of new Privacy & Electronic Communications Regulations;
- resolving the problem of third party disclosures by credit reference agencies;
- smooth and timely approval of FoI Publication Schemes;
- establishing offices in Belfast, Cardiff and Edinburgh;
- Belfast conference to launch our regional office and FoI in Northern Ireland;
- approaching the end of a Change Programme to introduce electronic case-handling;
- significantly higher media profile to articulate the benefits of data protection and freedom of information;
- working with international colleagues to pursue a pragmatic approach to data protection and freedom of information issues.

**Richard Thomas**  
**Information Commissioner**  
June 2004





Information Commissioner

## Developments in Freedom of Information and Data Protection

# the year in review



10 January 2016

Dear Sir/ Madam,

**Her Majesty's Information Act**

Enclosed is a copy of the Freedom of Information Act 2000 (FOIA) which provides the right to request access to information held by public authorities. The Act also sets out the conditions for the release of information held by public authorities. The Freedom of Information Act is intended to ensure that public authorities are open and transparent in their dealings with the public and to ensure that they are accountable to the public.



## **Freedom of Information Act 2000: Countdown to The Right To Know**

There have been two main strands to this year's work on freedom of information: preparation for the full statutory right of access to publicly held information which begins on 1 January 2005; and approval of public authorities' publication schemes.

### **Countdown to the right to know**

The Freedom of Information Act 2000 does not give an absolute right of access to all information held by public authorities. It contains a number of specific exemptions, most of which are subject to an over-riding test of whether the disclosure of information would be in the public interest. The application of the public interest test is clearly going to be crucial to many decisions about disclosure. It is clear from contact with public authorities that there is a widely felt need for guidance in this area. We have responded to this and, in addition to the guidance already published, more is being developed

The Information Commissioner's Office, and to a large extent the Freedom of Information Act itself, is likely to be judged by the effectiveness with which complaints about failures to comply with requests for information are dealt. There has been considerable interest from journalists and others in the Ministerial veto that the Freedom of Information Act contains. It has been suggested that this will make the law a 'damp squib' that will have no real effect in terms of giving greater access to the information that public authorities hold. The Ministerial override is not something which can be exercised in secret. When a certificate is issued, Ministers are under a duty to lay a copy of the certificate before both Houses of Parliament. It is the Information Commissioner's intention, on each occasion that a certificate is issued, to make a Special Report to Parliament giving our view of whether it we think it appropriate for a certificate to have been issued.

We anticipate receiving complaints about failure to give access soon after 1 January 2005. The proper handling of complaints will depend primarily upon the development of policy around the application of the exemptions in the Freedom of Information Act, and upon thorough understanding

and application of the public interest test. It is envisaged that the bulk of our policy development work will be completed by the end of July 2004. This will allow a reasonable period of time for training case officers and disseminating relevant advice to public authorities.

In November 2003, we commissioned the Constitution Unit to carry out research into the likely volumes, complexity and sensitivity of freedom of information casework. This work studied the experience of Australia, Canada, New Zealand and the Republic of Ireland, most of which have legislation similar to that in the UK. The research will help us to judge the resources we are likely to need once the right of access to information commences in January 2005, but substantial uncertainty remains about the volumes we will receive in practice.

It is also important for us to know how well the various bodies covered by the Freedom of Information Act are preparing for its full implementation. So, over the summer of 2003 questionnaires were sent to some 200 authorities falling within waves 1 - 3. The survey suggested a good level of preparedness by central government and Northern Ireland departments. The response from police forces suggested similarly high levels of preparedness. There appeared to be a greater appreciation of the opportunities presented by freedom of information among the Northern Ireland responses. So far as local government was concerned it was clear that preparations were not as advanced as in the other sectors surveyed. Local authorities were also more likely to complain about the lack of additional resources for compliance. The survey gave some interesting indicators of the sorts of information the public are interested in. For example, local authorities detected particular interest in planning committee agendas and reports. In fact these are already available under existing legislation.

We have also been preparing for our responsibilities in respect of the Environmental Information Regulations. These Regulations will give the public a right of access to a wide range of information relating to environmental issues such as land use, air quality, water quality and pollution.



These give effect to a recent EU Directive and are due to be introduced at the same time as access rights under the Freedom of Information Act. As far as possible the two access regimes will be brought together into a single regime to be enforced by the Information Commissioner. However, there are some significant practical differences, for example the manner in which requests can be made and the charges that can be levied for giving access.

Guidance has been issued on several of the exemptions in the Act, and work is well advanced on developing our thinking around its other exemptions. In several cases we have had extensive discussions with those who will be affected by the exemptions. These include relevant public authorities, representative bodies, and, wherever possible, representatives of those who are likely to use the Act's statutory right of access. In July 2003 we published our 'Introduction to the Freedom of Information Act 2000'. We have also published 'awareness guidance' on the following topics:

- personal information;
- information received in confidence;
- the public interest;
- legal professional privilege;
- commercial interests;
- information accessible by other means;
- information intended for future publication; and
- frequently asked questions on records management.

A considerable amount of detailed work has been done on the procedural and technical issues arising from the Freedom of Information Act. These include:

- issues relating to fees and refusal notices;
- questions of how to communicate information;
- the identification of vexatious and repetitious requests;
- the development of policy around disability and other access issues; and
- the Act's provisions relating to records held by the National Archives.

This stream of work has been coupled with work around the statutory codes of practice on access to information and records management provided for in the Act. We have also issued advice to public authorities on the process involved in handling a request for information.

It is important, as the independent regulator, that we take our own view of the meaning of the exemptions and the circumstances in which the public interest may or may not require disclosure. At the same time we have been happy to work with others on the development of guidance on the exemptions and on other aspects of freedom of information. We have worked, for example, with the Local Government Association, the Association of Chief Police Officers and the Department for Constitutional Affairs (DCA). We are awaiting final draft guidance from the DCA working groups before deciding what additional work we may need to carry out ourselves. We are also awaiting Government regulations on access to environmental information and on fees before we can offer advice to public authorities on these matters.



### **Promoting access rights**

We have promoted freedom of information in various ways, including numerous face to face meetings with public authorities, seminars and conferences. We have addressed audiences at events organised by the DCA, umbrella organisations such as the Local Government Association, professional associations, universities and private sector conference organisers. We have addressed awareness raising seminars for several central government departments, for instance the MoD and DEFRA. We have spoken at a large number of events aimed at other authorities including local government, higher education and the NHS. Our Northern Ireland office was launched at a major conference with freedom of information as its theme. This was attended by some 250 delegates from public authorities in Northern Ireland. The interest in freedom of information has been constant and is certainly increasing further as we move towards 2005.

In general we intend to promote the Act to the public once the 'Right to Know' has been implemented. However, we have published a short information leaflet for the public, 'Read All About It – A Guide to Information Available from Public Authorities.' The leaflet has been distributed through libraries and Citizens Advice Bureaux. We will be issuing further advice for the public later in the year.

### **Working with others**

There are various bodies who are either given specific roles by the Freedom of Information Act itself or with whom it is important to have a particularly close working relationship. These include:

- The Department for Constitutional Affairs: we continue to have a close relationship with the DCA both as our sponsoring department and as the lead department for FOI in central government. The Commissioner continues to co-chair with the relevant Minister the Lord Chancellor's Advisory Group on the Implementation of Freedom of Information. The group has members from across the public sector and from the DCA and our own office. It also has independent members, including an academic, a journalist and others with a specific interest in freedom of information.



- The National Archives/Public Records Office of Northern Ireland: we have held regular meetings with the Keeper of the Public Record. Work on the development of formal Memoranda of Understanding to do with records management is well underway.
- The Parliamentary Commissioner for Administration (the Ombudsman): the relationship between the Ombudsman and Commissioner is particularly important as requests for information under the Open Government Code give way to requests under the Act. The Ombudsman and her staff have proved to be invaluable sources of advice and experience of dealing with access to information issues. A formal memorandum of understanding between our offices is expected to be agreed shortly.
- The Scottish Information Commissioner: Scotland has its own Freedom of Information Act and a Commissioner responsible for implementing it. It is very important to have a good working relationship with our Scottish counterpart. The development of this relationship will be facilitated by meetings involving the DCA, the Information Commissioner, Scottish Executive and Scottish Information Commissioner. Again, a formal memorandum of understanding is also under development.

### Publication Schemes

There is a requirement under the Freedom of Information Act 2000 for public authorities falling within the scope of the legislation to adopt and publish a 'publication scheme'. A publication scheme is in essence a guide to the information that an authority commits to make readily available to the public when requested to do so. In order to ensure that a scheme provides for an appropriate level of public access to official information, an authority's publication scheme must be approved by the Information Commissioner.

It is estimated that over 100,000 public authorities fall within the scope of the Freedom of Information Act 2000. These range from individual NHS practitioners to the largest government departments. The scrutiny and





approval of publication schemes is a major administrative task for us. Therefore we have set up a specialist unit that is entirely devoted to the approval of public authorities' publication schemes.

The development and approval of publication schemes takes place in six "waves". The first wave consisted of central government departments and some non-departmental public bodies, including the Information Commissioner's Office. These organisations were required to adopt a publication scheme and publish information in accordance with it from 30 November 2002. By June 2004 all public authorities subject to the Freedom of Information Act 2000 should have adopted an approved scheme.

#### Timetable for adoption of publication schemes

Wave 1	November 2002	Central government (except the Crown Prosecution Service and Serious Fraud Office), Parliament, National Assembly for Wales, non-departmental public bodies currently subject to the Code of Practice on Access to Information
Wave 2	February 2003	Local government (except police authorities)
Wave 3	June 2003	Police, police authorities, Crown Prosecution Service, Serious Fraud Office
Wave 4	October 2003	National Health Service
Wave 5	February 2004	Schools, universities, remaining non-departmental public bodies
Wave 6	June 2004	Remaining public authorities

All but a handful of the schemes in Waves 1-4 were submitted on time and all of those were approved on time. This has been a considerable achievement, both for my Office and for the large number of public authorities concerned. Regrettably, one District Council has failed to submit a scheme for approval and is currently the subject of enforcement proceedings. However, we have been generally encouraged by the positive attitude adopted by the vast majority of public bodies. Although some have done little more than include information which they were already making available, others took the opportunity to publish much more. We hope the message continues to get through that the more material is included in a publication scheme on a voluntary basis, the less onerous it will be to deal with requests for access to publicly held information once full individual access rights go live in January 2005.

The Information Commissioner's Office approves both 'bespoke' and 'model' publication schemes. A bespoke scheme is one designed by a particular public authority for its own use. A model scheme is a generic one that may be adopted by particular categories of public authority, who are likely to hold and make available similar types of information. For example, model schemes have been designed and approved for use by general practitioners, schools and parish councils. Schemes are approved for a limited period of time, usually four years, after which new approval must be sought. There is however a duty to review schemes regularly.

For the first round of approvals, we have not set particularly high thresholds for approval. At this stage, our most important objective has been to ensure that schemes are adopted and that processes are established for scheme development, review and renewal. This does not mean, however, that we are under-estimating the importance of publication schemes as a means of promoting public openness. We have initiated a wide-ranging review of schemes, looking at their content, the effectiveness of particular schemes, the efficiency of our approvals systems and, importantly, the use that the public makes of publication schemes. This work will lead to revised approval criteria for the second round of approvals and to a review of our own systems and procedures.



Initially, all public authorities were asked to submit either their bespoke scheme to us for approval or to advise us of their adoption of a model. Many smaller organisations found model schemes suitable. For example, there are about 10,000 parish councils and parish meetings. Virtually all of these have adopted a model scheme. Those doing so were required to notify us that they had adopted the model and we had to record that fact. However, there are no comprehensive lists of some of the types of authority caught by the Freedom of Information Act, typically smaller ones such as NHS dentists and community pharmacists. This made it impossible to tell whether there were any public authorities that had failed to adopt a scheme when required to do so. Therefore, in order to simplify the process for all concerned, for some of the later waves of public authorities for whom model schemes have been approved, we have publicised the existence of the model and the obligation to adopt a scheme but have not required a formal return. Once the first round of approvals has been completed, we intend to carry out a check of a representative sample of those authorities who should have adopted a model scheme to ascertain whether this “light touch” approach has been effective.

### **Freedom of Information: Your Right To Know**

The Freedom of Information Act gives access to information held by public authorities in two ways:

- it requires public authorities to adopt and maintain a publication scheme - a guide to the information that an authority commits to make readily available to the public when requested to do so. This should increase the amount of information routinely made available to the public;
- it gives individuals a right to make a request for information, effective from 1 January 2005;
- anyone will have the right to ask public authorities for any information they hold.

### **How Does The Right To Know Work?**

**Prior to 1 January 2005:** you can have access to any information falling within a public authority's publication scheme. You are entitled to see a copy of any public authority's scheme, and the authority has a duty to ensure that the types of information described in it are genuinely readily available upon request. The scheme will also specify the format in which the information is made available and whether there is a charge any of the information.

**From the 1 January 2005:** in addition to accessing information via publication schemes, you may make a request for specific information to any public authority. The authority must deal with a request in accordance with the Freedom of Information Act.

### **Making a request:**

- your request must be made in writing, which includes e-mail;
- you should state your name and address and describe the information you seek;
- the public authority should send you the information within twenty working days of receiving your request;
- if an exemption applies you must be advised of this within the initial twenty day period;
- if a fee is required for supplying the information a fees notice must be sent to you saying how much you need to pay. The information need not be supplied to you until you pay the fee.



---

**The benefits of Freedom of Information - the right to know will:**

- allow individuals to understand decisions made by public authorities that affect their lives, and in some cases to challenge those decisions;
  - improve decision-taking by facilitating greater public debate;
  - promote accountability and transparency in respect of decisions taken by public authorities, including the spending of public money;
  - ensure the personal probity of political leaders and officials;
  - encourage democratic re-engagement in the face of growing public apathy;
  - further public understanding of, and participation in, public debate of issues of the day;
  - assist policy makers and the public in identifying key issues;
  - bring to light information that affects public safety;
  - challenge a culture of secrecy in public authorities.
-

**Data Protection Act 1998: Privacy, Access, Standards****Clearly explained**

The Universities' Central Admissions Service is responsible for allocating university places to applicants. All applicants for a place on an undergraduate course had to complete a form which contained a standard question asking for previous criminal convictions to be declared. No clear explanation was given of why this information was required or how it would be used. As a result of negotiations which followed preliminary enforcement action, UCAS agreed to change the application form to limit and specify the type of conviction information that has to be declared. The information required will be limited to convictions indicative of a significant risk to fellow students. In addition, an explanation of how the information will be used will now be provided to applicants.

**Data protection: friend or foe?**

During the year the Data Protection Act 1998 received an unprecedented amount of negative publicity. This emanated from ill-judged comments made in the context of two high profile and tragic cases; the Soham murders and the death of two pensioners who had their gas supply cut off. (The events of Soham are described in detail later in this Report.) The comments, which blamed the Data Protection Act for the destruction of intelligence about the Soham murderer and for an inability to share information on those at risk, were eventually retracted. However the publicity given to these original assertions has had a lingering detrimental effect. The Data Protection Act is not the most elegant or easily understood statute. It is not written for the casual reader. This is particularly regrettable given that the eight enforceable rules of good practice that lie at the heart of the legislation are simple, clear and attractive. We had already embarked upon our 'Make Data Protection Simpler' initiative long before the negative publicity referred to above. There have been few calls from our respondents to change the principles that lie at the heart of the legislation. They do though, quite understandably, want clearer, more focussed guidance on what they need to do to comply with the law. To this end we have embarked on a programme of producing a set of concise 'Good Practice Notes', and on revising our existing guidance, including our CCTV Code of Practice. We are committed to producing clear, straightforward, plain English guidance that readers of all levels of expertise can understand and convert into good practice. Hopefully this will help to prevent any recurrence of the tragic events referred to above.

We have some way to go to restore the reputation of the law that we are responsible for enforcing. Our achievements of the last 19 years can easily be overlooked. For instance, we now accept as a given that we have to be told how our personal details will be used, that we can stop unwanted junk mail, that we can have access to records about us and that our applications for credit should not be refused because of the bad payment record of a stranger who once lived at our address. The Data Protection



Act and this office have played an instrumental role in all these positive developments. Similarly, when any initiative is undertaken that involves using personal information we now take it for granted that safeguards for protecting such information have to be built in. This is particularly important in the context of the Government's proposal to introduce identity cards. To its credit the Government has recognised that putting data protection safeguards in place is an essential requirement if the scheme is to proceed. During the year we expressed our concerns about identity cards and the national population register underpinning them when we gave evidence to the Home Affairs Committee. As our reporting year closes the draft Bill has been published and we are in the process of examining this closely to assess whether our concerns about the Government's proposals have been addressed. There is no doubt this will be a major topic of debate in the year to come. We are committed to ensuring that the need to safeguard information about individuals lies at the heart of the identity card debate.

### **Making it clearer, making it simpler**

Our work on making 'fair processing notices' shorter and more intelligible to the general public is a key element in our initiative to simplify data protection. 'Fair processing notices', or 'privacy statements' as they are sometimes called, are meant to ensure that when a person is asked to provide personal information, the person knows what will happen to the information requested. Fair processing notices should be provided when a person fills in a standard application form or is asked to provide information over the phone or internet. This should provide for transparency and give individuals a degree of control over their personal information. In the finance industry, in particular, these statements are usually long and often complicated. Some organisations try to ensure they cover absolutely everything they do, or may do, with the information to ensure their compliance with the Data Protection Act 1998 is not in doubt. The length and the complexity of these fair processing notifications mean that often individuals don't bother to read them. This is a situation that serves no one well.

### **Fully informed**

The complainant contacted us because he had made a request for access to a relative's speech and language therapy notes. Some notes were supplied, but the complainant required further information in order to ensure his relative's needs were met adequately. The relative's speech and language problems meant he required particular education services which were not being provided. The complainant believed that the other information in the file would show that the previous annual review of his relative's condition was flawed and that as a result his relative's needs were not being met.

The situation was made more difficult because two different Primary Care Trusts were involved – one where the complainant lived and one which was meant to provide the specialist care his relative needed. There was some confusion over who was responsible for dealing with the complaint. The delay in receiving the information was causing the complainant considerable distress.

continued next page



### Fully informed

We contacted the Trust which provided the specialist care as it held the relevant case notes. Initially the Trust claimed that it had provided all the notes that were available, but the complainant was able to provide evidence to show that this was not the case. After several months of correspondence the complainant was finally provided with the information he required. This should now enable his relative to receive the proper educational assistance he needs or at the very least assure the complainant that adequate educational provision is in place.

We are routinely asked to advise organisations of all sorts about fair processing notices. We have acknowledged the difficulties many organisations face in providing notices that are comprehensive and data protection compliant, but which individuals will read and understand. We have encouraged organisations to develop simpler and less complicated notices. Work on 'condensed privacy statements' is also under way in the USA, across Europe and in other parts of the world, indicating that unnecessarily long and complicated fair processing notices are a widespread problem. At the 2003 International Data Protection Commissioners' Conference, held in Sydney, it was resolved to look at providing information in more condensed, clearer and more effective ways. This work is being taken forward by an international working group drawn from industry, consumer groups and data protection authorities. Next year we intend to undertake a research project looking at fair processing notifications from the individual's viewpoint. This will inform our future work on fair processing notices in the financial and other sectors.



### Small businesses: simple guidance and lots of advice

The implications of mishandling personal information can be as serious for a small business as for a much bigger one. Larger organisations often have their own legal or compliance staff to turn to for advice and guidance. Smaller businesses are less likely to have this resource. The main message we have been trying to get across to small businesses this year is that we are available to offer free advice and assistance when there are data protection issues to resolve. The detail of data protection law may be complicated but for the most part we can explain how to comply in simple, clear and easy to understand terms.

We have done a great deal this year to promote awareness of personal information issues to small businesses, and to help them to comply with the law. We have:

- posted new guidance on our website – both as a moving sequence on our home page and as a straightforward paper for printing off and reading;
- produced additional advice about using CCTV;
- produced summary guidance on surveillance in the workplace;
- manned stands at various events held throughout the country at which our staff have given advice on any aspect of data protection compliance; and
- addressed the Federation of Small Business annual conference.

We have also provided advice to the Small Business Service as it developed materials of its own relating to data protection.

### Drug dealing?

A person applied for a job as a foster carer and for a place on a nursing course. A Criminal Records Bureau check was carried out. The 'disclosure' showed that between 1995 and 1999 she had associated with people who were allegedly responsible for local drug dealing. The police ascertained that the allegations did not relate to the applicant but to associates of her ex-husband who was still living in the marital home during the course of their separation. The police deleted this information from their records.

---

### **Make data protection simpler!**

The 'Make Data Protection Simpler' project is aimed at identifying ways of reducing the burdens of data protection without reducing protection for people.

During the year we have been asking the public and organisations how they think we can make data protection simpler. Some of these suggestions will be easier to act on than others, and many are already being worked on.

Here are some of the suggestions we received:

#### **Help us to comply:**

- make your guidance shorter, clearer and more accessible
- target guidance at particular sectors
- use plain English, avoid legalistic terms like 'data controller'
- produce simple checklists to help us comply with the law

#### **Improve your communications:**

- make your website easier to use
- put more staff on your Helpline so we can get through faster
- deal with casework more quickly

#### **Make notification more straightforward:**

- bring in 'lifetime' notifications
- have simplified notifications for small businesses
- allow simplified notifications for groups of organisations

#### **Change the law:**

- get rid of the 'conditions for processing'
  - make it clear that you can disclose personal information in life or death situations
  - extend the right to stop direct marketing so it covers any material sent to my house, not just that addressed to a specific person
-



## Raising public awareness

This year we launched a national advertising campaign intended to generate and increase awareness of personal information rights amongst those groups of people who are generally least aware.

Our innovative campaign involved national press, magazine and bus bulkhead advertising. It took place during October and November 2003. We also ran a student campaign which involved distributing beer mats to bars and pubs in and around university campuses and direct marketing activity on campus. The theme of this campaign was inaccuracy of information and the consequent 'mislabelling' of people.

The research findings suggest that the campaign contributed to:

- an increase in confidence in existing laws and an increase in trust of business practice amongst those who saw the campaign;
- an increase in perceived control over the way personal information is handled;
- an increase in awareness of data protection law, particularly its right of access; and
- a decrease in the percentage of people indicating they didn't know much about the Data Protection Act.

A report detailing the full evaluation of the campaign is available on our website.

## Data protection and policing

The key event of the year in the police sector was Sir Michael Bichard's Inquiry into the events surrounding the tragic Soham murders. The Report of the Inquiry was published in June. The Bichard Inquiry followed the conviction of Ian Huntley and the revelations that police checks had failed to disclose an extensive history of allegations of sexual offences. The Chief Constable of Humberside Police, David Westwood, in his press statement immediately following Huntley's conviction, pointed the finger of blame at the Data Protection Act for his lack of searchable records. Although he

subsequently accepted the Data Protection Act was not in fact to blame, his original statement did considerable damage to the reputation of data protection. The statement was widely reported in the media and we faced an uphill struggle to set the record straight. We still have some way to go. The main issue for us was the ability of the police to retain allegations of offences, particularly sexual offences, where there had been no conviction. The Act allows the police to keep such information where retention is justified by an ongoing policing need. There are many factors to be taken into account including the evidence to support the allegation, the nature of the allegation or the cumulative effect of a series of allegations. However, the detriment to individuals of the retention and potential disclosure of possibly unfounded or even malicious allegations, such as may be made by a pupil against a teacher, must be given due weight.

None of this would have dictated that Humberside Police should have deleted information with such obvious significance as that which, at one time, they held about Ian Huntley. We made several written submissions to the Bichard Inquiry and gave evidence in person. A difficult situation was not helped by a statement made by the Association of Chief Police Officers (ACPO) at the time of Huntley's conviction, and repeated subsequently in their evidence to the Bichard Inquiry, that action we were taking in two separate data protection cases would 'significantly undermine the ability of Criminal Records Bureau to help employers safeguard the interests of children in particular'. The issues raised in these cases are not the same as those in the Huntley case. They relate to the retention of conviction records on the Police National Computer (PNC). The Huntley case related to the retention of non-conviction information by a local police force.

ACPO have established rules to govern the removal of conviction records from the PNC. Many records, including those involving a crime of violence or a sentence of six months or more are retained for life. We have always



taken the view that standard retention periods are not a problem and, indeed are inevitable given the number of records held on the PNC. But there must be a willingness to depart from them where the circumstances of a particular case warrant it. The two cases referred to by ACPO are examples of where the conviction details are so old, and lack any degree of seriousness, that it is hard to see any policing reason for continued retention. Indeed, none has been put forward to us. We issued preliminary enforcement notices against the police forces concerned, but at the request of ACPO, delayed the issue of final notices to enable them to re-examine their “weeding rules” to address our concerns. ACPO’s response, which they put to the Bichard Inquiry, has been to propose that all conviction records, even those that would previously have been weeded after say 10 or 20 years, should now be retained indefinitely. We will revisit this matter now that the Bichard Inquiry has reported and will decide if and how to take the preliminary notices forward.

The Bichard Inquiry also focused its attention on the data protection guidance available to police forces. In the light of failings in Humberside, the Home Office set up a Working Group to review the available guidance. We have taken an active role in this Working Group and support the direction of its work. We will take the conclusions of the Bichard Inquiry into account in taking this work forward.

More generally, we welcome the Bichard Inquiry’s rejection of ACPO’s suggestion that we had influenced individual police forces on occasions to the detriment of the Police Service and vulnerable members of the community. But we fully accept the Report’s conclusion that our relationship with ACPO is an especially important one if data protection is to be properly understood in the Police Service, and that there needs to be a close and constructive relationship if confusion and uncertainty are to be avoided.

### In debt, indiscreet

Several faxes were sent to the general fax machine at the complainant’s place of work. These contained information about a debt she allegedly owed and details of the action that would be taken against her if she didn’t pay. We made it clear to the debt collection company that details of a person’s financial position should not be disclosed to third parties, such as the complainant’s workmates. As a result of our involvement the debt collection company stopped sending faxes to the complainant’s workplace. This prevented personal information about the complainant being improperly disclosed.

### Proving identity

An individual wrote to the National Probation Service (NPS) because he wanted access to his records. Initially the NPS would not comply with the request because they didn't think the individual had proved his identity satisfactorily. They asked him to prove his identity by attending an NPS regional office in person. The individual complained to us about this. It is quite right to require those seeking access to records to prove their identity. However we took the view that it was unreasonable to expect people to attend NPS offices in person to prove their identity, especially as some people might live along way from an office. Following our involvement the NPS provided the individual with a copy of his record and introduced new identification procedures to ensure that individuals wouldn't have to attend an NPS office in person to prove their identity.

### Auditing and inspecting

We have appointed a Senior Inspections Manager, the first step in developing a dedicated audit and inspections function within our Office. Building on our experience of auditing Europol and the development of our audit manual we have, by invitation, conducted a number of data protection audits to assist in our objective of promoting good practice. Interest to date in this initiative has been predominantly from the public sector and has often resulted from a prior identification of non-compliance.

Whilst no major problems have been identified there have been recurrent themes relating to data protection awareness within decentralised organisations and the unnecessary retention of personal information. From a positive viewpoint many examples of good practice were also identified together with a general recognition that good information handling makes organisations more effective.

Feedback from participating organisations has been positive with recognised benefits including the opportunity to focus attention on personal information matters and to gain an independent view of the issues involved. From our Office's perspective, the audits have also enabled us to gain a better insight into how these organisations operate. This knowledge should inform our compliance activity and the development of codes of practice and other guidance.

### Maintaining the register: another busy year

Keeping the publicly available register of organisations that hold information about people continues to be a major administrative task for us, but we have provided an efficient service, eliminating the backlogs which arose from the activities of self-styled notification agencies. These bogus organisations send out misleading, official-sounding letters and charge excessive fees for notifying on behalf of others. Their activities have continued to generate considerable extra work for us. However, the number of calls from those who have received these 'urgent' notices is not as high as last year and the number of applications made via these 'agencies' has dropped, indicating that fewer businesses are being duped.





Nevertheless nearly 43,000 of the 131,605 calls taken by the Notification Helpline related to these agencies.

Over the last year we have issued further press statements on this matter and have given a considerable number of radio and television interviews. We continue to work closely with the Office of Fair Trading (OFT), local trading standards departments and the police. The OFT has obtained undertakings from a number of individuals that they will not be involved in misleading advertising for data protection notification services. The OFT has obtained injunctions against Chris Yewdall, who was associated with the provision of such services under a number of trading names, and against the Data Processing Protection Corporation Ltd.

We have taken steps to minimise the risk of those who initially notify via an agency renewing their notifications at exorbitant cost. We now write to them to advise them that they can renew directly with us for £35 and remind them of this when renewal is due. We are also moving towards on-line notification. This will make it easier for those required to notify to deal directly with our Office. It will also be easier for the public to access an up-to-date version of the register.

### Notification Department Statistics

#### Stolen identity

As a result of a Police National Computer check a man found out that his record contained details of crimes which he had not committed. His innocence was confirmed through finger print evidence. It was established that the person who had in fact committed the offences was an illegal immigrant who had stolen Mr X's identity. The Police thought it impossible to remove the record as they had no other way of recording information about the offences. However they agreed to put comments on the record about Mr X's physical characteristics proving that he was not the offender.

The Data Protection Register	2002 - 2003	2003 -2004
Total Register Entries	211,251 (31.03.03)	251,702 (31.03.04)
New Applications		
Made under the Data Protection Act 1998	110,451	63,942
Renewals		
Requests for renewal made under the 1998 Act	124,782	194,828
Requests for Amendment	35,625	43,538
Under the 1984 Act	14,392	1,217
Under the 1998 Act	21,233	42,321

**Blagging, investigation and prosecution**

The majority of the work we carry out is intended to promote compliance with the law through education, negotiation and dialogue. There is, though, an organised and systematic industry whose lifeblood is the unlawful obtaining of personal information through deception, bribery and other underhand tactics. This is known as 'blagging'. It is the role of our Investigations Department to catch those who are involved in this activity. We are proud that our investigators have had significant success during the year under review. This success builds on last year's BAIRD project, a joint initiative involving the Information Commissioner, Department of Works and Pensions and Inland Revenue. This led to the successful prosecution of a number of individuals and organisations who unlawfully obtained personal information for various clients, usually by deceiving employees of the organisations they targeted. Following the success of BAIRD, the Investigations Department focused its attention on employees of various organisations who were abusing their position of trust by corruptly obtaining and then unlawfully disclosing personal information, usually for payment. This was a particular problem in organisations including police forces, the Department of Works and Pensions, the Inland Revenue and the DVLA. Several of these organisations worked with us closely to investigate the problem. As a result, a number of their employees currently stand suspended from duty pending prosecution.

It is worrying that a number of those involved in these offences were civilians working in police support roles, or actual serving police officers. They had unlawfully obtained and disclosed personal information from the Police National Computer (PNC). The police forces involved obviously viewed such conduct very seriously. In addition to prosecutions brought under data protection legislation by the Information Commissioner, all the forces involved have instituted additional proceedings against their employees for offences of Misconduct in Public Office, an offence which carries a penalty of up to 5 years' imprisonment. Not only have police employees been charged with this offence. Others identified in the chain,



many of whom are private detectives who paid these employees to unlawfully obtain the information for their clients, have been charged with aiding, abetting, counselling or procuring the offence of Misconduct in Public Office. This too carries a maximum of 5 years' imprisonment.

To date some fourteen individuals from three different police forces either stand charged or are still under investigation in relation to offences concerning Misconduct in Public Office. It should be noted that every police force involved in these investigations gave the Information Commissioner and his staff every assistance, as well as an assurance that any abuse of personal information held by the police would be treated as a matter of the utmost seriousness.

### The information blaggers

All the prosecutions in the past year have been for offences under section 55(1)(a) of the Data Protection Act 1998. This says that "a person must not knowingly or recklessly, without the consent of the data controller obtain or disclose personal data ..". Such offences may be committed where a person deceives or misleads an organisation into providing personal information that would not otherwise have been supplied. The offence may also arise where employees abuse their legitimate access to personal information by obtaining or disclosing it for their own purposes. Sometimes this is done for financial gain, in other cases the motivation to commit the offence may be a purely personal one.

- A private investigation company gave false and misleading information to the Driver Vehicle and Licensing Agency in order to find who a vehicle was registered to. The private detectives told the DVLA that they needed the information because they had repaired the vehicle but hadn't been paid. In fact they wanted the information for a client's use in on-going legal proceedings. The company was convicted of unlawfully obtaining personal data.

continued next page

### Records muddle

Mr Y was subject to a check by the Criminal Records Bureau, the organisation responsible for providing background information about individuals, including their criminal histories. A mistake was made and information about somebody else was provided. This led to problems with the Department for Further Education and Skills, who wanted to check out Mr Y's background in connection with his employment. The mix-up over the records occurred despite there being a number of discrepancies between Mr Y's details and the information on the retrieved records. The problem was sorted out and the issue led to CRB senior management ordering a review of the criteria used for matching records.

### Mistaken identity

A social worker's Enhanced Disclosure from the Criminal Records Bureau showed he had been given a twenty one month custodial sentence for robbery. Documentary evidence proved that the individual was undertaking a University degree course throughout the period when he was supposedly in prison. The force involved accepted that an administrative error had occurred due to its fingerprint procedures and arranged for force records and those of the CRB to be amended.

- A financial adviser wanted details of a potential client's insurance policies in order to provide him with financial advice. The client didn't give his authority for the adviser to contact his insurance company on his behalf. He preferred to contact his insurer himself and get back to the adviser in due course. Despite this, the adviser telephoned the insurance company pretending to be the client and obtained information about his policies. The adviser was convicted of unlawfully obtaining personal data.
- Before resigning from his job with a recruitment consultancy, the defendant forwarded copies of the company's clients' CVs to his home e-mail address. He did not seek permission to do this from his employer, nor were the clients aware of this. He was convicted of unlawfully obtaining personal data.
- A building society employee used his company's credit referencing facilities to find out information about the financial standing of his former partner's father. He should not have done this as the credit referencing facility was only to be used for business purposes, not for personal ones. He was convicted of unlawfully obtaining personal data.

Investigations Department Activity	98/99	99/00	00/01	01/02	02/03	03/04
Visits to business premises	700	388	480	448	573	649
Visits to dwellings	319	199	235	411	332	354
Witness statements obtained	433	346	355	375	513	544
Interviews under caution conducted	216	098	144	058	076	101



## Data protection in the global village

Data protection hit the headlines around the world when the United States and other governments started requiring airlines flying to their country, including European ones, to provide detailed passenger information (known as 'PNR'). Clearly it is legitimate for governments to put in place effective measures to prevent international terrorism. We accept that it is possible for governments to put in place adequate data protection safeguards whilst pursuing their objective of protecting citizens from the terrorist threat. However, the extent of the information, its lengthy retention and the range of organisations it could be passed on to contributed to concern that the safeguards in place to protect 'innocent' passengers would be insufficient to ensure compliance with international data protection standards.

The Article 29 Working Party, a forum of European data protection authorities in which we participate, considered the United States' requirements. Its conclusion was that there would not be an adequate level of protection for information about individual passengers. The European Commission's decision that the arrangements are adequate has been questioned by the European Parliament and referred to the European Court of Justice. Interestingly, the Article 29 Working Party considers that the arrangements put in place by the Australian government strike a proper balance between effective counter-terrorism and the protection of personal information. We fully support the European Commission's objective of finding a global solution to this difficult problem.

Outside Europe various countries and international bodies have been involved in initiatives to develop and implement data protection law. In some cases this may be motivated by a desire to facilitate the transfer of personal information to and from Europe. We have no doubt though that there is a realisation in many parts of the world that an effective data protection regime can provide valuable rights and protections for individuals and can bolster fledgling democracies. We have been particularly pleased to co-operate with the Commonwealth Secretariat on its work on privacy and access to information law.

After September 2001, there has been an understandable emphasis on ways of tightening international travel security. We have continued to support the work of the Organisation for Economic Co-operation and Development and the International Civil Aviation Organisation on the privacy implications of biometric travel documents. We hope that this work, and that carried out by other bodies such as the Council of Europe and the European Commission, will lead to a consistent body of useful guidance on the deployment of biometric identifiers in travel documents. We have also supported the OECD's work on the 'Economics of Trust', especially the privacy aspects of trust in e-commerce. We hope that some robust ideas about what individuals want and how to measure that will emerge, as well as information on the supply of privacy-enhancing products.

We have also supported work carried out by the Initiative for Privacy Standardisation in Europe, working under the auspices of the European Commission, on the role of standards work in contributing to the implementation of the data protection directives. This will look at contract clauses, best practice, audit, technological solutions and raising awareness. We have been very supportive of this work which is a way of helping those dealing with personal information to find robust and widely applicable solutions to data protection compliance problems in practical business circumstances.

### **The credit industry: another milestone in sight**

When you apply for credit how do you expect the lender to decide whether to give credit to you? Perhaps you think the decision will be based on:

- your current commitments;
- how you have repaid loans in the past;
- how you and your financial partner(s) have repaid loans in the past;
- how you and your family have repaid loans in the past, or
- a combination of these approaches.



Different lenders will make decisions in different ways, so there is no one answer. However, most lenders will use information provided by credit reference agencies when considering your application. This can include information about other people, usually ones with the same surname living at the same, or last previous, address at the same time as you in the same household. Many people object on privacy grounds to information about anyone except the person applying for credit being used in the decision whether to approve a credit application. We receive many complaints and queries about this. People object because of the principle involved. They also object because when they apply for their credit file they see information about the individuals linked to them. The situation also applies in reverse. On the industry side lenders have argued that the information about others linked to the person applying for credit is predictive and so valuable to them.

We have had concerns about this issue from the earliest days of the Office. Enforcement action and a data protection Tribunal decision in the early 1990's led to the current arrangements, which are an improvement on what had gone before. Yet our concerns and individuals' concerns about this issue remained. In late 2000 the credit industry proposed new processing arrangements to address these concerns and to ensure that individuals were protected from over-commitment and fraud by enabling the industry to continue to use certain aspects of others' information. Elizabeth France, the Information Commissioner at the time, commented that 'this is a 'win-win' situation for the individual and the credit industry.'

Since then we have monitored progress towards the implementation of these proposals and more recently have asked the industry to set a firm date for their industry-wide implementation. The industry has now announced that from October 31 this year the vast majority of lenders will be processing in line with the new proposals.

Once the new proposals are in place, when you apply for credit the credit reference agencies will only give the lender information about you and your financial partners. In some cases the lender may offer you the

### Travel Agent fined for serious breach of Data Protection Act

On Monday 10 November 2003, Nottingham Crown Court fined Mr Zbigniew Andrew Soltysik a total of £2,600 and ordered him to pay £1,000 costs for 13 offences of obtaining, and 13 offences of disclosing, personal information contrary to section 55 of the Data Protection Act 1998. In addition, the Defendant asked for a further 548 offences of unlawful obtaining and / or disclosing of personal information to be taken into consideration.

Mr Soltysik, from Mapperley, Nottinghamshire removed a database of customer details from his previous employer, Quality Travel in Grantham. He then used the database to send marketing material to Quality Travel's customers when he and his wife set up their own travel agents, New Style Travel. Quality Travel warned Mr Soltysik that his actions were breaching the Data Protection Act. However, as he continued to use the customer details, Quality Travel reported the case to us. We investigated and prosecuted Mr Soltysik under the Data Protection Act.

opportunity to 'opt -out' of this standard arrangement and to be assessed in your own right, subject to certain conditions.

The practical implementation of the new proposals is another milestone in bringing credit industry practices closer to individuals' legitimate expectations of privacy. This outcome has been achieved principally by co-operation rather than coercion. We will continue to work with the industry in this way as other credit-related issues come to the fore.

### Privacy at work?

Shortly before the publication of our last Annual Report we issued Part 3 of our Employment Practices Data Protection Code, 'Monitoring at Work'. The first two parts of the Code were criticised for being too long, detailed and complex for small businesses, in particular, to use. We tried to make Part 3 of the Code more accessible and user-friendly. In particular, we tried to translate the language of data protection into terms and concepts that the human resources professional, our primary target audience, would be familiar with. We were confident that the changes we made, including the provision of a summary document for small businesses, would address these concerns without losing the essential messages the Code was seeking to convey. It is encouraging that experience has confirmed that our confidence was justified. Part 3 of the Code has generally been well received, and we hope it will serve as a model for other guidance to be issued by us.

We have now drafted Part 4 of the Code. This deals with information about workers' health, including such issues as drug and alcohol testing in the workplace. We are using the same structure as Part 3 and put the draft version out for public consultation. We have now finished analysing the 100 plus responses, and generally they are favourable. The extent to which data protection requirements appear to be consistent with the professional standards of those working in the field of occupational health is particularly encouraging.

It now remains for us to publish the final version of Part 4, restructure Part 1 on 'Recruitment and Selection' and Part 2 on 'Employment Records'





in the new format and publish a combined volume. We hope next year to be able to report that this task has been completed.

### Health records, child protection

Given the sensitivity of health information, many individuals are keen to exercise their right of access to their health records. We have ensured that where this is the case, individuals are given the degree of access to which they are entitled by law. We have also supported and advised health professionals in making difficult decisions about whether or not the release of information would be likely to cause serious harm to the patient or to another individual. Our approach continues to be one which encourages the health sector to allow as much access to personal health information as possible.

For most individuals, the accuracy of their health record is an issue of great concern. We have conducted a number of assessments over the past year where the damage that could have been caused by an inaccurate record has been avoided by the record holder agreeing to correct the inaccuracy.

Towards the end of the year proposals for the NHS National Programme for IT emerged. This will provide for a nationally accessible form of all our health records. NHS officials have started to articulate the day to day working arrangements of the new system, and we have devoted a great deal of attention to this. These are early days for this significant development and we are committed to working with representatives from the programme to support them in developing realistic and sustainable data protection practices.

Elsewhere, public sector policy issues over the year included the development of a response to the Green Paper 'Every Child Matters', in which the Government detailed its policy response to the Victoria Climbié inquiry. The legislative proposals resulting from the Green Paper are now being taken forward in the Children Bill which was presented to the House of Lords in March 2004.

### Accountant fined £10,000 for data protection breach

On Monday 20 October 2003, at Birmingham Magistrates Court, Mr Abdullah Dervish pleaded guilty to eight offences of obtaining and two offences of disclosing personal information contrary to section 55 of the Data Protection Act 1998. In addition, the Defendant asked for a further 165 offences of unlawful obtaining and / or disclosing of personal information to be taken into consideration. The Magistrates fined Mr Dervish a total of £10,000 and ordered him to pay £5,000 costs. This is one of the largest financial penalties imposed by a court on an individual for offences under the Act.

Mr Dervish, a qualified accountant practising in Warley, West Midlands as A. Dervish & Co., had been an agent of Bradford & Bingley building society, providing a counter service from his offices. As such he had access to customer account data for the purposes of carrying out this service. In December 2000 he was given one month's notice terminating his agency for the company.

*continued next page*

### Accountant fined £10,000 for data protection breach

By February 2001 Bradford & Bingley had noticed that a number of accounts serviced by Mr Dervish had been placed on "notice to close". The court heard that Mr Dervish had placed closure notices on the accounts as part of a plan to open up new accounts for the same customers at another bank for which he had now become an agent. This action was outside the terms of his agency agreement. In March 2001 Mr Dervish was warned not to take any further unauthorised actions in relation to Bradford and Bingley customers. Nevertheless, the Defendant continued to contact these customers to try to get them to switch banks.

For the protection and benefit of its customers, Bradford & Bingley reported the facts surrounding this isolated incident to our Office and worked closely with us to bring the case to court. We investigated and prosecuted Mr Dervish under the Data Protection Act.

continued next page

### The end of spam and junk mail?

The Privacy and Electronic Communications (EC Directive) Regulations 2003 came into force on 11 December 2003. The Regulations expressly cover unsolicited marketing emails, and SMS messages, and include provisions regarding mobile phone location services.

Our experience in taking enforcement action in connection with unsolicited marketing faxes has convinced us that our existing enforcement powers are inappropriate. They do not allow us to take decisive action against those who continue to send unsolicited marketing material. The Department of Trade and Industry (DTI) is committed to reviewing our existing powers and continues to explore the possibility of providing us with some form of injunctive power which will enable us to take swift effective action.

The Regulations do not apply to emails sent to a corporate subscriber. This means that whilst an unsolicited marketing message sent to an individual's mobile phone or email address is covered, exactly the same message sent to a company-provided mobile phone or workplace computer will not be. Not surprisingly many find this difficult to understand.

The restrictions on unsolicited emails should ensure that reputable UK and EU based companies do not continue to send unwanted marketing material to individuals. It seems though that some major companies have difficulty in swiftly and efficiently ensuring suppression. Much 'spam' comes from outside the EU, giving rise to obvious jurisdictional problems which rule out any imminent end to the spam problem. However, the wide recognition of the problem has led to increased cooperation between industry, regulators and governments. We are committed to cooperating with DTI and the Office of Fair Trading, and with appropriate bodies outside the UK. However, we appreciate that formal regulation can be only part of the solution and recognise the efforts being made by industry in this area.

### Sending personal information overseas

The UK's data protection law, and the laws in place in the other EC countries, regulate the circumstances in which personal information can be transferred outside the European Economic Area. This is intended to



prevent data protection rules being circumvented by sending information to places where it will have no legal protection. This has been a particular issue recently in the context of companies outsourcing call-centres and similar operations to countries in Asia and elsewhere.

There are various ways in which an overseas transfer can be legitimised. However many companies find the existing options complex and onerous. Therefore the Article 29 working party, a group representing data protection authorities across the EC, agreed a working document in June 2003 aimed at providing a mechanism to enable multinational companies to transfer personal information throughout their organisation, even though this could involve sending information outside the European Economic Area. The idea is that the multinational organisation will establish a corporate-wide code of conduct for internal international transfers, binding upon all parts of the organisation. This should provide effective protection for individuals and permit appropriate supervision by national data protection authorities.

The ultimate intention is to simplify the approval process so that an application for approval of a set of such 'Binding Corporate Rules' is only made to one national data protection supervisory authority, usually in the country where the organisation has its EU headquarters. This supervisory authority then, in turn, seeks the view of the other national data protection authorities where the organisation has an interest in establishing the approval of all the authorities concerned. This is intended to reduce the burden on multinational organisations by removing the need to address the requirements of each EU Data Protection Authority separately.

We are keen to promote awareness and development of the binding corporate rules concept and have been working with organisations within the UK that are interested in this approach. We have also worked with other supervisory authorities with a view to developing a pan-European cooperation procedure.

### **The scope of data protection law: the 'Durant case'**

An important development this year was the judgment of the Court of Appeal in the case of *Durant v the Financial Services Authority (FSA)*.

### **Accountant fined £10,000 for data protection breach**

We were pleased to see the courts recognising the seriousness of these offences. The fines meted out in this case are significant. The result of this prosecution by our Office sends out a clear message to those engaged in similar activity that sharp practice in the handling of personal information, which amounts to an invasion of personal privacy, will not be tolerated by the Information Commissioner or by the Courts.

Mr. Durant was a customer of Barclays Bank plc. There was litigation between them which Mr. Durant lost in 1993. Since then he has sought disclosure of records in connection with the dispute which he believes may assist him to re-open claims against Barclays. In 2000 he asked the FSA to help him obtain disclosure. In addition, he wanted to know what documents the FSA had obtained from Barclays in its supervisory role. The FSA completed its investigation against Barclays and closed the investigation without informing Mr. Durant of the outcome due to its obligation of confidentiality under the Banking Act 1987. Mr. Durant complained about that to the FSA Complaints Commissioner who dismissed his complaint. In September/October 2001 Mr. Durant made two subject access requests under the Data Protection Act 1998 to the FSA. In October 2001 the FSA provided copies of documents relating to him held in computerised form, some redacted so as not to disclose the names of others. However, it refused access to all its manual files on the basis that the information sought was not “personal” and even if it was, it did not form part of a “relevant filing system”.

The Court considered four important issues of law concerning the right of access to personal data.

- What makes ‘data’ ‘personal’ within the meaning of ‘personal data’?
- What is meant by a ‘relevant filing system’?
- When is it ‘reasonable in all the circumstances’, within the meaning of section 7(4)(b) of the Data Protection Act 1998, to comply with a request for access to personal data even though the personal data include information about another person who has not consented to disclosure?
- How much discretion does the court have to order compliance with a request if it finds the data controller has wrongly refused a request under section 7(4)?

We have issued guidance on what we consider to be the two most important issues considered by the Court.

- What makes ‘data’ ‘personal’ within the meaning of ‘personal data’?
- What is meant by a ‘relevant filing system’?



In this case the Court of Appeal did not consider the issue of the identifiability of an individual in the definition of ‘personal data’ set out in section 1(1) of the Data Protection Act. Instead, the Court of Appeal concentrated on the meaning of ‘relate to’ in that definition, identifiability not being an issue in the case.

The Court of Appeal concluded that ‘personal data’ is information that affects [a person’s] privacy, whether in his personal or family life, business or professional capacity’. In situations where it is not immediately apparent what is meant by ‘relates to’, the Court offered some notions to assist in determining whether information is information which affects a person’s privacy.

‘The first is whether the information is biographical in a significant sense, that is, going beyond the recording of [the individual’s] involvement in a matter or an event which has no personal connotations...’

The second concerns focus. ‘The information should have the [individual] as its focus rather than some other person with whom he may have been involved or some transaction or event in which he may have figured or have had an interest ...’

In relation to relevant filing systems the judgment concluded that:

‘a ‘relevant filing system’ for the purposes of the Act, is limited to a system:

- 1) in which the files forming part of it are structured or referenced in such a way as to clearly indicate at the outset of the search whether specific information capable of amounting to personal data of an individual requesting it under section 7 is held within the system and, if so, in which file or files it is held; and
- 2) which has, as part of its own structure or referencing mechanism, a sufficiently sophisticated and detailed means of readily indicating whether and where in an individual file or files specific criteria or information about the applicant can be readily located.’

A case summary and the Commissioner’s comments on the impact of the case on the interpretation of the Data Protection Act 1998 can be found on our website.

## A Growing Office



### Home improvements at the Information Commissioner's Office

During the year we undertook a comprehensive review of our corporate objectives and operational structure. Our 'Home Improvement Project' (HIP) was based on wide staff participation and is intended to determine how we should be organised in order to carry out our increased statutory responsibilities in the most effective way. A number of HIP task forces were formed to consider issues ranging from the establishment of our core values to a review of our approach to enforcement and complaints handling. The work of these task forces is reflected in our Corporate Plan for 2004-2007. Our challenge in the coming year is put in place a revised organisational structure and improved procedures that will best enable us to meet our responsibilities.

### Home improvement: our objectives

- become more proactive and maximise our influence, targeting issues and cases where detriment is greatest and where we are especially well-placed to make a real impact;
- be more customer-focused and better at communicating with target audiences and working with other organisations;
- shift attention away from those complaints where we cannot provide remedies in favour of activities which promote good practice;
- transform our internal working methods, especially to enable us to demonstrate success;
- ensure a reputation for helpfulness and effectiveness;
- get the best from all those working here; and
- make the most of new technology and our regional offices.



Revisions to our corporate governance arrangements also took place during the year. Four non-executive members were appointed to our Management Board. We are already benefiting from the depth of their knowledge and the breadth of their expertise. Other revisions to our corporate governance arrangements include new support arrangements for our senior staff, the re-constitution of the audit committee and improvements to our risk management procedures.

The increasing demands on our office for advice about privacy and access issues have necessitated various improvements in our service delivery. Our Office runs a helpline which offers free advice on any aspect of data protection or freedom of information compliance. Feedback from the many that use our helpline is generally good. We are aware though that some callers were finding it very difficult to get through. Therefore in November we introduced new telephone software which has led to more efficient call distribution. The software enables us to monitor the number of calls we are taking and those that do not get through. This confirmed that we were unable to answer a considerable number of calls. We have tried therefore to ensure that more telephone lines are open. Despite staffing constraints we are now answering a significantly larger number of calls. During the period April to November 2003 the average number of calls answered per month was 5098, with a high of 5902. During the period December 2003 to March 2004 the average number of calls answered per month was 6630 with a high of 7674.

Last year we reported on activities taking place in connection with the modernising government programme. A new ICT infrastructure was rolled out in March 2003. This will support our key business processes and will help us meet targets related to electronic records management and electronic service delivery. A new electronic case handling system with integrated records management has been rolled out to teams handling enquiries, data protection casework and freedom of information publication schemes. New cases are scanned, classified, routed electronically and tracked through the case life-cycle. The benefits of the new application are:



**Job offer withdrawn**

The complainant successfully applied for a job with a local authority. However the local authority received a reference from her former employer and the job offer was withdrawn two days before the complainant was meant to start her new job. By this time the complainant had already resigned from her former position. The local authority refused to provide the complainant with a copy of the reference on the grounds that it was subject to a duty of confidence. The complainant was understandably concerned that if she continued to provide her former employer as a referee, which she would need to do, this would continue to have a detrimental effect on her chances of getting a new job.

continued next page

- increased productivity through better casework handling, correspondence tracking and more effective distribution of workload;
- better analysis of our casework, allowing us to target our guidance more effectively;
- more effective use of our resources; and
- the ability to pass work quickly to individuals, teams and, when fully rolled out, to our regional offices.

**Setting up in Scotland, Wales and Northern Ireland**

The Assistant Commissioners for our regional offices have now been in post for more than a year. Having completed their initial training in our main office, the Assistant Commissioners have now moved to offices in Edinburgh, Cardiff and Belfast. The Scottish Regional Office is settled in permanent accommodation in Thistle Street, Edinburgh. The Welsh and Northern Ireland regional offices are currently in temporary accommodation but the search for permanent accommodation is underway. Staff from Wilmslow and from the Welsh Assembly have been seconded to help establish the regional offices. It is hoped that over the next year recruitment for permanent staff will commence. However, the regional offices have already been very active in carrying out promotional activities in the areas of data protection and freedom of information.

The situation in Scotland is somewhat complicated because freedom of information is a devolved matter, with Scotland having its own Freedom of Information Act and Scottish Information Commissioner. This can be confusing, and we have done a great deal of promotional work to deal with this problem. For example, our Assistant Commissioner explained the data protection – freedom of information interface to an audience of over 500 people at a conference in Edinburgh. The interest in this area was such that the conference had to be repeated in early 2004 to cater for those who had been unable to attend the first event. Robert Turnbull, the Assistant Commissioner for Scotland, has said that ‘the move by the Commissioner to open an office in Scotland has been very warmly welcomed across all sectors especially local government and the Scottish





Executive. It shows that the Commissioner has responded positively to the devolution settlement and demonstrates his commitment to providing a local service tailored to local needs.'

Since our Cardiff office opened in November last year, Anne Jones, the Assistant Commissioner for Wales, has been developing contacts and building relationships with local public authorities and other interested parties, mainly through speaking engagements and other meetings. 'Issues of Welsh language, politics and geography are now starting to add local flavour to the office, with a Welsh language scheme currently in draft form, an audit underway of key guidance for possible translation and plenty of travel to meeting venues accessible to both north and south Walians,' said Anne. With more staff in place, the coming year should see the Office's profile raised considerably, in terms of awareness workshops, a freedom of information conference and greater publicity about the Office's existence.

Although the Northern Ireland Regional Office deals with both data protection and freedom of information, Marie Anderson, the Assistant Commissioner for Northern Ireland, has discovered that this year her work has mainly focused on promoting freedom of information. According to Marie, 'public authorities in Northern Ireland are keen to be ready for the January 2005 deadline. There is enormous interest in freedom of information here in Northern Ireland.' In January of this year a major freedom of information conference was held in the Stormont Hotel in Belfast. Speakers included the Information Commissioner, Maurice Frankel of the Campaign for Freedom of Information and Mrs Emily O'Reilly, the Irish Information Commissioner. The conference was an opportunity to launch our Belfast office. It was a great success and brought together 240 delegates from across the public sector in Northern Ireland.

### Job offer withdrawn

The local authority confirmed to us that the job offer was withdrawn because of the reference. The authority explained that it had a policy of giving access to references unless those giving the reference objected to this. In this case the reference had been marked 'confidential' and so it was withheld from the complainant. We decided to serve the local authority with a preliminary enforcement notice, requiring the authority to give access to the reference. We took this course of action because the information in the reference had already had a seriously adverse effect on the complainant and would probably continue to have such an effect. The former employer didn't provide any compelling reason for not disclosing the reference, and eventually a copy of the reference was provided. The Local Authority also said it would amend the guidance it gives to referees in order to encourage a more open approach in the future.



### **Marketing and communicating: increased understanding, greater professionalism.**

This year we have again increased our investment in supporting the public media. We recruited Citigate Communications to provide us with a full press office service and to support us in undertaking more proactive work. Early in the year we also developed a new media relations policy, which sets out our approach to dealing with the media. This was timely given that this year there has been a substantial increase in the volume of media enquiries and coverage of privacy and access to information issues. In particular, interest in the Freedom of Information Act grows as full implementation approaches. Clearly the journalistic community is interested in the increased access to official information that the Act will bring. As reported elsewhere in this Report, events like Soham led to a great deal of negative publicity coming our way. We have since launched a number of proactive media campaigns to challenge the myths and misunderstandings surrounding the legislation. This is part of a wider initiative to demystify the law we are responsible for enforcing.

We have undertaken a range of research projects this year, intended to develop our understanding of the needs of those we serve. These have included the following:

- annual tracking studies conducted to identify key patterns and trends in awareness of rights and obligations amongst the public, record holders and public authorities;
- a segmentation study, conducted to identify how individuals can be grouped and thus targeted with messages relating to their attitudes towards personal information, its use and potential abuse;
- an advertising tracking study aimed at evaluating the effectiveness of our national advertising campaign;
- a survey to identify how prepared public authorities are for the introduction of freedom of information access rights; and

- a qualitative study conducted amongst record holders on their attitudes to the legislation, the business benefits it provides and the services we offer to assist them.

We have also introduced a number of monitoring mechanisms to evaluate the performance of the services we offer. These include a website feedback facility, website visitor monitoring statistics and a publications feedback slip. We have also invested in a much improved website. This supports an e-mail alert when new content is posted, is easier for the public to navigate and generally has a more colourful and user-friendly appearance. We expect to make further improvements to the website in the near future.



'Review of Data Protection aims to remove confusion'. 24th December, 2003, Financial Times

'Reforms will crack data monitor codes'. 20th January, 2004, Personnel Today

'Don't hide behind data law, officials warned'. 14th January, 2004, Financial Times

'Workplace Monitoring - Code bans employers from snooping on workers'. 11th June, 2003, Financial Times

'Rogue firms exploit confusion over data'. 3rd February, 2004, Personnel Today





Information Commissioner

# accounts



01 January 2005

Dear UK Citizens

## Re: Freedom of Information Act

From the 1<sup>st</sup> of January 2005 everyone will have the right under the Freedom of Information Act to ask to see information which public authorities hold. This law will strengthen law laid down in the existing public subjecting. The Freedom of Information Act is designed to set the values of transparency, opening up the inner workings of all public authorities and subject to citizens and business.

## Information Commissioner's Accounts

for the year ended 31st march 2004

Foreword	54-58
Statement of the Information Commissioner's Responsibilities	59
Statement on internal control	60-64
Certificate and report of the Comptroller and Auditor General to the Houses of Parliament	65-67
Income and expenditure account	68
Balance sheet	69
Cashflow statement	70
Notes to the accounts	71-86

---

## Foreword

### Introduction

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 £19,200 (2002/2003 £18,150) and no other assurance or advisory services were provided.

### 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 the Data Protection Commissioner changed to the Information Commissioner with effect from 30 January 2001.



## Principal activities

The Information Commissioner has responsibilities and duties under the Data Protection Act 1998 and the Freedom of Information Act 2000.

The main purposes of the Data Protection Act 1998 are to:

- make the nature and use of personal data in computer systems and structured manual records open to public scrutiny (through promoting and enforcing the data protection principles);
- ensure good practice in the use, processing and protection of personal data in computer systems and structured manual records (through promoting and enforcing the data protection principles); and
- allow individuals to claim compensation for damage and any associated distress arising from any contravention of the requirements of the Data Protection Act.

During the year work has continued to implement the Freedom of Information Act 2000 and the revised Environmental Information Regulations expected to be made sometime in 2004. The main purposes of the Freedom of Information Act 2000 are to:

- provide for the general right of access to recorded information held by public authorities and to specify the conditions which need to be fulfilled before an authority is obliged to comply with a request for information;
- establish the arrangements for enforcement and appeal.

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 who reports directly to Parliament. He 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. All his 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.

The Information Commissioner also has responsibilities in relation to the Consumer Credit Act 1974, the Privacy and Electronic Communications (EC Directive) Regulation 2003 and in respect of European wide law enforcement systems. The Commissioner is the UK national supervisory authority for Europol, Eurodac, and the Customs Information System (CIS) and is a member of the Europol, Eurodac, Eurojust and CIS Joint Supervisory Authority. The Commissioner is also the designated national supervisory authority for the Schengen Information System and attends the SIS Joint Supervisory Authority as an observer prior to the UK accession.

Fuller details of the Information Commissioner's activities and progress towards his objectives during the year are given elsewhere in the annual report.

### **Results for the year**

The results for the year and the Information Commissioner's financial position at the end of the year are shown in the attached accounts.

The Income and Expenditure Account for the year ended 31 March 2004 shows a retained deficit of £254,397. This deficit arises due to HM Treasury guidance on the issue of grant in aid that precludes NDPBs from retaining more funds than are required for their immediate needs. Under normal conventions applied to Parliamentary control over income and expenditure, such grant in aid may not be issued or anticipated in advance of need.

As a result, the year on year movements in working capital (bank balances, debtors and creditors) held at the end of each financial year represent the retained deficit for the year and consequently the cumulative deficit in the Income and Expenditure reserve shown on the balance sheet represents the total working capital held by the business.





Grant in aid for 2004-2005 has already been included in the Department of Constitutional Affairs Estimate for that year, which has been approved by Parliament, and there is no reason to believe that the Department's future sponsorship and future parliamentary approval will not be forthcoming. It has accordingly been considered appropriate to adopt a going concern basis for the preparation of these financial statements.

### **Changes in fixed assets**

An IT based case-working and records management system has been developed and is currently being rolled out across the Office. An upgrade to the notification processing system platform is nearing completion. More details on fixed assets are given in note 8 to the accounts.

### **Future developments**

Full individual rights of access under the Freedom of Information Act 2000 come into force for all public authorities in January 2005. In the coming year the Office will approve the remaining publication schemes prepared by public authorities in accordance with the timetable laid down by the Lord Chancellor and will continue to expand accordingly to meet projected workloads.

Assistant Commissioners for Northern Ireland, Wales and Scotland have been recruited, and the Commissioner will take forward the development of their respective offices.

### **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, religious belief or disability. To further this policy the Office promotes the observance of good employment practice particularly when relevant to disabled people.

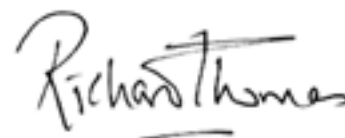
The Commissioner has an Equality Scheme approved by the Northern Ireland Equality Commissioner, produced as part of his responsibilities under section 75 of the Northern Ireland Act 1999. The Scheme has been reviewed in the year in advance of recruiting an Assistant Commissioner team to be based in Northern Ireland.

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 Office. 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 staff intranet and regular meeting with Trade Union representatives and this year briefings for all staff were held to ensure all staff were being kept up to date with changes affecting the Office. A formal Health and Safety Policy and Manual is available to all members of staff and a Health and Safety Committee is in place to address health and safety issues.

#### **Better payment practice code**

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 2004, 97.1% (31 March 2003 – 96.3%) 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%.



**Richard Thomas**  
**Information Commissioner**  
7th June 2004



## 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, total 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

### 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 I set for my Office, whilst safeguarding the public funds and assets for which I am personally responsible, in accordance with the responsibilities assigned to me in Government Accounting.

### 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 I set for my Office; 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 I have set, to evaluate the likelihood of those risks being realised and the impact should they be realised, and to manage them efficiently, effectively and economically. Unless noted otherwise the system of internal control has been in place for the year ended 31 March 2004 and up to the date of approval of the annual report and accounts, and accords with Treasury guidance.

### Capacity to handle risk

Each year a risk workshop is conducted involving managers from across all areas of activity within my Office. The workshop is facilitated by an external consultant and is used as an opportunity to provide guidance and training to staff on the management of risks, as well as identifying the key risks facing my Office.

The key risks arising from the Risk Workshop are identified for active management and members of my Management Board assume personal responsibility for the management of these key risks that could affect the achievement of the objectives I have set for my Office. Key risks which emerge at other times, for example, as a result of internal audit, are subject to the same management regime.



Risks that could affect the achievement of my objectives have been reviewed by my Management Board on a regular basis throughout 2003-2004. The main risks currently being actively managed result from the significant change and growth that my Office has and will continue to experience. The risks are:

- Information Technology: The organisation is currently 'rolling out' a significant programme of IT developments including a new casework and enquiry handling system, electronic service delivery channels, electronic records management system and a fully networked IT service to the devolved offices in Northern Ireland, Scotland and Wales. The risk is that a failure of, or delay in, the planned enhancements will impede the efficiency of my office and service delivery.
- Freedom of information: As January 2005, the date for full implementation of the Act draws nearer, there is a risk that the challenge of implementing FOI legislation effectively will not have been met. To succeed my Office has to give adequate explanation to the public to allow them to exercise their rights to information and to public authorities to allow them to meet their obligations to provide that information. I need to have approved, where appropriate, the publication schemes which have been submitted to me. I also have to have in place a management system and staffing to meet the as yet unknown demands of FOI casework. In addition I need to work closely with the Scottish Information Commissioner to ensure that our respective responsibilities are appropriately understood and discharged.
- Staffing and personnel: Staff numbers are continuing to grow in preparation of FOI casework. It is important that staff pay and conditions remain competitive in order to attract and retain the skills required for our work. The risk is that otherwise I shall be unable to meet the staffing demands of the FOI team and maintain my data protection work.

- **Reputation:** It is important for my Office to maintain public confidence. The risk to the reputation of my office is such that, as a regulator, I could find myself unable to carry out my data protection and freedom of information duties effectively.
- **Effective Management:** This is a time of significant change for my office, including freedom of information, significant IT enhancements, the development of devolved offices, and internal reorganisation. The risk is that ineffective management will result in the failure of one or all of these processes. As with all change it is essential therefore to manage the process well to ensure success.
- **Business Continuity:** My office needs an integrated and up to date business continuity plan for the IT and business functions of the office. My staff and I need to understand the potential impact on our business, put in place measures commensurate with the risk, and test those plans regularly. The risk is that without such preparation I shall be unable to respond effectively in time of unexpected challenge or disaster.

#### **The risk and control framework**

The main processes in place embedding risk management within the activity of the organisation are:

- a Management Board which now meets six times a year to consider the strategic direction of my Office, comprising both my Deputy Commissioners, my Legal Adviser, my Director of Personnel and Finance, and my Director of Marketing and Communications. In addition I have been able to enhance the composition of the Management Board with the appointment of four Non-Executive Board Members. The Board first met in its re-constituted form on 2 February 2004;
- an Executive Team of senior managers which (since February 2004) meets usually on a weekly basis to consider operational issues. Prior to this change my Management Board met formally once a month and informally most other weeks.



- the production of a Corporate Plan covering a three year period which is updated annually, which sets out the strategic objectives of my Office, which is translated into an annual Business Plan to articulate the detailed tasks and activities to be undertaken by each of the teams within my Office for the coming year;
- regular reports by internal audit to standards defined in the Government Internal Audit Manual which include their independent opinion on the adequacy and effectiveness of the Office's internal controls, together with recommendations for improvements where necessary;
- an Audit Committee which meets four times a year to monitor the operation of internal controls. For most of 2003-2004 the Audit Committee was chaired by myself and comprises my previous Management Board and one independent external member. It was attended by other members of my staff and representatives from the external and internal auditors. In March 2004 the new Management Board accepted my proposal to re-constitute the Audit Committee in line with the latest Guidance from HM Treasury. The new Audit Committee has clear terms of reference and is now chaired by one of my Non-Executive Board Members. The two other members are a second Non-Executive Board Member and one of my Deputy Commissioners. I and other members of my senior staff and representatives from the external and internal auditors will attend meetings.

### **Review of effectiveness**

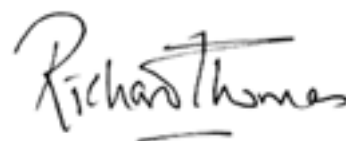
As Accounting Officer, I have responsibility for reviewing the effectiveness of the system of internal control. My review of the effectiveness of the system of internal control is informed by the work of the internal auditors and the executive managers within my Office who have responsibility for the development and maintenance of the internal control framework, and comments made by the external auditors in their management letter and other reports. I have been advised of the result of my review of the effectiveness of the system of internal control by my Management Board and the Audit Committee and a plan to address weaknesses and ensure

continuous improvement of the system is in place. All recommendations made by my internal auditors have been considered by the Audit Committee and the Committee is informed of progress toward implementing the outstanding recommendations at each meeting. I am able to report that there were no material weaknesses in the Office's system of internal controls which affected the achievement of my aims and objectives.

As mentioned in last year's statement, in view of the recent growth and increased responsibilities facing my Office I have strengthened Corporate Governance in the year by adding four Non Executive Board Members to my Management Board and re-constituting my Audit Committee with two Non-Executive Board Members, one of whom has succeeded me as chair to the Committee. I am also bringing forward plans to replace the current system of monitoring risks with a formal risk register.

Following the expiry of the current contract for provision of Internal Audit services on 31 March 2004, I have carried out a tendering process and am contracting with Price Waterhouse Coopers for the coming five year period.

I have also introduced improvements to the corporate planning process to ensure the three year Corporate Plan is a more relevant document for identifying my strategic objectives, and introduced a system of quarterly meetings with each team within my Office to monitor progress against my annual Business Plan.



**Richard Thomas**  
**Information Commissioner**  
7th June 2004



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

I certify that I have audited the financial statements on pages 68 to 86 under the Data Protection Act 1998. These financial statements have been prepared under the historical cost convention as modified by the revaluation of certain fixed assets and the accounting policies are set out on pages 71 and 73.

### **Respective responsibilities of the Information Commissioner and Auditor**

As described on page 59, the Information Commissioner is responsible for the preparation of 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 the Treasury and for ensuring the regularity of financial transactions. The Commissioner is also responsible for the preparation of the other contents of the Annual Report. My responsibilities, as independent auditor, are established by statute and I have regard to the standards and guidance issued by the Auditing Practices Board and the ethical guidance applicable to the auditing profession.

I report my opinion as to whether the financial statements give a true and fair view and are 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 the Treasury, and whether in all material respects the income and expenditure have been applied to the purposes intended by Parliament and the financial transactions conform to the authorities which govern them. I also report if, in my opinion the Foreword is not consistent with the financial statements, if the Commissioner has not kept proper accounting records, or if I have not received all the information and explanations I require for my audit.

I read the other information in the Annual Report and consider whether it is consistent with the audited financial statements. I consider the implications for my certificate if I become aware of any apparent mis-statements or material inconsistencies with the financial statements.



I review whether the statement on pages 60 and 64 reflects the Commissioner's compliance with Treasury's guidance on the Statement on Internal Control'. I report if it does not meet the requirements specified by Treasury, or if the statement is misleading or inconsistent with other information I am aware of from my audit of the financial statements. I am not required to consider, nor have I considered whether the Accounting Officer's Statement on Internal Control covers all risks controls. I am also not required to form an opinion on the effectiveness of the Commissioner's corporate governance procedures or its risk control procedures.

#### **Basis of audit opinion**

I conducted my audit in accordance with United Kingdom Auditing Standards issued by the Auditing Practices Board. An audit includes examination, on a test basis, of evidence relevant to the amounts, disclosures and regularity of financial transactions included in the financial statements. 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 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 are free from material mis-statement, whether caused by error, or by fraud or other irregularity and that, in all material respects, the income and expenditure 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 have also evaluated the overall adequacy of the presentation of information in the financial statements.



## Opinion

In my opinion

- the financial statements give a true and fair view of the state of affairs of the Information Commissioner at 31 March 2004 and of the income and expenditure, total recognised gains and losses and cash flows for the year then ended and 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
- in all material respects the income and expenditure 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**  
18th June 2004

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

### Income and Expenditure Account for the year ended 31 March 2004

	Note	2003/2004		2002/2003	
		£	£	£	£
<b>Income</b>					
Grant-in-aid	2	10,562,113		8,246,622	
Other income	6	16,334		62,035	
			10,578,447		8,308,657
<b>Expenditure</b>					
Staff costs	5	4,679,504		3,810,307	
Other operating costs	7	5,569,268		3,826,346	
Depreciation of tangible fixed assets	8	567,738		553,583	
			(10,816,510)		(8,190,236)
<b>Operating (deficit)/ surplus</b>			(238,063)		118,421
 Fee Income	3		8,764,030		7,577,427
Interest receivable			36,315		103,044
Notional cost of capital	1.7		(201,619)		(201,055)
 <b>Surplus for the year before appropriations</b>			8,360,663		7,597,837
 Notional cost of capital reversal	1.7		201,619		201,055
Appropriations due	4		(8,816,679)		(7,742,506)
 <b>Retained (deficit)/surplus for the year</b>			(254,397)		56,386

There were no recognised gains or losses other than reported above.

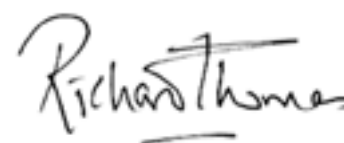
There were no material acquisitions or disposals in the year.

The notes on pages 71 to 86 form part of these accounts.

**Balance Sheet as at 31 March 2004**

	Note	31 March 2004		31 March 2003	
		£	£	£	£
<b>Fixed assets</b>					
Tangible fixed assets	8		6,590,321		5,952,435
<b>Current assets</b>					
Debtors and prepayments	9	5,119,008		4,860,568	
Cash at bank and in hand	13	326,597		234,854	
		5,445,605		5,095,422	
Creditors – amounts falling due within one year	10	(6,083,634)		(5,479,055)	
<b>Net current assets</b>			(638,029)		(383,633)
<b>Net assets</b>			5,952,292		5,568,802
<b>Capital and reserves</b>	11				
Income and expenditure reserve			(638,030)		(383,633)
Deferred government grant reserve			6,590,097		5,952,210
Revaluation reserve			225		225
			5,952,292		5,568,802

The notes on pages 71 to 86 form part of these accounts.



**Richard Thomas**  
Information Commissioner  
7th June 2004

## Cashflow Statement for the year ended 31 March 2004

	Note	2003/2004		2002/2003	
		£	£	£	£
Net cash inflow from operating activities	12		124,632		(937,694)
Returns on investment & servicing of finance					
Interest received			36,315		103,044
Investing activities					
Payment to acquire tangible fixed assets			(1,207,193)		(4,701,564)
Net cash inflow before financing			(1,046,246)		(5,536,214)
Financing					
Grant-in-aid for capital expenditure			1,207,193		4,701,564
Fee income	3		9,077,553		8,233,185
Appropriations made	4		(9,146,757)		(8,310,214)
			1,137,989		4,624,535
Increase/(Decrease) in cash			91,743		(911,679)

The notes on pages 71 to 86 form part of these accounts.

## 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 Executive Non-Departmental Public Bodies Annual Reports and Accounts Guidance 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 issues or adopted by the Accounting Standards Board to the extent that those requirements are appropriate.

These accounts have been prepared on a going concern basis.

### 1.2 Grant-in-aid

Grant-in-aid received for revenue expenditure is credited to income in the year to which it relates.

A proportion of the grant-in-aid received, equal to expenditure on fixed asset acquisitions in the period is taken to the Deferred Government Grant Reserve at the end of the financial year. The amount deferred is released back to the Income and Expenditure Account in line with depreciation charged. Losses on disposal of fixed assets are not debited to the Income and Expenditure Account, but are debited directly to the Deferred Government Grant Reserve.

### 1.3 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 the Price Index Numbers for Current Cost Accounting published by the Office for National Statistics when the effect of revaluing assets is material.

#### 1.4 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.

The principal rates adopted are:

Office fixtures	10 years
Office equipment	5 – 10 years
IT equipment and software	5 years
Assets under construction	nil

#### 1.5 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.

#### 1.6 Income recognition

Fee income comprises notification fees in respect of notifications by data controllers, under the Data Protection Act 1998. The notification fee 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.

Fee income is remitted regularly to the Secretary of State for Constitutional Affairs, and thus a prepayment is included in respect of income appropriated in advance of recognition of the income in the Income and Expenditure Account.

#### 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 % (2002-2003 – 6%) applied to the mean value of capital employed during the year.

#### 1.8 Pension costs

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



## 1.9 Operating leases

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

## 1.10 Value added tax

Most of the 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	Grant-in-aid	
	2003/2004 £	2002/2003 £
Grant-in-aid drawn from the Department for Constitutional Affairs	11,200,000	11,626,000
Grant-in-aid prepaid by the Lord Chancellor's Department	-	1,000,000
Transfer to deferred government grant reserve re: fixed assets additions	(1,205,625)	(4,932,961)
Release of deferred government grant re: depreciation charged	567,738	553,583
	<u>10,562,113</u>	<u>8,246,622</u>

3	Fee income	
	2003/2004 £	2002/2003 £
Deferred income at 1 April 2003	4,605,304	3,949,546
Fee receipts	9,077,553	8,233,185
Deferred income at 31 March 2004	(4,918,827)	(4,605,304)
Fee Income	<u>8,764,030</u>	<u>7,577,427</u>

## 4

## Appropriations

All data protection notification fees and other sums received by the Information Commissioner in the exercise of his functions are paid by him to the Secretary of State for Constitutional Affairs, in accordance with sub-paragraph 9(1) of Schedule 5 to the Data Protection Act 1998.

Sub-paragraph 9(3) of Schedule 5 to the Data Protection Act 1998 requires any sums received by the Secretary of State under sub-paragraph (1) shall be paid into the Consolidated Fund. However on 9th May 2003 HM Treasury laid before Parliament a Minute under the Government Resources and Accounts Act 2000 directing that such sums may be applied by the Department of Constitutional Affairs as appropriations in aid authorised by Parliament to resource the Department's Supply services, including amongst others, the Information Commissioner's grant-in-aid for the year ending 31 March 2004.

The income paid over by the Information Commissioner to the Secretary of State for Constitutional Affairs for these purposes was as follows:

(in cash terms)	2003/2004 £	2002/2003 £
Fee receipts (note 3)	9,077,553	8,233,185
Interest received	36,315	103,044
Other income (note 6)	16,334	62,035
Uncleared fees at 1 April 2003 (note 10)	233,874	145,824
Uncleared fees at 31 March 2004 (note 10)	(217,319)	(233,874)
	<u>9,146,757</u>	<u>8,310,214</u>

Appropriations due to the Secretary of State for Constitutional Affairs were:

(in accruals terms)	2003/2004 £	2002/2003 £
Fee receipts (note 3)	9,077,553	8,233,185
Interest received	36,315	103,044
Other income (note 6)	16,334	62,035
Deferred income at 1 April 2003 (note 10)	4,605,304	3,949,546
Deferred income at 31 March 2004 (note 10)	(4,918,827)	(4,605,304)
	<u>8,816,679</u>	<u>7,742,506</u>

**5****Staff numbers and costs****5a. Staff costs**

The aggregate staff costs were as follows:

	2003/2004 £	2002/2003 £
Wages and salaries	3,804,953	3,121,290
Social security costs	278,965	192,601
Other pension costs	481,345	403,340
Temporary agency staff	114,241	93,076
	<u>4,679,504</u>	<u>3,810,307</u>

The salary and pension entitlements of the Information Commissioner are paid directly from the Consolidated Fund and thus are not included above.

The Principal Civil Service Pension Scheme (PCSPS) is an unfunded multi-employer defined benefit scheme but the Information Commissioner is unable to identify its share of the underlying assets and liabilities. A full actuarial valuation was carried out at 31st March 2003. Details can be found in the resource accounts of the Cabinet Office: Civil Superannuation ([www.civilservice-pensions.gov.uk](http://www.civilservice-pensions.gov.uk)).

For 2003-2004, employers' contributions of £476,619 were payable to the PCSPS (2002/2003 - £381,749) at one of four rates in the range of 12% - 18.5% of pensionable pay, based on salary bands. The scheme's Actuary reviews employer contributions every four years following a full scheme valuation. Rates will remain the same next year, subject to revalorisation of the salary bands. The contribution rates reflect benefits as they are accrued, not when the costs are actually incurred, and reflect past experience of the scheme.

Employees joining after 1 October 2002 could opt to open a partnership pension account, a stakeholder pension with an employer contribution. Employers' contributions of £3,543 were paid to one or more of a panel of four appointed stakeholder pension providers. Employer 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 contributions of £1,183, 0.8 per cent of pensionable pay, were payable to the PCSPS to cover the cost on death in service and ill health retirement of these employees.

No persons retired early on ill-health grounds; the total additional accrued pension liabilities in the year amounted to £nil.

## 5b. Staff numbers

The average number of full time equivalent persons employed by the Information Commissioner during the year was as follows:

	2003/2004 No.	2002/2003 No.
Management Board	5	5
Senior staff	11	8
Other staff	181	176
Casual and temporary agency staff	11	9
	<u>208</u>	<u>198</u>

## 5c. Senior management

The salary and pension entitlements of the most senior managers were as follows:

	Column 1 Salary including performance pay (£k)	Column 2 Benefits in kind (rounded to nearest £100)	Column 3 Real increase in pension and related lump sum at age 60 (£k)	Column 4 Total accrued pension at age 60 at 31/3/04 and related lump sum (£k)	Column 5 CETV at 31/3/03 (nearest £k)	Column 6 CETV at 31/3/04 (nearest £k)	Column 7 Real increase in CETV after adjustment for inflation and changes in market investment factors (nearest £k)	Column 8 Employer contribution to partnership pension account including risk benefit cover – to nearest £100
* Non Executive Board Member appointed 17/12/03	(2002/2003 Comparative in brackets)							
Richard Thomas Commissioner	90-95 (25-30)	-	0-2.5	20-25	277	302	12	-
Francis Aldhouse Deputy Commissioner	70-75 (65-70)	-	0-2.5 plus 0-2.5 lump sum	25-30 plus 85-90 lump sum	490	527	23	-
Graham Smith Deputy Commissioner	60-65 (55-60)	-	0-2.5 plus 2.5-3 lump sum	0-5 plus 5-10 lump sum	17	30	12	-
Dr Robert Chilton Non-Executive Board Member*	0-5	-	-	-	-	-	-	-
David Clarke Non-Executive Board Member*	0-5	-	-	-	-	-	-	-
Sir Alistair Graham Non-Executive Board Member*	0-5	-	-	-	-	-	-	-
Clare Tickell Non-Executive Board Member*	0-5	-	-	-	-	-	-	-

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

Pension benefits are provided through the Civil Service pension arrangements. From 1 October 2002, civil servants 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 good quality 'money purchase' stakeholder arrangement with a significant employer contribution (partnership pension account).

Employee contributions are set at the rate 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 year's 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 as per 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. 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 CSP arrangements can be found at the website [www.civilservice-pension.gov.uk](http://www.civilservice-pension.gov.uk)

Columns 5 & 6 of the above table show the member's cash equivalent transfer value (CETV) accrued at the beginning and the end of the reporting period. Column 7 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 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 or

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 CSP arrangements and for which the CS Vote has received a transfer payment commensurate to 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.

**6****Other income**

	2003/2004 £	2002/2003 £
Legal fees recovered	7,785	6,245
Contributions toward cost of international conference	-	39,640
Other	8,549	16,150
	<u>16,334</u>	<u>62,035</u>

**7****Other operating costs**

	2003/2004 £	2002/2003 £
Rent and rates	674,557	633,827
Maintenance, cleaning, heating and lighting	139,926	129,335
Office supplies, printing and stationery	179,539	246,162
Carriage and telecommunications	178,778	133,180
Travel, subsistence and hospitality	443,807	310,537
Staff recruitment	139,097	105,236
Specialist assistance and research	407,036	135,189
Education and awareness	1,275,153	1,149,679
Legal costs	175,627	173,971
Staff training, health and safety	197,736	152,215
IT/IS expenses	1,736,751	637,663
Vehicle expenses	2,061	1,202
Audit fee	19,200	18,150
	<u>5,569,268</u>	<u>3,826,346</u>

Included above are operating lease payments for land & buildings of £545,240 (2002/2003 £511,883).

## 8

## Tangible fixed assets

	Equipment & Furniture £	Information Technology £	Assets under construction £	Total £
<b>Cost or valuation</b>				
At 1 April 2003	277,029	2,530,181	3,777,559	6,584,769
Additions	26,508	-	1,179,116	1,205,624
Transferred		52,589	(52,589)	
At 31 March 2004	303,537	2,582,770	4,904,086	7,790,393
<b>Depreciation</b>				
At 1 April 2003	126,298	506,036	-	632,334
Charged in year	51,184	516,554	-	567,738
At 31 March 2004	177,482	1,022,590	-	1,200,072
<b>Net Book Value</b>				
At 31 March 2004	126,055	1,560,180	4,904,086	6,590,321
At 31 March 2003	150,731	2,024,145	3,777,559	5,952,435

Tangible fixed assets totalling £49,986 (2002/2003 - £69,537) have not been capitalised and are included within 'Other operating costs', as the individual costs were below the capitalisation threshold of £2,000.

Assets have not been re-valued in the year as the effect of revaluing assets would be to reduce the cost of assets in use by £82,191 and makes no material difference to the results for the year or the financial position at the year end.

Assets under construction represent Information Technology projects not yet brought into service, comprising a casework management system £4,433,014 and upgraded notification platform £408,288 and IT infrastructure £62,784.

As described in note 15, Information Services are provided by a managed service agreement. The title of hardware and software procured under this agreement is owned by Fujitsu Services Limited. The Commissioner is entitled to purchase the title of such assets for a nominal sum in the event the agreement is terminated. Payments made for IT hardware purchase and software development are capitalised and the net book value of such assets at 31 March 2004 was £6,422,195 (31 March 2003 - £5,801,704).



**9 Debtors**

	31 March 2004 £	31 March 2003 £
Fee income prepaid to the Secretary of State for Constitutional Affairs	4,918,827	4,605,304
Other prepayments	188,823	241,045
Other debtors	11,358	14,219
	<u>5,119,008</u>	<u>4,860,568</u>

**10 Creditors; amounts falling due within one year**

	31 March 2004 £	31 March 2003 £
Trade creditors	462,762	169,053
Payroll	50,624	73,185
Other taxes and social security	3,754	6,449
Accruals	26,725	18,150
Un-remitted and un-cleared fees	325,376	233,874
IS/IT retentions on assets under construction	295,566	373,040
Deferred income	<u>4,918,827</u>	<u>4,605,304</u>
	<u>6,083,634</u>	<u>5,479,055</u>

**11 Reserves**

	Income & Expenditure Reserve £	Deferred Government Grant Reserve £	Revaluation Reserve £	Total £
Balance at 1 April 2003	(383,633)	5,952,210	225	5,568,802
Retained surplus for the year	(254,397)	-	-	(254,397)
Grant deferred for additions	-	1,205,625	-	1,205,625
Release for depreciation	-	(567,738)	-	(567,738)
Balance at 31 March 2004	(638,030)	6,590,097	225	5,952,292

**12 Reconciliation of operating surplus to net cash inflow from operations**

	2003/ 2004 £	2002/2003 £
Operating (deficit)/surplus for the year	(238,063)	118,421
Depreciation provided in year	567,738	553,583
Release of deferred government grant	(567,738)	(553,583)
Reduction/(Increase) in debtors relating to operating activities	55,084	(102,938)
Increase/(Reduction) in creditors relating to operating activities	307,611	(953,177)
Net cash inflow from operating activities	124,632	(937,694)

**13 Cash at bank and in hand**

	2003/ 2004 £	2002/2003 £
Balance at 1 April 2003	234,854	1,146,533
Increase/(Decrease) in cash	91,743	(911,679)
Balance at 31 March 2004	326,597	234,854
Commercial banks	325,937	234,183
Cash in hand	660	671
	326,597	234,854

**14****Commitments under operating leases**

At 31 March 2004 the Information Commissioner was committed to make the following annual payments in respect of operating leases expiring:

	Land and Buildings	
	31 March 2004 £	31 March 2003 £
within one year	-	3,380
between two to five years	106,328	79,019
after five years	381,875	381,875
	<u>488,203</u>	<u>464,274</u>

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

**15****Contingent liabilities**

The Information Commissioner has entered into a managed service agreement with Fujitsu Services Limited for the provision of Information Services (note 8). The contract term is ten years expiring in July 2007. Expenditure under the contract in the year was:

	31 March 2004 £	31 March 2003 £
Desktop and Notification services	852,825	635,277
IS/IT development	1,417,884	4,153,762
	<u>2,270,709</u>	<u>4,789,039</u>
Cost of cancelling the contract at 31 March	<u>152,447</u>	<u>108,114</u>

**16****Capital commitments**

No capital commitments were outstanding at 31 March 2004 (31 March 2003 – nil).

## 17

## Related party transactions

The Information Commissioner confirms that he had no personal or business interests which conflict with his responsibilities as 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 of notification fee income and 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 Superannuation Service.

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

## 18

## Financial instruments

Financial Reporting Standard 13, Derivatives 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 that 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 FRS13, 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 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's financial assets and liabilities carry nil or fixed rates of interest. The Information Commissioner is not, therefore, exposed to significant interest rate risk.

## Foreign currency risk

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

19

## Statement of resources by function

The Secretary of State for Constitutional Affairs provides grant-in-aid to the Commissioner for data protection and freedom of information statutory functions annually.

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 accounts system. This system allocates expenditure to various value centres across the organisation. A financial model is then used to apportion expenditure between the functions on an actual basis where possible, or by way of a reasoned estimate where costs are shared between functions.

In accruals terms	Unaudited Comparatives					
	freedom of information £	data protection £	2003/2004 £	freedom of information £	data protection £	2002/2003 £
<b>Income</b>						
Grant-in-aid	3,811,109	6,751,004	10,562,113	2,181,651	6,064,971	8,246,622
Other income	-	16,334	16,334	-	62,035	62,035
	<u>3,811,109</u>	<u>6,767,338</u>	<u>10,578,447</u>	<u>2,181,651</u>	<u>6,127,006</u>	<u>8,308,657</u>
<b>Expenditure</b>						
Staff costs	1,360,993	3,318,511	4,679,504	968,803	2,841,504	3,810,307
Other operating costs	2,301,335	3,267,933	5,569,268	1,057,183	2,769,163	3,826,346
Depreciation	209,777	357,961	567,738	136,018	417,565	553,583
	<u>3,872,105</u>	<u>6,944,405</u>	<u>10,816,510</u>	<u>2,162,004</u>	<u>6,028,232</u>	<u>8,190,236</u>
<b>Operating deficit/surplus</b>	<u>(60,996)</u>	<u>(177,067)</u>	<u>(238,063)</u>	<u>19,647</u>	<u>98,774</u>	<u>118,421</u>
<b>Fee income</b>	-	8,764,030	8,764,030	-	7,577,427	7,577,427

The data protection notification fee is set by the Secretary of State for Constitutional Affairs, and in making any fee regulations under Para. 26 of the Data Protection Act 1998, as amended by Para. 26 of Section 17 of Schedule 2 to the Freedom of Information Act 2000, the Secretary of State shall have regard to the desirability of securing that the fees payable to the 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 Commissioner, other than for the grant-in-aid payments made to the Commissioner, and therefore the accounts cannot be used to demonstrate that the data protection fees match expenditure on data protection activities.

The segmental information above has not been disclosed for the purpose of Standard Statement of Accounting Practice 25: Segmental Reporting, or for compliance with the Treasury Fees and Charges Guide.

## Facts and Figures

### Output Measures and Performance Indicators

Financial Years 2002 / 2003 to 2006 / 2007

Notification	Actuals 2002/2003	Ests/Targets 2003/2004	Actuals 2003/2004	Ests/Targets 2004/2005	Ests/Targets 2005/2006	Ests/Targets 2006/2007
Number of weighted transactions processed	505,754	415,427	515,640	350,874	306,785	295,980
Number of weighted transactions processed per officer day	88.02	127.14	133.33	135.89	126.88	124.68

There are three notification 'products' - new applications, renewals and changes. Each product is weighted in accordance with its processing time so year-on-year comparisons of performance can be made, reflecting the differing workloads encountered. The 'processed per officer day' figures incorporate different levels of staff from year to year and encompass increased productivity targets, and are calculated from the weighted figures. Transformations (from the 1984 Act) ceased during FY 2003/2004. The target for processing weighted transactions was revised to reflect the improved systems of handling the notification products, as shown by the outcome.

Assessments and Complaints	Actuals 2002/2003	Ests/Targets 2003/2004	Actuals 2003/2004	Ests/Targets 2004/2005	Ests/Targets 2005/2006	Ests/Targets 2006/2007
Total requests for Assessment received	12,001	12,866	11,664	11,500	11,500	12,000
Handled as Enquiries	5,677	6,086	5,595	5,517	5,517	5,756
No Assessment made	1,317	1,411	1,197	1,180	1,180	1,231
Sub-total	6,994	7,497	6,792	6,697	6,697	6,987
Assessments completed*	4,564	4,893	4,798	4,731	4,731	4,937
Complaints from the 1984 Act closed	244	57	54	3	0	0
Sub-total	4,808	4,950	4,852	4,734	4,731	4,937
Number closed per Officer day	0.72	0.77	0.70	0.74	0.74	0.77

\*Assessments completed comprise 'Telecom Regulations, Consumer Credit Act cases and request for assessment completed'. Currently there are still 3 complaints being investigated (made under the provisions of the 1984 Act). Requests for assessment made under the 1998 Act are processed differently from complaints. From 2000/2001 the number closed per officer day figure encompasses complaints closed and assessments completed.

<b>Contact with our customers</b>	Actuals 2002/2003	Ests/Targets 2003/2004	Actuals 2003/2004	Ests/Targets 2004/2005	Ests/Targets 2005/2006	Ests/Targets 2006/2007
Telephone Enquiries received by the data protection Helpline*	59,486	75,000	68,076	100,000	100,000	100,000
Calls received per line hour	9.21	7.36	7.25	7.52	7.52	7.52

Contact is to all areas of the Office. Notification has its own dedicated enquiry line and media enquiries with whom they have had previous contact. The Helpline handles all general calls from organisations and individuals. Telephone enquiries represent the calls received by the Helpline, and 'line hours' are the hours spent by staff dealing with these enquiries. The target figures for the 'calls received per line hour' are based on efficiency improvements gained from using new telephony equipment and having more lines open. Staff employed on the Helpline also deal with written queries, correspondence connected with existing cases and administrative work for the compliance departments.

\*Previously the Information Line

#### Public Awareness and Awareness of Rights

<b>Data Protection</b>	Actuals 2002/2003	Ests/Targets 2003/2004	Actuals 2003/2004	Ests/Targets 2004/2005	Ests/Targets 2005/2006	Ests/Targets 2006/2007
% Total data controllers aware of subjects rights	92%	94%	89%	92%	94%	96%
% individuals aware of own rights	74%	78%	74%	75%	75%	76%

<b>Freedom of Information</b>	Actuals 2002/2003	Ests/Targets 2003/2004	Actuals 2003/2004	Ests/Targets 2004/2005	Ests/Targets 2005/2006	Ests/Targets 2006/2007
% individuals aware of own rights of their obligations	49%	50%	56%	60%	63%	65%
% of public authorities aware	53%	60%	84%	95%	98%	98%

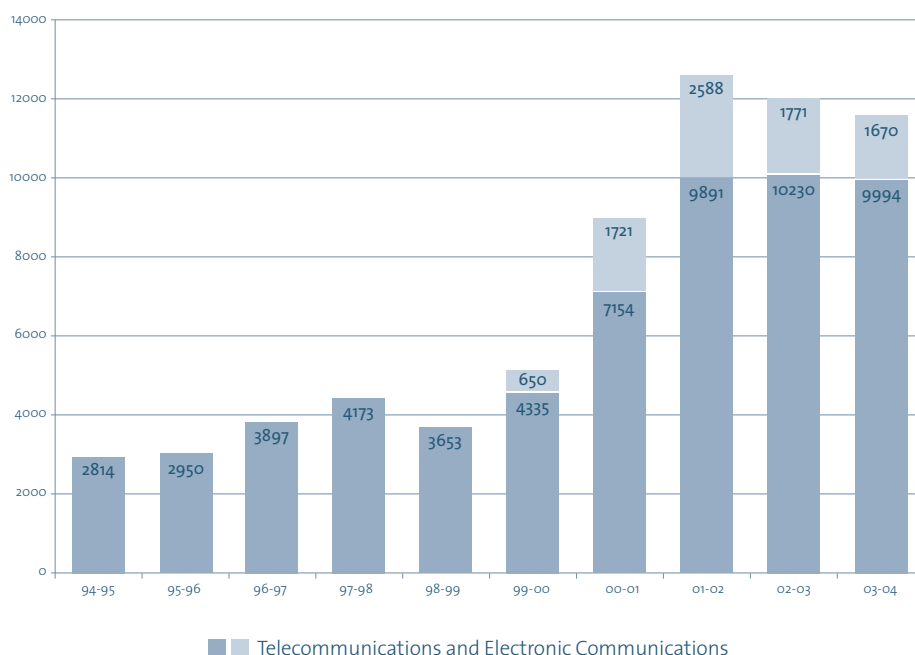
The figures are based on annual tracking research in the spring of each year. Anyone requiring more detailed statistics and information is welcome to apply to the Office.



## Our Annual Caseload

Our caseload consists of enquiries and complaints of differing sorts. The bulk of complaints are requests under the Data Protection Act 1998 to assess whether the processing of personal information carried out by an organisation met the requirements of the Act. However we also receive complaints about companies which have failed to comply with the Privacy and Electronic Communications Regulations 2003<sup>1</sup> under which complaints can be made about the sending of unsolicited direct marketing phone calls, faxes, automated calls, text/picture/video messages and emails. Some 1670 complaints of this type were received in the last year. We also deal with complaints about inaccurate consumer credit files which fall under the Consumer Credit Act 1974 and unfair contract terms. The total number we received this year was 11,664.

Complaints/ requests for assessment received 1994 - 2004



<sup>1</sup> These replaced the Telecommunications (Data Protection and Privacy) Regulations 1999 in December 2003

The types of issues which are raised in these complaints can be seen in the case summaries throughout this report. These put the flesh on the bones of these statistics and make clear how important these issues can be to the individuals concerned. However we are not able in every case to consider the issues which someone raises. Some 12 % of the complaints we dealt with in the last year fell outside the remit of the Act.

When we consider a complaint under the Data Protection Act we are under a duty to decide whether or not the processing in question was likely or unlikely to have met the requirements of the Act. This means that in some cases we are able to come to a decision straight away by examining the evidence presented to us. However it is not always possible to do this and we may require further information from the complainant, the organisation or both. Our aim is to give the complainant a view as to the likelihood as to whether or not the provisions of the Act have been broken. The Data Protection Act gives individuals the right to claim compensation in the courts if they have suffered damage from a contravention of the Act. The assessment we are under a duty to make will in some instances help individuals to do this.

Every year we respond to a significant number of written enquiries from the public about these issues – this year there were 5,595. In some cases, when for lack of information we are not able to give a view as to whether an organisation has complied or not with the Act, we are able to give authoritative advice on the issue so that individuals are able to take the matter forward for themselves.

The number of cases which we resolved in 2003-2004 was 11,644 in total. Of these some 90% were closed within 3 months.

### Complaints made under DPA 1984

1984 Complaints Investigated and Closed

54

### Assessments Enquiries made under DPA 1998

Total cases received (includes enquiries)

11664

Telecommunications and Electronic Communications

1670

### Cases Closed

Enquiries

5595

No assessment made (assessment declined + no assessment made)

1197

Telecom Regulations, Consumer Credit Act

cases and requests for assessments completed

4798

### Total cases complete

11644

### Requests received and closed were about:

Consumer Credit (Total of Team 8's work)

2097

17%

Telecoms and Electronic Communications

1540

13%

Other

8007

70%

### Time to Close

Closed within 0-3 months

10423

90%

Closed within 3-6 months

571

5%

Closed within 6-9 months

157

1%

Closed within 9-12 months

262

2%

Closed in over 12 months

177

2%

1984 cases closed

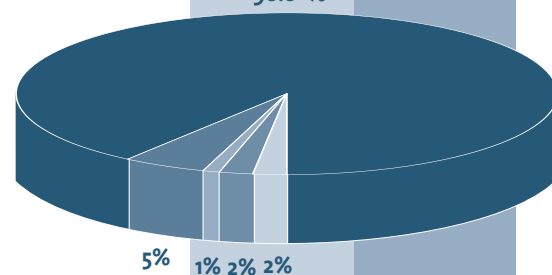
54

### TOTAL

11644

100%

90.0 %



### Recorded Outcomes

Advice Given (including telecoms)

5690

57.0%

Request for assessment declined

628

Threshold criteria not met

569

Sub total

1197

12.0%

Compliance Unlikely

1588

16.0%

Compliance Likely

1469

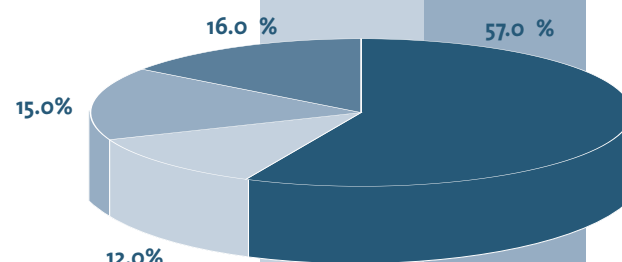
15.0%

(percentages calculated to give 100% of outcomes listed)

### TOTAL

9944

100%



### Assessments outstanding

1210

## Prosecutions 1 April 2003 – 31 March 2004

[illegible]

NOTE: 55(1) Obt means obtaining personal data. 55(1) Dis means disclosing personal data.  
TICs Other offences taken into consideration



01 January 2005

Dear UK Citizens

**Re: Freedom of Information Act**

From the 1<sup>st</sup> of January 2005 everyone will have the right under the Freedom of Information Act to ask to see information which public authorities hold. This law will stretch from No. 10 down to the smallest public authority. The Freedom of Information Act is designed to end the culture of unnecessary secrecy opening up the inner workings of all public authorities and service to citizens and business.



Information Commissioner



01 January 2005

Dear UK Citizens

**Re: Freedom of Information Act**

From the 1<sup>st</sup> of January 2005 everyone will have the right under the Freedom of Information Act to ask to see information which public authorities hold. That law will stretch from No. 10 down to the smallest public authority. The Freedom of Information Act is designed to end the culture of unnecessary secrecy, opening up the inner workings of all public authorities and service to citizens and business.



Information Commissioner

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

**Online**

[www.tso.co.uk/bookshop](http://www.tso.co.uk/bookshop)

**Mail, Telephone, Fax & 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](mailto:book.orders@tso.co.uk)

Textphone 0870 240 3701

**TSO Shops**

123 Kingsway, London WC2B 6PQ

020 7242 6393 Fax 020 7242 6394

68-69 Bull Street, Birmingham B4 6AD

0121 236 9696 Fax 0121 236 9699

9-21 Princess Street, Manchester M60 8AS

0161 834 7201 Fax 0161 833 0634

16 Arthur Street, Belfast BT1 4GD

028 9023 8451 Fax 028 9023 5401

18-19 High Street, Cardiff CF10 1PT

029 2039 5548 Fax 029 2038 4347

71 Lothian Road, Edinburgh EH3 9AZ

0870 606 5566 Fax 0870 606 5588

**TSO Accredited Agents**

(see Yellow Pages)

and through good booksellers

