



# Information Commissioner Annual report and accounts for the year ending 31 March 2001

**June 2001**

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

Ordered by the House of Commons to be printed 10 July 2001

London: The Stationery Office

Price: £14.95





# Contents



<b>Our mission</b>	<b>5</b>
<b>Commissioner's foreword</b>	<b>6</b>
<b>Chapter 1: Review of the year</b>	<b>8</b>
<b>Chapter 2: Some challenges ahead</b>	<b>11</b>
Making Modern Government Work	11
Improving Data Quality	12
Responding to Cybercrime	14
Delivering Our Employment Code	15
Promoting Publication Schemes	16
Managing Change	17
<b>Chapter 3: Implementation</b>	<b>19</b>
Enforcement Action	21
Other Enforcement Work	23
National Security Appeals	23
Utilities	24
The BAIRD Project	26
<b>Chapter 4: Investing in education and awareness</b>	<b>27</b>
Identifying Needs	27
Raising Awareness	27
Monitoring Effectiveness	28
A Corporate Change	30
Investing in Knowledge	30
Working with the Media	30
Empowering Individuals	31

<b>Chapter 5: International and European work</b>	<b>32</b>
European Work	32
Europol, the Customs Information System and Schengen	33
European Codes of Practice and Standards	34
Other European Issues	35
The Council of Europe Cybercrime Convention	35
The Wider World	36
 <b>Chapter 6: Organisational matters</b>	 <b>38</b>
Staffing Matters	38
Finance	41
Planning	42
Property	42
 <b>Chapter 7: Financial matters</b>	 <b>44</b>
 <b>Chapter 8: The year ahead</b>	 <b>47</b>
 <b>Information Commissioner's Accounts 2000/2001</b>	 <b>51</b>
 <b>Appendix:</b>	 <b>75</b>
Our Annual Caseload	76
Notification Department Statistics	82
Output Measures and Performance Indicators	83

Note: The main body of this report outlines the main issues and developments of the office during the year. Although most figures relate to the year ending 31 March 2001, the report includes references to the developments which have taken place between the year-end and publication.

# Our mission



We shall develop respect for the private lives of individuals and encourage the openness and accountability of public authorities:

- by promoting good information handling practice and enforcing data protection and freedom of information legislation; and
- by seeking to influence national and international thinking on privacy and on information access issues.



**Management Board** (left to right):

Francis Aldhouse, *Deputy Commissioner*; Mike Duffy, *Director of Personnel and Finance*; Elizabeth France, *Commissioner*; Nicholas Tyler, *Legal Adviser*; Graham Smith, *Deputy Commissioner* & Helen Corkery, *Director of Marketing & Communications*.



# Commissioner's foreword



This year we report on a full year's work under the regime introduced by the Data Protection Act 1998. The changes it has brought have been developments from the framework of rights and responsibilities provided by the 1984 Act which, over many years, we had learned to interpret and apply. It has been a year of transition. We have had to ensure our own familiarity with the changed requirements placed upon us. Differences in the detail of the law are having an impact on our approach. Notification is not the same as registration. Our response to a 'request for an assessment' made under the 1998 Act cannot be the same as our approach to a 'complaint' under the 1984 Act. Most significantly, changes in definitions of key terms have had an effect on the scope of the 1998 Act which has become clearer as we have moved from studying the requirements to applying them in practice.

The law itself allowed a period of transition so that its new requirements only apply from 24 October 2001 to processing that was already under way. This period of grace has been understood and well used by many major data controllers. There are, however, some who are only now appreciating that the Act will apply fully to their processing in a few months time. This has led to a number of recent reactions of concern which we have already worked through with others. There should be nothing in the Data Protection Act which prevents the achievement of a legitimate business objective. What it does is to ensure that that objective is met in a way which respects the rights of the individual whose data are being processed. That does not mean that processing can only be done with consent (the Act provides other bases). It does, however, mean that in most cases we have a right, as individuals, to know what is being done.

Volumes of work have been higher than ever before. That has fitted with our annual tracking research showing data subjects awareness of their rights also at their highest. Awareness levels can be linked to our advertising spend, however news items relating to the role of the Act and the fact that the right of 'subject access' (the right to see what is held about oneself), was considered a suitable issue for the Mark Thomas show, will also have had an impact. Indeed media interest indicates that the Act provides a set of rights which are of increasing value in modern society.

Research surveys support this view. The growth of public concern about on-line privacy becomes ever clearer from them. A number of major

companies, such as Intel, have experienced the severe market and publicity impact of failing to take account of privacy issues and have now taken very positive steps to reconstruct their policies and working methods. When reporting last year the US and the EU were still in dialogue seeking to achieve a way to allow transfer of personal data. Their perspectives seemed very different. The 'Safe Harbor' agreement represented the best way forward. Perhaps the Intel example is an indication of what may be a changing spirit in the US. It was also reflected in recent Congressional Committee hearings to which one of our Assistant Commissioners gave evidence. We look to see whether the international privacy scene might not be transformed by US legislation.

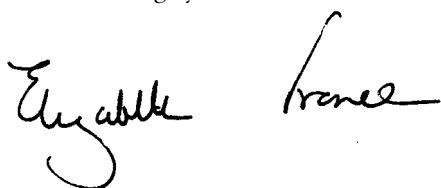
On 30 January 2001 I took responsibility for freedom of information. My title was changed to Information Commissioner. At this stage there is little to report. We are working on the development of publication schemes and await a timetable for the phasing of implementation. This will now be a matter for the Lord Chancellor who took responsibility for data protection and freedom of information policy in June. The significant change is that the UK does now have the two sets of statutory rights and obligations which I said last year I considered to be important if we are to ensure that public bodies give due weight to both the public's right to know and the individual's right to respect for private life. There will be difficult decisions to take at the interface. Those will present challenges for my Office once individual rights under the Freedom of Information Act are in place.

A year of increased volumes of work and many changes has been another challenging one for all the staff. They responded magnificently. Newcomers had to be trained while experienced staff had themselves to learn. The backlogs we had in notification this time last year were quickly dealt with. This year as we have started to deal with assessments some backlogs have arisen there. These are being addressed.

We lost some experienced members of the team. Some went to carry on data protection compliance work from within the organisations of data controllers; others retired. Dr John Woulds was one of those who retired. John joined the Office when it was set up in 1985, he contributed personally to the development of the Office over the years and as Acting Deputy Commissioner took the lead responsibility for the introduction of freedom of information to our portfolio of responsibilities. We shall miss him.

To deal with all the changes confronting us we have been provided with increased funds. These we are using to build up our staff, to introduce new information systems and to consider whether our expansion provides an opportunity to organise ourselves differently.

The build up of staff and responsibilities over the next four years will lead to a very different organisation. The decisions we take in the next few months will largely determine its nature.

A handwritten signature in black ink, appearing to read 'Elizabeth France', with a stylized flourish at the end.

*Elizabeth France*, **Information Commissioner**

## Chapter 1:

# Review of the year



*“ensuring the most  
efficient use of  
our resources”*

Last year's report set out the Office's overarching aims with a list of key objectives for the year.

**In ensuring that our statutory duties are met efficiently and effectively, we aim to position the organisation as one responsive to change and ready to manage risk.**

During the year, a review of the office structure was undertaken in the light of the future freedom of information responsibilities. The proposed new structure will allow us to fold in these additional responsibilities into the current technical core of the organisation. It will provide the flexibility we need to assume these additional responsibilities whilst also ensuring the most efficient use of our resource over the phased implementation of the law.

We have made progress in achieving the transition from the Data Protection Act 1984 (DP Act 1984) to the Data Protection Act 1998 (DP Act 1998). The new notification system is fully operational, and much work has been undertaken in refining this system. We have seen rapid adoption of the Internet based forms, advice and self-assessment guides introduced last year, and expect to continue to improve such services over the forthcoming year.

The new procedures for undertaking assessments under the DP Act 1998 have been implemented and are under continuing review. Early in the year an assessments database was developed to streamline the assessments casework process and provide management information.

During the year a review of some of the operational measures and performance indicators was undertaken. The process of identifying operational performance indicators will now feed into our capital investment project, a



primary output from which will be the development of a management information system.

**We will ensure that policy makers give appropriate weight to individuals' rights.**

We are collaborating with the University of Manchester Institute of Science and Technology on two projects. The first project concerns the development of guidance on data protection in systems design, the second concerns an exploration of human issues in security and privacy in e-commerce.

Our participation in European and international activities directed towards the effective implementation of common privacy protection by legislative or co-regulatory means is described in detail in Chapter 5.

We have offered to organise a further meeting of the EU Data Protection Commissioners' Police Working Party and we continue to contribute to other such working groups.



We have closely followed progress of the Freedom of Information Bill as it has proceeded through Parliament and the Commissioner gave a press briefing on 30 January 2001. A schedule detailing our initial work plan during the next few months has been published and is available on our website.

**We will ensure that those who handle information in the public and private sectors, are aware of their obligations and act accordingly.**

A review of the guidance published by the Office was conducted during the year and a programme of phased revision and publication of the guidance under the DP Act 1998 agreed.

The CCTV code of practice on the use of CCTV in public places was finalised and published in July 2000. Copies of this code are available in hard copy from this office or via the website.

*“participation in  
European and  
international activities”*

*“national television  
advertising campaign”*

The draft code of practice on the use of personal data in employer/employee relationships was put out to consultation early in the year. Our revised plans for publication of the final code are detailed in Chapter 2 of this report.

Our audit manual has been subject to editing and quality review during the year and is now ready for publication.

We held a workshop in collaboration with the University of Manchester Institute of Science and Technology on 9 November 2000 to discuss best practice guidance on data protection for e-commerce system designers. Privacy experts, industry practitioners and a representative of the Dutch data protection authority attended the workshop.

Work on our freedom of information responsibilities included hosting a publication schemes workshop on 13 February which was attended by representatives from a cross-section of public authorities, including: Home Office, Public Record Office, MOD (Ministry of Defence), Health and Safety Executive, Local Government Association, NHS Executive, and the Stationery Office.



**We will ensure that individuals are aware of their rights to information, and feel confident that those rights are respected and can be exercised.**

A national television advertising campaign was implemented during August 2000. More details on the effectiveness of our advertising and communications activity are available in Chapter 4.

The education packs for primary and secondary schools have been finalised and tested. These will be launched to schools on a rolling basis over the coming year.

## Chapter 2:

# Some challenges ahead



We, and the community of data controllers and public authorities we deal with, face many challenges. Most obviously, there are new freedom of information responsibilities but there are also many other factors that impact on us. The political, legal and technical worlds within which we operate are forever changing.

### **Making Modern Government Work**

Sometimes called ‘joined-up government’, sometimes ‘information age government’, sometimes ‘electronic government’ the Government’s vision has several strands. There is a target of delivering 100% of government services electronically by 2005 through mechanisms such as the government portal, call centres, and one-stop shops. In round terms the challenge is simple: to ensure that the system works in the way in which it is supposed to. If it doesn’t citizens will lose confidence and interest. Setting and meeting data protection standards is a key component. We will continue to work with the Office of the e-Envoy and the Cabinet Office more generally to develop these standards. In the area of on-line authentication and identification in particular there is still much work to be done.

In promoting e-government, stress is often laid upon the use of technology to deliver the same services in a smarter way. For instance, over the last year a ‘joined-up’ change of address service has been piloted. In other scenarios the whole point of the deployment of new technology is that it allows different objectives to be achieved through the use of data mining and profiling. Whereas previously benefit claims or tax returns might be sampled for accuracy, today it is possible to check, say, all applications for taxi licences against all applications for benefit, to identify all possible cases of error and to automatically rank cases in order of the likelihood of fraud. Not only does this raise questions as to whether the ‘quality’ of the data is sufficient to support the conclusions that are drawn, it also raises questions about

*“setting and meeting data protection standards is a key component”*

*“making better use of  
personal data need not be  
incompatible with privacy”*

transparency. Is information about how data are to be used and the purposes for which they are disclosed made sufficiently clear to data subjects? Without transparency the necessary public debate about the extent to which it is right that individual conduct should be routinely monitored can never take place.

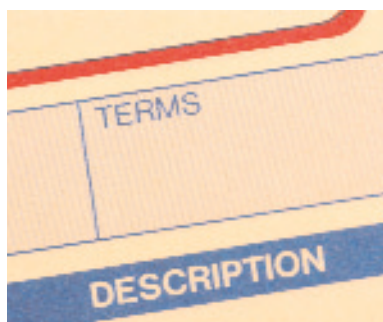
Another strand of the modernising agenda is the use of IT to reconfigure service delivery. For example joint initiatives between Social Services Departments and NHS Trusts depend upon the sharing of information about clients between partners who do not necessarily have the same attitudes towards issues such as confidentiality. One of the ways in which data protection and privacy concerns have been addressed within multi-agency environments has been through the development of local information sharing protocols. In some cases national model protocols have been successfully developed, allowing local agreements to be put in place relatively easily, but this has not always been the case and too often local bodies are struggling to agree standards.

Perhaps the greatest challenge is in grasping the relationship between the different strands of the modernisation agenda. Over the past year the Performance and Innovation Unit (PIU) at the Cabinet Office has been conducting a study into privacy and data sharing across the public sector. The report is due to be published in summer 2001. We welcome the report. It asserts a belief we share that making better use of personal data to deliver public services need not be incompatible with privacy and that enhancing privacy should be a Government objective. Nevertheless, it is clear that there is much to be done if this vision is to be turned into reality.

Recent experience suggests that some parts of the public sector, for instance, the NHS, which has announced a comprehensive strategy for improving the protection of patient data, have a quite different attitude than, say, the DSS whose Fraud Bill proposals (subsequently amended) threatened very significant intrusions into individual privacy. Joined-up government requires a shared concern with privacy across the whole of the public sector. Failure to establish and deliver a common standard can only have adverse consequences for the modernising government agenda.

### **Improving Data Quality**

Any system of data matching that brings together information on individuals from different sources relies heavily on the quality of the data it receives. If names and addresses are not provided accurately and always in the same format the system will not link up information that genuinely relates to one individual. If the system employs ‘fuzzy matching’ to overcome this problem, records that are similar but in fact relate to different individuals will be matched incorrectly. In either case the consequences can be considerable.



With the introduction of the DP Act 1998, those involved in data matching can no longer deny responsibility for the accuracy of the data they receive from third parties.

Data quality has always been a problem with credit reference systems. Alongside the practice of using third party data under which information about family members is automatically linked, poor data quality has been at the root of the majority of complaints we receive. We are pleased that the attention the industry has given to third party data has now borne fruit in terms of proposals for change that will largely answer our concerns. The challenge is now to deliver the same degree of commitment to achieving substantial improvements in data quality. We accept that in some cases this might require some increase in the extent of personal data held, for example, full name rather than just surname and initials. Those we meet regularly recognise the need for improvement but real results rely on action by all those who contribute to the credit reference databases.



*“poor data quality has been at the root of the majority of complaints we receive”*

One area where the consequences of poor data quality are, if anything, even more serious is the Police National Computer (PNC). The Phoenix application contains records of individuals who are arrested and charged with offences together with the details of criminal convictions. There are many millions of existing records and the data they contain are essential to the police and courts. Problems with the accuracy and timeliness of records have been identified in two independent reports. The Association of Chief Police Officers (ACPO) has formulated a welcome compliance strategy to attempt to rectify the identified failings, however, progress towards implementation has been very slow.

The situation is becoming critical due to the establishment of the Criminal Records Bureau (CRB). Later this year this new body is to begin to issue ‘Disclosures’. These amount to criminal convictions certificates and are based on the information contained in the PNC. Many employment decisions will take these ‘Disclosures’ into account. Delays in updating Phoenix records with court results is a particular problem as this can take many months. There is a real risk that details of actual convictions may not appear on certificates and that successful appeals against conviction may not be taken into account. We expressed our concerns to the House of Commons Home Affairs Committee during its study of the arrangements for the operation of the CRB.

### Case Study

#### **CONVICTED: Unlawful disclosure**

A telecoms employee passed information to his friend about a female customer’s telephone account in order to assist that friend with a domestic situation. He was convicted of unlawful disclosure of data.



*“the use of such data where they are a key element of addressing specific criminal activity will be justified provided proper controls are in place”*

Police forces have embarked on urgent work to attempt to rectify matters and Her Majesty’s Inspectorate of Constabulary has formulated a review methodology to assess progress. The challenge is whether sufficient progress can be made to enable the CRB to issue ‘Disclosures’ as planned without a substantial risk of contravention of the DP Act 1998. We are keeping this matter under close scrutiny.

## Responding to Cybercrime

Developments in communications, particularly the Internet and mobile phones, have provided new opportunities for criminals. The new media can be an integral part of the criminal activity, as is the case with the distribution of child pornography on the Internet, or merely a means of communication through which unrelated criminal activity is facilitated. Not surprisingly law enforcement agencies want the ability to access these communications. The challenge is to ensure that such access is limited to cases where the need to prevent or detect crime or safeguard national security justifies the privacy intrusion.

In some cases the new media provide new opportunities for surveillance. One example is the use of the increasingly precise location data generated by mobile phones to track individuals’ movements. The use of such data where they are a key element of addressing specific criminal activity will be justified provided proper controls are in place. However, the temptation to use them as a more general resource to spot, and require individuals to account for, apparently suspicious patterns of activity should be resisted.

In other cases the new media mean that existing opportunities for surveillance may be lost. An example is the move to carry voice messages over the internet



rather than through traditional telephone systems which may render conventional ‘telephone tapping’ techniques obsolete. Here there is a temptation to generate and store personal information solely on the basis that it might come in useful for law enforcement purposes. Again, we must ensure that the measures in place are a proportionate response to the problem the law enforcement agencies face, that as far as possible information is only generated and stored on those under suspicion and that existing safeguards are strengthened not weakened. It is, for example, hard to see the case for imposing a requirement on telecommunications providers to retain all traffic data for a period of seven years as has been suggested in some quarters.

Cybercrime does not recognise national borders. There are several international initiatives to develop cooperation between countries including a draft convention from the Council of Europe and work undertaken by the G8 group of countries. We are concerned that the international organisations involved, not least the Council of Europe with its human rights pedigree, and the UK’s negotiators should give proper weight to privacy and data protection considerations. International cooperation inevitably involves the exchange of personal information. In the UK, the EU and in an increasing number of countries throughout the rest of the world this personal information is protected by data protection law. It is essential that if other countries wish to be party to the exchange of personal information in the context of tackling cybercrime they should accept obligations to handle the personal data they receive in accordance with recognised data protection standards.

### **Delivering our Employment Code**

The issue of interception of communications also featured in our draft code of practice on the use of personal data in employer/employee relationships. The draft code was published for consultation in October 2000 and elicited an unexpectedly large and detailed response. It was developed partly to meet demands for comprehensive and authoritative guidance on the application of the DP Act 1998 to employment but has been criticised by some for being overly long and complex. We are reluctant to scrap substantial areas of advice which many find valuable but intend to recognise the concerns expressed by publishing the final version in several distinct parts. We are also seeking expert assistance in the final drafting to ensure the code is as accessible as possible to its primary audience of human resources managers. The code itself will be supported by summaries of key points for particular target groups such as smaller businesses.

Several challenges have arisen in the course of our work on the code. The DP Act 1998 requires that personal data are processed fairly. Employment decisions increasingly involve the processing of personal data particularly given the

### **Case Study**

#### **CONVICTED: Unregistered data user/controller**

An employee appropriated client data from his employer’s database then left that firm and established his own company. The appropriated data was retained on computer. He was convicted of unlawfully using the data for his own purposes and his new business convicted of being an unregistered data user.

*“International cooperation  
inevitably involves  
the exchange of  
personal information”*

*“Monitoring of employees, in particular their emails and Internet access, has drawn much comment, not least from the media”*



wider definitions of both “personal data” and “processing” introduced by the DP Act 1998. Can the DP Act impose, for example, an obligation on an employer to make recruitment decisions that are “fair” to applicants, to an extent that goes beyond the restrictions on specific types of discrimination that already exist in law? Should it do so? If so, how is “fairness” determined?

One issue that has attracted particular attention is the keeping of sickness records. Those necessarily involve the processing of “sensitive” personal data. The circumstances in which such data can be processed without an individual’s explicit consent are limited by the DP Act 1998, which reflects the terms of the EU Data Protection Directive 95/46/EC. Although we do not question the need for employers to keep reasonable sickness records and we recognise that obtaining explicit consent may be unrealistic, we are not in a position to rewrite the Act. We can only advise on its interpretation.

Monitoring of employees, in particular their emails and Internet access, has drawn much comment, not least from the media. The fact that such activity falls within the scope of the DP Act 1998 is inescapable. Any monitoring must therefore address the specific risks that an employer faces, it must be a proportionate response to those risks, it must be conducted with no more intrusion than necessary and employers must be open with their employees about its existence. Our challenge is to translate these high level requirements into standards that are realistic and can be readily understood and put into practice by employers. It is with this in mind that we held a one-day conference on the issue of employee monitoring at the end of June 2001.

### **Promoting Publication Schemes**

The Freedom of Information Act 2000 (FOI Act) is expected to be implemented in stages across the public sector from 2002 to 2005. The public will have the right to access information held by all public bodies. We will be issuing guidance and working with public authorities to help them understand and meet their new obligations. There is clearly a challenge in ensuring that all bodies are ready to comply when their time comes.

We see publication schemes as a vital part of this process. They must set out:

- the classes of information an authority publishes;
- the manner in which the information is published; and
- details of any charges.

Developing publication schemes will require public authorities to decide, in advance of individual requests, what information they will routinely make available to the public and how. Provided they are comprehensive and easy to use, publication schemes will reduce the day-to-day administrative burden of

responding to individual requests. We hope that publication schemes will encourage public authorities to release information automatically and to make disclosure a natural part of their working routine. They should also stimulate good government as authorities become aware of the need to ensure that their procedures are ready for the scrutiny that FOI makes possible.

We have already drafted criteria for the approval of publication schemes, guidance and details of our own scheme. Later this year we shall be consulting as widely as possible to ensure that bodies affected by the FOI Act have the opportunity to contribute to our policy development. Meanwhile, a selection of



public bodies will be conducting pilot schemes and reporting back to us on their progress. We will be holding a seminar in July where a range of authorities will be able to discuss with our staff and with each other the implications of complying with the FOI Act and operating a publication scheme.

We want the development of publication schemes to encourage public authorities to remove barriers to access to information. Operating a formal system of information access, and helping the public to discover more about the way the public sector works is a vital step in creating the culture of openness across government, local authorities and other public bodies that will be an essential ingredient of FOI Act compliance.

## Managing Change

The impact of the FOI Act 2000 on us is huge. Although the Data Protection Commissioner has simply been renamed “Information Commissioner” and our office and staff continue, we are in many ways a new organisation. Over the next four to five years we expect to more than double in size. This is at a time when we are losing staff whose skills are in demand in the private sector. Recruitment has already become a continuous process. We will need to develop our structures and procedures to cope. Some of the informal arrangements that have served us well up to now will no longer be adequate. We may have to find new accommodation. To achieve this transition when at the same time we are facing additional demands, albeit welcome ones, because of the recognition that privacy and data protection are now receiving is no small challenge.

We also have £5m to spend on our IT infrastructure over a two-year period. This is undoubtedly a position many organisations would like to be in. It will enable us not only to develop new systems to help us deliver our FOI

## Case Study

### **BREACH:** **Unfair processing** **(1st DP principle)**

An individual placed, by telephone, an advertisement in a regional newspaper, but was surprised to discover later that the newspaper had undertaken a search with a credit reference agency.

The newspaper explained that it was usual policy to run a credit check on all non-prepaid advertising customers, and that a notification was given to these customers beforehand. In particular, it was explained that a notification is read to customers placing advertisements by telephone.

The newspaper accepted, however, that on this occasion, the member of staff who took the order did not follow the correct procedure, and the credit check was undertaken without the customer receiving prior notification.

#### **OUTCOME:**

Unfair processing, breach of the First Data Protection Principle. As a result, the newspaper removed the record of the search from the credit reference file.

responsibilities effectively but also to update or replace our existing systems with knock-on benefits on the data protection side. In doing so we will look to meet our commitments under the “Modernising Government” initiative to deliver services electronically. We now have to work hard to ensure the money available to us is spent as effectively as possible in the relatively short time scale available for an investment of this size. A starting point has been the appointment of a Change Programme Manager.

At the same time we have to respond to changes in the legal and political framework within which we operate. One aspect of this is devolved government. Towards the end of the year work began on a short-term project to consider the implications of the new constitutional arrangements. The project report will include initial recommendations as to whether an office presence should be established in each of Scotland, Northern Ireland and Wales. The scope of the FOI Act and the DP Act 1998 differ. Data protection is a reserved matter; the legislation applies in England, Scotland, Northern Ireland and Wales. Freedom of information is not similarly reserved. A draft Bill to establish a freedom of information regime for devolved Scotland has been published by the Scottish Executive. One issue that we need to address is the interface between the Scottish and UK freedom of information regimes and the need for effective liaison with the Scottish Information Commissioner. We await the project report with interest. Although our office has to grow, all the growth does not necessarily have to take place in Wilmslow.

On the legislative side the Human Rights Act 1998 which came into force in October 2000 is important to us. Not only does it contribute significantly to the framework within which we have to interpret and apply the DP Act 1998 and, to a lesser extent, the FOI Act, it also affects how we, as a public body, deal with those who approach us and those we regulate. All our staff have received training on the impact of the Human Rights Act. We now have to ensure that we keep track of the developing case law and respond appropriately.

Lastly we have, of course, to apply the freedom of information legislation to our own activities. We need to lead the way but are hindered by Section 59 of the DP Act 1998 which imposes inappropriate restrictions on our ability to disclose information about our activities. We have consulted widely on how far the outside world believes we should go and this will inform our publication scheme. Like others we will undoubtedly have to change our practices to meet our new obligations.



## Chapter 3:

# Implementation



Our compliance advice this year has covered a wide range of data controllers. Indeed, one of the lessons of the first full year of implementation of the DP Act 1998 has been the recognition that the changes in definitions which the Act gives us, increase its scope in ways which may not have been immediately apparent. The extension of the definition of 'data' to cover some manual records; the fact that a data controller is defined as a person who determines the purpose and manner of processing (itself now broadly defined) and the definition of personal data have a combined effect that distinguishes the DP Act 1998 clearly from its predecessor. Some of our time during the year has been spent in internal discussion on the interpretation of these and other key terms in the Act. This will lead to the publication this year of further legal guidance aimed at providing a common understanding of the way we interpret the DP Act 1998 for the benefit of those seeking to comply.

Such guidance is a helpful foundation but does not always provide the handbook to compliance which many data controllers look for. Codes of practice are intended to provide more detailed advice. The CCTV code of practice referred to in last year's report, has been widely welcomed. The code we are producing on the use of employee data has already been referred to in Chapter 2. Codes of practice do not add to the regulatory burden, nor go beyond the requirements of the law already in place. Their aim is further to explain the interpretation which this Office (as regulator) is taking of the requirements of the DP Act 1998.

Where industry bodies or other umbrella organisations are willing to produce guidance on how the Act applies in their area, this can be very helpful. We have commented on a number of such guides this year. For example, the Direct Marketing Association launched a guide on the DP Act in March; the British Bankers Association, Association of British Insurers, Finance and Leasing Association, Association of Unit Trusts and Investment Funds, Consumer Credit

*“Where industry bodies or other umbrella organisations are willing to produce guidance on how the Act applies in their area, this can be very helpful.”*



Trade Association and Council of Mortgage Lenders worked together on a guide for the finance sector. Other general guidance on which we provided comments includes that produced by the Factors and Discounters Association, the Chief and Chief Fire Officers Association (CACFOA), the Church of England, the Office of National Statistics and the General Medical Council.

We have commented more specifically on proposed notifications, designed to satisfy the transparency requirements with the first data protection principle, which have been submitted to us.

We have provided advice for pupils and parents on access to pupil records; to those involved in alumni fund raising; to local government elected representatives and to political parties. We are in the process of developing guidance for members of the public on how to exercise their rights under the DP Act 1998.

### *Case Study*

#### **CONVICTED: Unlawful procurement**

A bank employee abused her employer's on-line credit checking facilities by conducting a credit search that had nothing to do with her employment but had everything to do with her domestic situation. She was convicted of unlawfully procuring information from the credit reference agency.

We have contributed comments to assist the work of the Human Genetics Commission; the Parliamentary Science and Technology Committee; the Task Force on Overindebtedness; an Economic and Social Research Council research project on social responsibility in the information age; and the Cabinet Office Performance and Innovation Unit's (PIU) work on privacy and data sharing.

The PIU project has involved significant input. We seconded an Assistant Commissioner to work with the team on a part-time basis and the Commissioner was a member of the Advisory Board. The project looks at the drivers for data sharing, both to achieve efficiencies and to prevent fraud while recognising the importance of protecting the citizen's right to private life. Its recommendations addressed to public authorities, have the potential to

achieve a common framework for addressing these policy objectives. In relation to fraud prevention we have addressed the issue of balance on other occasions during the year. We are talking to CIFAS (a fraud avoidance scheme) about the need to review their roles in the context of the altered legislative and cultural environment brought about by changes to the DP Act 1998, the introduction of the Human Rights Act, and changed consumer expectations about the way their data will be handled. Most significantly, we offered comments on the draft Government Bill to deal with Benefit Fraud, and were pleased to see those comments taken into account by way of Government amendment during the passage of the Social Security Fraud Act 2001.

We are concerned that there continues to be increasing pressure for the wider forensic use of genetic information in the form of DNA profiles. The new Criminal Justice and Police Act contains provisions which expand the circumstances where such profiles may be retained. We continue to remain concerned about such developments.

## Enforcement Action

Formal enforcement action was taken against two companies, Second Telecom Limited and Top 20 Limited, in relation to contraventions of the Telecommunications (Data Protection and Privacy) Regulations 1999 (the “Telecoms Regulations”) in respect of the sending of unsolicited direct marketing faxes. The Enforcement Notices served upon these companies were concerned with their compliance with regulations 23 and 24 of the Telecoms Regulations. Both companies appealed against the Notices.

Regulation 23 prohibits the sending of unsolicited direct marketing material by fax to individual or corporate subscribers who have objected either specifically to the sender in question (regulation 23(2)(a)) or generally by registering with the Fax Preference Service (FPS) (regulation 23(2)(b)). Regulation 24 prohibits the sending of direct marketing material by fax to individual subscribers without their prior consent.

The enforcement action was based on numerous complaints received by the Commissioner. As at the date of both Notices (25 May 2000) we had received around 90 complaints per company. In addition, the Commissioner was mindful of reports received by her on a bi-monthly basis from FPS indicating numerous breaches of regulation 23(2)(b) by both companies.

Both companies were part of the same “group” of companies sharing the same trading address as well as having directors in common. It also emerged that both companies used the same database to conduct their activities. When the matter first came before the Data Protection Tribunal for a directions hearing

## Case Study

### CONVICTED: Unlawful procurement

In two quite separate cases information was obtained from the DVLA, by deception, concerning the registered keepers of motor vehicles. All were convicted of unlawfully procuring information from the DVLA.

## Case Study

### **BREACH:**

#### **Unfair processing (1st DP principle)**

#### **Inadequate, irrelevant and excessive (3rd DP principle)**

#### **Inaccurate (4th DP Principle)**

A complainant applied for a current account and a mortgage with a leading bank. Although the mortgage was granted the current account was declined. The bank advised the complainant that he should resubmit his application for the current account when his mortgage had been arranged, as preference was given to people with mortgages. Unfortunately, at the time he did so the complainant had moved to the new house so the address details on the application form were incorrect.

The bank also conducted three credit reference checks, on two occasions using different periods for length of time at address. A fraud prevention database spotted this anomaly and the file was passed to a fraud investigator. Several procedural errors then took place, the outcome of which was the addition of a marker indicating possible fraud which was shown when a credit reference check was made.

*Case Study-continued on page 23*

(to set a timetable for preparations for the substantive hearing of the appeals) the Deputy Chairman of the Tribunal ordered that the two appeals be consolidated and heard together in the circumstances.

Whilst preparations for the substantive Tribunal hearing continued, parallel discussions and negotiations between the Commissioner and the companies took place on a without prejudice basis, including a visit by the Commissioner's representatives to the companies' premises. These discussions ultimately proved fruitful and an agreement was reached that averted the substantive contested appeal hearing taking place.

Both companies agreed to submit to Enforcement Notices effectively requiring them to comply with regulation 23. Such Notices (the "regulation 23 notices") were ratified by the Tribunal on 20 November 2000. Prior to that further Enforcement Notices (the "regulation 24 notices") had been served upon both companies requiring them to take specified steps in an effort to achieve a satisfactory level of compliance with regulation 24. The terms of the

regulation 24 notices had been agreed between the Commissioner and the companies and were noted by the Tribunal in its decision dated 20 November 2000 as well as in the certificate issued by the Tribunal pursuant to the requirements of rule 20 of the Data Protection Tribunal (Enforcement Appeals) Rules 2000 (S.I. 2000 No. 189). That certificate, together with the decision, the statement of the Commissioner containing the material findings of fact relating to the appeals, and the regulation 24 notices served on each of the companies can all be found on our website.

Since the notices came into force against the companies, the Commissioner has been monitoring each of their compliance with the respective requirements of the notices. The Commissioner is not yet in a position to judge whether, or to what extent, the regulation 24 notices have achieved, or are likely to achieve, a level of compliance with regulation 24 that is satisfactory to her.

The Commissioner continues to monitor the compliance of these and a number of other companies with regulations 23 and 24 of the Telecoms Regulations. Preliminary Enforcement Notices were served on three other companies in the



year. The Commissioner will continue her efforts to achieve compliance by these and other companies without resorting to formal action. However, should such efforts prove unsuccessful she will consider taking such action.

### Other Enforcement Work

There has been no other formal enforcement action taken by the Commissioner. A preliminary notice was served upon a data controller in the public sector resulting in them providing an undertaking to the Commissioner that addressed the compliance issue in question to her satisfaction. In the circumstances of the particular case the Commissioner did not consider it necessary to proceed to formal enforcement action.

### National Security Appeals

Section 28 of the DP Act 1998 provides an exemption from a number of provisions of the Act if exemption from any such provision is required for the purpose of safeguarding national security. Such an exemption is in effect asserted by means of certificates, signed by a Minister of the Crown, certifying that exemption from all or any of the provisions is or was required for the requisite purpose. Such a certificate is conclusive evidence of that fact. However, any person directly affected by the issuing of such a certificate may appeal to the Data Protection Tribunal against the certificate.

The Tribunal is specially constituted to hear such appeals and is subject to different rules than in the case of appeals against enforcement and information notices (namely the Data Protection Tribunal (National Security Appeals) Rules 2000 (S.I. 2000 No. 206)). The first appeal to be heard by this Tribunal is expected to take place at the end of June this year. As it is the first appeal the parties consented to the proceedings taking place in public (subject to certain

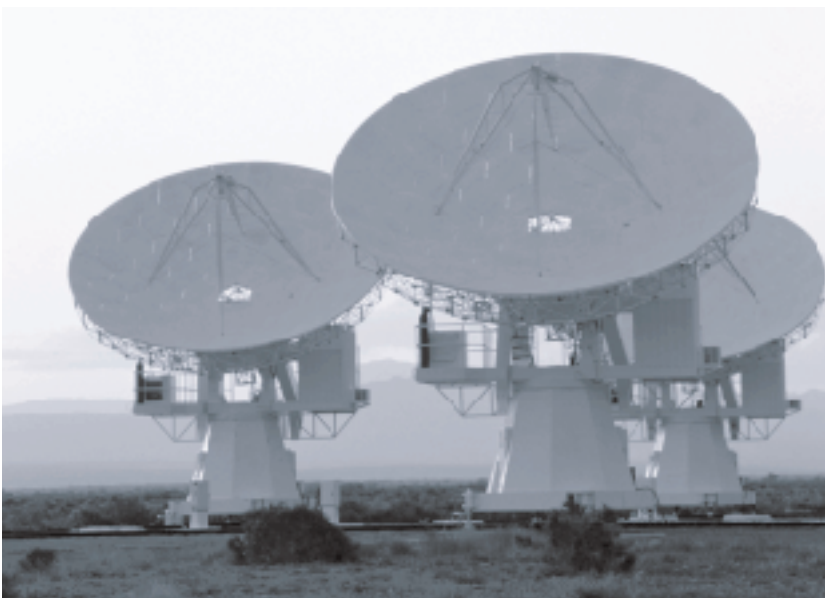
#### *Case Study-continued from page 22*

The complainant worked within the financial services sector.

It was his belief that this marker prevented him obtaining employment within this field, as finance houses are unwilling to employ someone whose probity is in any doubt.

#### *Outcome:*

The assessment was made that this processing breached the first, third and fourth data protection principles. A review of all the relevant procedures, plus additional data protection training for staff at branch level was required.





## Case Study

### OUTCOME:

#### **Bank to review and alter application procedures and undertake systems-development work.**

An on-line Bank introduced a range of investment products. The on-line application process, however, required the completion of several mandatory fields requesting information that was often not relevant to the purchase of the product in question. Such information appeared to be solely for the purpose of identifying future marketing opportunities.

### OUTCOME:

Since the Act gives individuals the right not to have their personal data processed for direct marketing purposes, this raised the question whether it was fair to obtain information in this way, and whether any information so gathered could be excessive for the purpose of purchasing an investment product, in breach of the third data protection principle.

It was recommended to the Bank that the application procedure should be amended: either to remove the irrelevant questions, or to make them optional with an appropriate explanation. Providers of services or products over the Internet must provide an on-line means for the individual to object to the use of their personal data for direct marketing

*Case Study-continued on page 25*

restrictions to protect the identity of certain witnesses). At the time of writing this report the result of the appeal was not known.

At a directions hearing at the end of April 2001, the Tribunal ordered that the Commissioner be allowed to give evidence to the Tribunal to assist it in its determination. The Commissioner's evidence will seek to place the provisions of section 28 of the Act in the wider context of data protection law and practice from the perspective of the Commissioner and in light of her role and statutory functions.

The Commissioner's limited involvement in these proceedings was largely precipitated by the fact that this is the first appeal to be considered by this Tribunal. The Commissioner does not envisage involving herself to the same degree, or even at all, in relation to any appeals subsequent to the present one. The rules governing these appeals provide for the Commissioner to be served with copies of the parties' formal notices in the appeal. The Commissioner will consider the issues arising out of each appeal and may consider applying to the Tribunal to be involved in a similar capacity should any future appeal raise issues not previously dealt with by the Tribunal and with which she considers she can assist the Tribunal. The further involvement of the Commissioner in such circumstances will then depend upon the Tribunal.



## Utilities

In the utility area, the revised enforcement notice (the "Midlands Notice") settled and approved by the Data Protection Tribunal on 20 July 1999 in the case of Midlands Electricity plc v The Data Protection Registrar and referred to in last year's Annual Report, came into force on 1 January 2001 as did the



*Case Study-continued from page 24*

purposes. The Bank agreed to undertake systems-development work, to ensure that any information gathered during the purchase of a specific product would be relevant for that purpose.

undertaking on comparable terms entered into by London Electricity plc on 11 January 2000. The Commissioner is determined to ensure that the obligations imposed on those utility companies upon whom notices and undertakings are effective are also met by those utility companies not currently subject to a notice or undertaking.

We wrote to all the energy utility companies on 8 February 2001 requesting copies of bill inserts sent to those customers who have not informed such companies that they agree to the receipt from them of marketing material. We shall continue to monitor compliance by all companies in the sector and, if necessary, use enforcement powers where that appears the most effective way to achieve compliance.

We wrote to all the public water undertakers on 10 July 2000 to remind them of their obligations in light of the Tribunal cases and the undertakings in the utility sector in relation to the fair processing of supply customer data. In this respect we were able to refer to the undertaking entered into by Thames Water Utilities Limited on 6 January 2000 which, like the London Electricity plc undertaking, was also on comparable terms to those contained in the Midlands Notice but suitably adapted to relate to the provision of water supply, sewerage, drainage and sewage disposal services. We continue to monitor compliance in this area.

## The BAIRD Project

August 2000 saw the commencement of a joint initiative between the Department of Social Security, the Inland Revenue and the Data Protection Commissioner (using her powers under the DP Act 1998) to clamp down on those people and organisations who unlawfully and systematically obtain, or seek to obtain, people's personal details and who then pass these on to interested clients at a price. Investigators from the other two organisations are seconded to the Commissioner for the purposes of this project.



The initiative is making good progress and a number of organisations have already come under close scrutiny. The successful bid in 'Invest to Save Round 3' has enabled the project to continue for another year.

## Chapter 4:

# Investing in education and awareness



### Identifying Needs

In April each year we conduct our annual tracking studies to identify levels and trends in awareness of individual rights and responsibilities amongst data controllers and data users. These annual studies are conducted to provide us with an indication of the effectiveness of our communications and of equal value, an indication of how we can refine our communications strategies to better meet the needs of our public.

This year both these studies were revised to incorporate questions on attitudes towards, and awareness of, the freedom of information legislation. It was recognised that awareness of the details of this legislation would be relatively low at this early stage, but we felt it important to establish baseline figures so that the effectiveness of our activities over the coming years can be monitored.

Brief summaries of the key findings from this year's tracking studies are available on our website.

### Raising Awareness

We had promised to undertake an awareness generating advertising campaign following the introduction of the new data protection law last year. The campaign was targeted at individuals with the primary aims to increase awareness of the law, specifically individual rights, and to provide a call to action to give individuals more detailed information on their rights should they require it.

The campaign included a television advertisement and leaflet issue and ran for a period of three weeks in August 2000.

Although a significant part of the Office budget, a spend of £400,000 is relatively low in the context of a national advertising budget. By undertaking

*“our own tracking research  
has indicated a 93%  
increase in awareness  
of rights”*

## Case Study

### Outcome: Bank to ensure that all staff are aware of their responsibilities under the DP Act.

A customer entered a branch of a Bank to conduct a particular business transaction. As part of the procedure, the customer was required to give some personal details.

The customer later received an anonymous telephone call, which contained a specific accusation. The customer deduced that the caller must have been associated with the branch of the Bank visited earlier, as the personal details given at the time were the only likely source of the information used to make the call.

The customer returned to the Bank to seek an explanation. There, it was claimed that branch-management sanctioned the use of the personal data, previously given in confidence, to make the call.

#### OUTCOME:

There was no justification for the use made of the data.

The Bank accepted that the actions at branch-level were regrettable, and acknowledged that this use of a customer's personal data was outside the purpose for which it had been obtained. This matter thus had implications relating to the

*Case Study-continued on page 29*

the campaign in August 2000, we achieved the best value for money in terms of both coverage and the number of opportunities for each individual to see the adverts. The channel mix, using GMTV, Channel 4, Channel 5, HTV, ITV and a number of appropriate satellite channels, proved most effective in terms of coverage. A media schedule was posted on our website during the period of the campaign.

We were particularly pleased with the awareness levels generated from the campaign. Our own tracking research has indicated a 93% increase in awareness of rights amongst individuals over the year and an independent study undertaken following the second week of the campaign ranked the television advertisement amongst the top twenty television advertisements recalled across all adults within the UK, with 19% of respondents stating that they had recently seen the advertisement.

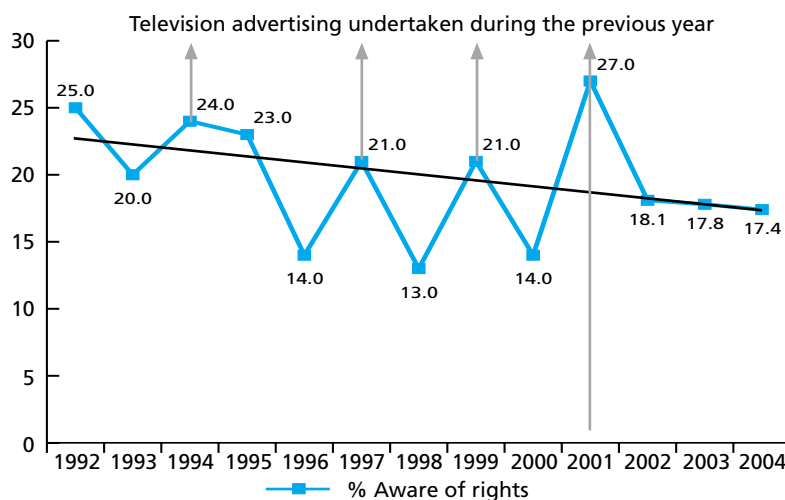
The television advertising was supplemented by a poster campaign on the Underground in London to ensure a balanced coverage.

Awareness amongst data controllers also increased during the year with awareness of individual rights amongst large organisations and small organisation increasing by 10% and 9% respectively.

## Monitoring Effectiveness

In the past we have used awareness of individual rights as a key performance indicator of our communications activity. An analysis of awareness of rights amongst data subjects over the years suggests that awareness correlates positively with the value of our spend on paid for communications as illustrated.

### Awareness of rights amongst data subjects (%)

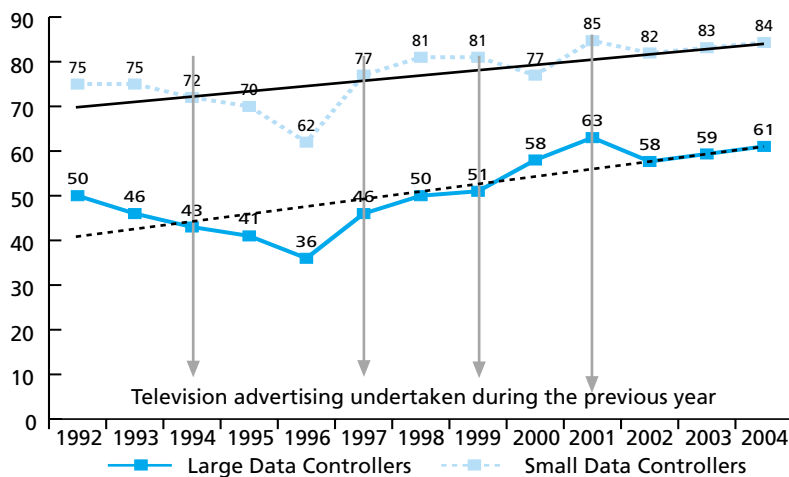




The most recent figure for data subject awareness suggests that the significant spend on advertising activity during the last year has proved effective. What is apparent, however, is that following such activity, awareness levels have tended to drop rapidly in the absence of advertising activity. This suggests that our longer term communications strategy should include greater provision for maintaining awareness levels during the period between high spend campaigns or that we should spread the activity over the years to combat what appears to be an underlying downward trend in awareness.

An analysis of data controller awareness over the years suggests that there is also a positive correlation between advertising spend and awareness, although to a lesser degree than with data subjects. Awareness of rights amongst data controllers does not appear to drop off to the same extent following high spend activity, suggesting that the continued investment in ongoing educational activity is relatively effective and should be continued.

#### Data controllers awareness of individual rights (%)



In an attempt to further understand the relationships between the amount of activity and understanding of the legislation amongst our targets, we have now introduced a further monitoring mechanism: taking the form of two questions on a larger omnibus study which can be undertaken on a monthly basis throughout the year.

This additional study provides us with the flexibility to quickly gauge awareness levels following campaigns and other activity in such a way that comparisons can be made, before and after activity and with the broader findings of the existing studies. This should particularly benefit us as we begin to make decisions on investment in communications activity regarding freedom of information.

#### Case Study-continued from page 28

security of the personal data provided, and also to whether the data were being processed both fairly and for purposes specified to the customer.

The Bank was advised to take steps to ensure that all staff are aware of their responsibilities under the DP Act 1998, and to ensure that they act accordingly.

## Case Study

### **BREACH: Unfair processing (1st DP principle)**

A police force disclosed information about a victim of crime to a voluntary organisation providing counselling services to victims. The victim complained that this contravened the Act as he did not want his details to be disclosed to a third party unconnected with the investigation of the crime. The police force accepted that this was an error on their part and agreed to review procedures to ensure victims' wishes are respected

## **A Corporate Change**

Last year we introduced a new identity following the introduction of the DP Act 1998 and to reflect the change in name from Data Protection Registrar to Data Protection Commissioner. This year we experienced a further change in corporate identity following the introduction of the FOI Act and the change in name to Information Commissioner. Having foreseen this likely change in title, the data protection brand introduced last year has been kept, but revised to sit alongside a new brand for freedom of information and a new umbrella identity for the Information Commissioner's Office. This new identity incorporates many of the features introduced during the previous year, including the specifications for type size, font and layout to ensure accessibility.

As with most corporate changes like this, we expect it to take time for awareness of the new identity to reach the levels achieved with the previous identity. Our primary concern regarding awareness generation however is to ensure that individuals are aware of their rights and to ensure that organisations have the knowledge to comply with the legislation we are responsible for implementing.

## **Investing in Knowledge**

This year, work continued in developing a schools pack for children at primary and secondary schools. The CD-ROM based packs have been market tested amongst children and teachers and will be launched into schools over the coming year.

The on-line training seminars reported on in last year's report have taken longer than expected to develop, but should be available via our website later this year.

## **Working with the Media**

We have continued to invest in supporting media journalists and editors in covering data protection and freedom of information issues over the year.

We received a great deal of positive feedback on the media briefing issued when the DP Act 1998 was implemented. We therefore produced and issued a similar media briefing pack on the FOI Act to members of the press in January.

As part of the launch of last year's annual report, we set up a separate website to host an on-line press briefing, involving live questions and answers, a webcast of the Commissioner's speech and background information. This replaced the usual press conference held in London each year.



Media interest remains very high. Throughout the year we have produced 14 press releases and our staff have been involved in over 530 public media interviews leading to seven television and 15 radio appearances.

### **Empowering Individuals – The Information Padlock**

The Information Padlock introduced at the end of last year continues to be adopted by a diverse range of data controllers. The symbol was introduced to encourage data controllers to be open about their use of personal data and to provide a reminder to individuals that they have rights regarding the processing of their information. The symbol and advice on its use are available to data controllers via our website.



### **Case Study**

#### **BREACH: Inaccurate data (4th DP principle)**

A police force mistakenly attributed another person's record to an individual undergoing an employment vetting check. The individual complained that this breached the DP Act. The police force agreed to modify its procedures to prevent a recurrence and made an ex-gratia payment to the individual.

## Chapter 5:

# International and European work



*“a model contract being developed by the European Commission to permit personal data flows to countries with inadequate protection”*

The involvement of the office in international and European work grows ever greater. Much of it has become routine operational activity and not just the attendance at infrequent conferences by the Commissioner and her senior staff. A good example is the development over the last year of six monthly workshops for the staff of EU Data Protection Commissioners on the handling of complaints. That has now led to the development of a special web-site for the exchange of information between authorities on complaints with a cross-border element.

### European Work

Our principal European activity has been participation in the Working Party of Data Protection Commissioners established under Article 29 of EU Data Protection Directive 95/46/EC. These meetings over the last year have concentrated on transborder data flow problems especially on the difficult issue of the ‘safe harbor’ agreement between the EU and the US to permit the flow of personal data from the EU to the US. The negotiations proved most protracted, especially on the issue of whether complaints by individuals should be resolved in the US or by a determination of EU authorities. A second sensitive point was the extent to which EU authorities should retain powers to prohibit data flows to companies within the ‘safe harbor’. The arrangement was adopted by the European Commission on 26 July 2000 and came into effect last November. We have not yet had to address any difficult issues arising from the scheme in practice. At the same time, the European Commission approved Switzerland and Hungary as having adequate data protection on the basis of their general laws. More recently in this area the Working Party has turned its attention to a model contract being developed by the European Commission to permit personal data flows to countries with inadequate protection. Even though the Working Party’s agenda was dominated by transborder data flow issues it did manage to address other matters. Particularly valuable was the Working Party’s adoption of a lengthy

report from its Internet Task Force on data protection on the internet. Also of great importance was an opinion on the routine retention of traffic data for policing purposes, an issue referred to later.

## Europol, the Customs Information System and Schengen

Another aspect of the growing European work relates to policing and related matters ('third pillar' issues). To supervise the work of the European Police Office in The Hague which carries out crime analysis projects related to organised international crime, the Europol Convention established a data protection Joint Supervisory Body (JSB). The JSB now meets quarterly and has adopted a systematic programme of work including the auditing of Europol. The first audit inspection has been carried out and our office took an active part in the work. This is innovative for us, because unlike many of our colleague authorities we do not have a significant statutory audit function.

The UK has now agreed to join the Schengen arrangements for the sharing of police data and we now attend the Schengen Data Protection Common Control Authority as observers. The Customs Information System has come into force, but the special data protection body has not yet been able to meet.

One of the most valuable initiatives in relation to these three bodies (JSB, Schengen Information System Common Control Authority, and Customs



Information System Joint Supervisory Authority) has been the agreement to establish a single secretariat. An independently recruited Secretary with data protection experience will work within the support arrangements of the Secretariat of the Council of the European Union. A competition has been conducted and the first permanent Secretary will be a well-respected colleague from the Dutch data protection authority.

## Case Study

### **BREACH:** **Unfair processing** **(1st DP principle)**

### **Inaccurate data** **(4th DP Principle)**

A complaint was received from a woman who had recently left the employment of a local authority Social Service Department. There were some outstanding administrative issues surrounding her departure. The Council intended to make a note to this effect on one of their systems. Unfortunately, through a clerical error her name was instead entered onto a list of the Department's clients. This database was accessible by a number of the complainant's ex-colleagues one of whom brought this to her attention.

### *OUTCOME:*

The case raised issues of accuracy of personal data, and fair processing in that at the time the Council had no procedure in place to notify data subjects that they were to be included on such a register. Action has been taken to rectify this by the council.



## Case Study

### **BREACH: Unsecured data (7th DP principle)**

A council employee sent into the Office a large amount of employee personnel information found in a black bin liner in a skip at the council depot where he is employed. He alleged that the manager of the depot disposed of the personnel files of employees working at the depot by placing them in black bin liners and thence into skips to be transported to a public refuse tip. He said that two additional bags containing similar information had also been found.

The retrieved documents contained a large amount of personal data relating to the employees and their relatives – pay and financial details, leave applications, medical information relating to sick leave and so on.

Virtually all the documents retrieved were copies of manual documents, which did not come under the scope of the DP Act 1998.

However there was one document, a sickness record relating to the complainant, which appeared to have been computer generated. On this basis we notified the council concerned that we had formed the view that there had been a contravention of the seventh Data Protection principle in this case.

*Case Study-continued on page 35*

## European Codes of Practice and Standards

For some time, we have actively supported those who call for an approach to the implementation of data protection law and EU Data Protection Directive 95/46/EC in particular which integrates formal law and self-regulation. Industry lead efforts: standards and codes of practice can be the most practical means of implementing principles declared in the law. A number of bodies have come forward with codes of practice, for example, FEDMA (Federation of European Direct Marketing Associations), in relation to direct marketing, and particularly ICX (International Commerce Exchange) which has prepared a comprehensive code from the point of view of European based multi-national companies which wish to follow a single system of good practice throughout their international operations.

Pursuing the integrated approach the European Commission issued a mandate to the European Standards bodies, CEN (European Committee for Standardization), CENELEC (European Committee for Electrotechnical Standardization) and ETSI (European Privacy Standardization Initiative). CEN has taken up the work and established a project to examine what rôle standards activity might play in securing the implementation of the data protection directives. We take part in the Project Steering Group. Notwithstanding the fears of some that this work will result in an expensive and unwanted type of quality standard, we believe that data protection is best achieved if those who have to comply with the law own the problem and generate widely accepted good practice solutions, whether they be of a technical or managerial nature.



## Other European Issues

Many of the issues of data protection concern in the UK are reflected in discussions at the European level. Notable are the adoption of the European directive on electronic commerce, the review of the telecommunications data protection directive with its proposal for opt-in to e-mail marketing, emerging discussions about data protection and employment, and concerns about the special nature of genetic data and its consequences for personal privacy. This latter issue and the announcement of the first sequencing of the human genome prompted the Article 29 Working Party to adopt the following opinion:

The completion of a first draft of the DNA blueprint has been recently announced by those involved in the Human Genome Project.

“The Working Party recognises that this achievement of long lasting significance may permit the diagnosis and treatment of diseases in a manner previously unimaginable.

At the public presentation on 26 June it was recognised that the risks of abuse of genetic knowledge raise legitimate concerns about the privacy of individuals. The Working Party shares these concerns. The decoding of the DNA blueprint paves the way to new discoveries and uses in the field of genetic testing. On the other hand, the information can identify individuals, link them to others, and reveal complex data about the future health and development of those individuals and other people to whom they are genetically related.

The Working Party wishes to emphasise the importance of privacy as a fundamental right and the consequent necessity of deploying new genetic technologies with safeguards adequate to protect that right.”

## The Council of Europe Cybercrime Convention

The issue of cybercrime was raised in Chapter 2. This issue, which has raised concerns nationally, in Europe and at a wider international level, presents a real risk about which governments are properly concerned. The Council of Europe has become the forum in which negotiations to develop a Cybercrime Convention are being conducted. The retention of traffic data beyond the period demanded by technical and commercial reasons would be an invasion of the right to private life assured by Article 8 of the European Convention on Human Rights. The Data Protection Commissioners made their position clear at Stockholm in April 2000 and reaffirmed that view at their Spring Conference in Athens on 10 and 11 April 2001 by the following Declaration:

*Case Study-continued from page 34*

### OUTCOME:

The council responded explaining that whilst systems and procedures were in place at the depot concerned these had not been strictly adhered to. As a result of the complaint all depots had been issued with shredders and management had been reminded of the procedures, which should be followed. In addition all employees were to receive data protection awareness training. Data protection liaison officers throughout the council were informed of the incident and asked to apply the lessons learned in their own areas.

## Case Study

### **BREACH: Not processed in line with Individual's rights (6th DP principle)**

An NHS Trust repeatedly failed to meet the 40-day target for subject access requests. It was clear that the difficulties it was experiencing were to do with the fact that the DP Act 1998 includes accessible health records and this requires the inclusion of copies of X-rays. In view of the number of requests for assessments received about this particular Trust a compliance visit was made. Working with senior personnel at the Trust we advised on and agreed improvements in their administrative arrangements to ensure that in future the subject access requirements would be met.

“The Spring 2001 Conference of European Data Protection Commissioners notes with continuing concern proposals that ISP's (Internet service providers) should routinely retain traffic data beyond the requirements of billing purposes in order to permit possible access by law enforcement bodies.

The Conference emphasizes its view expressed in Stockholm that such retention would be an improper invasion of the fundamental rights guaranteed to individuals by Article 8 of the European Convention on Human Rights and in relation to the processing of personal data by the 1981 Council of Europe Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (Convention 108). The Conference point out that such retention would also invade the rights specified by Articles 8 and 7 of the Charter of Fundamental Rights of the European Union. Where traffic data are to be retained in specific cases, there must be a demonstrable need, the period of retention must be as short as possible, and the practice must be clearly regulated by law.”

### **The Wider World**

Although much of our work outside the United Kingdom looks first to the European Union and then the wider Europe, data protection and informational privacy has always been an international matter as reflected in the 1980 OECD Guidelines and the long running series of International Conferences of the Data Protection Commissioners, of which the most recent in the series took place in Venice in September 2000.



An issue canvassed in Venice was whether the time was right for a review of the international instruments dealing with data protection and the preparation of a more global multi-lateral convention. The predominant view was that it would be more constructive for the moment to concentrate on pragmatic means

of securing the implementation of and compliance with the acknowledged international principles declared in instruments such as the OECD Guidelines. [There will, in any case, be regional reviews of legislation such as the report on EU Data Protection Directive 95/46/EC which the European Commission have to make in the autumn of 2001.] The International Conference next meets in Paris in September 2001 after that all the British and Irish data protection authorities including the smaller islands (including

Jersey, Guernsey and the Isle of Man) will jointly act as host for the conference in 2002 at a location to be announced in Paris this autumn.

Our international work is a contribution to the worldwide development of good information handling practice. Data Protection rules arose in the 1970s and were expressed in the Council of Europe Convention and the OECD Guidelines as a means of providing protection for individuals whilst permitting the free flow of information for trade purposes. The growth of the internet and e-commerce has intensified the global nature of the problems and so we have continued to work not only with our international colleagues, but particularly with the OECD and the newly created Commonwealth Centre for Electronic Governance. Following the 1998 Ministerial meeting, the OECD has continued its work to find pragmatic means of securing the implementation of its Privacy Principles in global electronic networks. The last year has seen the adoption of the OECD Privacy Statement Generator for web sites (<http://cs3-hq.oecd.org/scripts/pwv3/pwhome.htm>), the start of its work to find on-line Alternative Dispute Resolution methods for dealing with privacy and consumer disputes arising in e-commerce, and also the start of work on the special privacy problems of genetic research data. The Commonwealth Centre is new, but we hope to be able to contribute to good practice methods through the important global channel of the Commonwealth.



### Case Study

#### **BREACH:** **Unfair processing** **(1st DP principle)**

#### **Inadequate, irrelevant** **and excessive** **(3rd DP Principle)**

A “Lifestyle Survey” being carried out by a Health Authority resulted in a complaint to a regional newspaper about the survey not being as confidential as the Health Authority claimed. It became clear that information had not been fairly processed; explanations had not been as clear as they should have been; they had used full postcodes without realising that this could still be personal data; they had also included a question in the survey which did not relate clearly to the data subject’s health or to the declared aims of the survey.

#### *OUTCOME:*

The Health Authority accepted that clearer information needed to be provided to respondents about the purpose of the survey. They decided not to use full postcodes; they agreed to ignore any responses to the irrelevant question and not to use it in any future surveys.

## Chapter 6:

# Organisational matters



*“We have offered specific training posts for which we have recruited staff on the promise of support to pursue professional qualifications.”*

### Staffing Matters

#### Recruitment and retention

Throughout the year, we have seen the effects of the demand for, and associated salary packages available to, staff with data protection expertise. A number of staff have moved on to posts in the private sector, within and outside the UK.

We have always accepted that, in an office of this size, we cannot always offer all the staff who join us the opportunities to develop their career quickly enough to ensure that they stay with us. Indeed, particularly in the fast moving and developing areas with which we are concerned, some turnover of staff is healthy. However, people moving on can quickly become a problem if we are unable to recruit suitable replacements, particularly when our public profile and the resultant workloads, are increasing.

In the first half of the year, we experienced a very difficult period in terms of recruitment. The health of the local economy meant that there was very little unemployed talent to tap into. Recognising that, we found that employers understandably fought hard to retain their staff, offering to match salaries or provide other benefits in ways which those of us in the public sector are, quite understandably, prevented from doing.

Facing real recruitment and, thus, workload problems, we looked hard at what packages we could offer which others would have difficulty in matching. We have offered specific training posts for which we have recruited staff on the promise of support to pursue professional qualifications. In attracting staff we have concentrated on the benefits of working in the public sector, our expanded role, the growth over the coming years, and the possibility of acquiring knowledge which is increasingly sought and valued in the employment market.



We have now created a healthy recruitment situation, attracting increased interest, applications and competition for appointments. This is necessary, given the extra demands which await us over the next few years. We shall need to continue to effectively compete to ensure that those who we need to make a contribution will join us. Whilst accepting that some of those who join us will go on to develop their careers elsewhere (many in the data protection or freedom of information fields) we do need to be able to offer a sufficiently attractive package to ensure a level of staff retention throughout what will be testing times.

### **Investors in people**

Last year, we made significant progress towards accreditation as an investor in people. We have always seen that the benefits of this come from the steps we have to take to achieve the award and the need to benchmark ourselves against accepted best practice rather than the award of the accreditation itself.

This year a second full assessment of the standards of the office was undertaken. The resultant report was very complimentary on a number of the initiatives we have taken in furtherance of meeting the standards. Although there are still areas where we have more work to do, we feel that many of the benefits have already begun to feed through.

### **Training**

Training will have a major role to play over the next few years in terms of preparing staff for the increased responsibilities of the Office, increasing the size of the establishment and ensuring that those who stay to develop their career with us derive maximum benefit from their time here. A major training initiative during the year included a concentrated programme of IT training to refresh existing skills and to develop further skills in the use of the suite of programmes used throughout the Office. A special rate was negotiated with a local training provider to meet our needs and the programme received very favourable feedback from staff at all levels who attended.

Specific training was also organised to familiarise staff with the Human Rights Act 1998.

### **Secondments**

We view secondments as an alternative way of delivering training by broadening experience in a way that is not always possible in a small office. There is never an ideal time to pursue secondment opportunities – there are always more short-term reasons to keep staff rather than let them go elsewhere for long-term gains. Given the workloads we have faced and the recruitment difficulties in the early part of the year, this last year might have seemed to

## Case Study

### **BREACH: Unlawful disclosure (S29)**

The DSS carried out an investigation into potential benefit fraud on a housing estate in the course of which a large number of vehicle registration numbers were collected. These were then submitted in bulk to the DVLA who provided name and address details of the vehicle keepers to the DSS to aid their investigations. The lawful basis cited for the disclosure was s29.

Following a request for assessment made to the Commissioner the DVLA's application of the s29 exemption was called into question. S29 permits disclosures on a case-by-case basis for crime prevention purposes. The DSS exercise on the other hand appeared to constitute a kind of "fishing expedition", raising important questions about the rights of individuals to privacy except where their actions justify an intrusion into their privacy. It was assessed, therefore, that a breach of the requirements of the Act was likely in this case since proper steps had not been taken to apply the exemption on a case-by-case basis.

*Case Study-continued on page 41*

have definitely been a time to resist any such moves. Despite this, we have stood by our policy.

With Office support, a member of staff has completed a legal qualification in his own time. We successfully sought accreditation as a training provider from the Law Society, and have loaned him out for a period to an Insurance Society to ensure that he receives a broader based training contract than we could have provided on our own. In return, we have taken two management trainees for six months periods, to assist us and to give them an insight into the work of a regulator that will benefit both them and their employer on their return.

A long-standing member of staff has been seconded as Deputy Data Protection Commissioner in Guernsey for 12 months. He will play a key role throughout the period of their transition to revised legislation along the lines of our DP Act 1998.

A solicitor from the Crown Prosecution Service completed a review of our procedures during an eight-month secondment period, and recommended that we conduct more of the prosecutions work in-house. A new post of prosecutions solicitor was identified and filled.

We have recently begun discussions with a solicitors' practice to explore the potential mutual benefits of their seconding a solicitor to work for us for a period.



Late in the year, we arranged for someone to join us for six months on a secondment from the Government Office (North West) to assist us in carrying out a broad-ranging review of compliance issues.

### **Pensions**

All the administrative arrangements to cover the movement of staff from the by-analogy scheme to the PCSPS have been completed. We have provided advice

based on our experience to a number of other organisations that would like to follow the same path.

## Finance

### Income

This was the first year in which the reduced income from transition to payment for a single year of notification, rather than a 3-year registration fee, took effect. Although our income was reduced as a result, we managed to exceed our forecast for the number of fees received from new applications, transformations from previous registration entries, and the first renewals of the one-year notification entries. In consequence, our income for the year was slightly ahead of our projection, coming in at just over two million pounds.

Our income will increase in each of the two coming years as, in addition to these first renewals of notifications under the DP Act 1998, all of the previous multi-year registration entries will become liable for transformation to notification entries with a one year fee and life.

The trend to move to payment by direct debit has continued which has meant an improved service for all those involved in notification.

### Grant-in-Aid

We received notification of the level of grant well ahead of the start of the financial year, which greatly assisted the planning process.

We were very happy that our requests for additional funds to enable us to update and reinvigorate our Information and Communications Technology were answered with a capital grant of five million pounds over the coming two financial years (2001/2 to 2002/3). A project to ensure that the money is used in the most effective way to assist us in meeting our own and central government's aims is now underway.

There have been some changes to the accounting arrangements to ensure that spending on data protection and freedom of information could be identified separately for budgetary purposes. That has meant a change in our financial memorandum. A draft revision was sent to our sponsor unit for discussion and agreement before the end of the year.

### Invest to Save

We were delighted that our bid for funding for the BAIRD project was recognised as worthy of investment in a competition open to all bodies throughout central government. We secured £100,000 to fund the project for a further year.

*Case Study-continued from page 40*

#### OUTCOME:

DSS and DVLA procedures were subsequently reviewed and revised versions submitted to the Commissioner. These were considered by compliance staff and viewed as appropriate to ensure the proper application of the s29 exemption.

## Enquiries

### Of the enquiries we receive:

#### 12,000 calls concerned with individual rights:

The enquiry line received approximately 12,000 calls from individuals seeking advice and information on their rights under the Act.

#### 3,800 calls on subject access to credit files:

There were over 3,800 calls on the subject access to credit files. These enquiries ranged from simple requests for the details of the credit rating agencies through to individuals experiencing difficulties in obtaining retail credit due to old or inaccurate data being held on files.

A typical scenario would be: the individual had recently moved, then applied for retail credit in a store. The individual would then be told that their request has been turned down “probably due to your address being blacklisted”. More often than not the problem is caused by the individual not being listed on the Electoral Roll at the address cited.

#### 3,000 calls on how to access rights:

There were over 3,000 calls in relation to how individuals can exercise their rights in relation to access to personal data held on them. Many of the calls suggest a belief that the Commissioner’s Office processes and stores all personal data that any organisation processes in the UK.

*Enquiries-continued on page 43*

## Planning

### Changed Responsibilities

Our extra responsibilities have affected every aspect of the work of the Office, starting at the highest level with the Mission Statement. The Statement was formulated following a series of workshops attended by all staff that focused on the expanded role of the Office. From that mission statement, a series of steps lead down to individual contributions, which feed back through team targets, office annual milestones and three-year objectives over the course of the corporate planning cycle to progress against the Office long-term aims. Full details of these are set out in Chapter 8.

### Risk Management

Management of risk has always been a vital part of management. In an office of this size, it is an aspect often covered by a series of formal and informal reporting mechanisms, involving all members of the Senior Management Group. Although such an approach works well in a small single-site operation with regular management interface, in line with the Turnbull Report recommendations, the Office has set up a more formal risk management policy which identifies the most significant risks which the Office needs to contain in order to achieve its objectives, and the assignment of ownership of these risks.

The aim will be for the responsible manager to produce an up-to-date report for the Board on a quarterly basis, or an immediate one in the event that he or she perceives there to have been a significant change in the level of the risk.

### Northern Ireland

The Office has submitted a draft Equality Scheme to the Equality Commission for Northern Ireland. Although the number of requests for assessment that we receive is broadly in line with the relative size of the population, we do relatively little work actually within the Province. We expressed our concern that the limited presence would make it difficult for us to make a meaningful contribution to some of the aims of the relevant legislation, but also accepted that our expanded role might also indicate that we should review the way in which we respond to the needs of the people of Northern Ireland.

## Property

### Longer Term Needs

The findings of the Devolution Study will guide us on how many offices we should plan to have over the next few years. Those decisions will affect how large an office we shall need in Wilmslow, whether and how many others there ought to be, and how large any other premises will need to be.

During the year, we held a number of meetings with BEMU (the Home Office Buildings and Estates Management unit) who will provide advice on the strategy and options for accommodation in Wilmslow and elsewhere.

During the year, we secured the lease for the remainder of the one building we currently occupy. Our space needs are a constantly evolving picture as so much of our future workload will become clear only as we experience the impacts, not just of the Freedom of Information legislation, but of the growing spread, awareness and complexities of data protection issues. Securing the current accommodation was important but we have kept under review the need to take on additional space on a short term basis should the need arise ahead of longer term needs being firmly established.



#### *Enquiries-continued from page 42*

These calls tend to follow the line of “I want you to send me all the information you hold on me”. When it is explained that we only hold limited information such as the Data Protection Register, staff details, contacts and data held in relation to assessments, the enquirers tend to ask how to get the information. We explain that they must write to individual organisations. A suggested letter is in our leaflet: ‘Using the law to protect your information’.

#### **1,200 calls on unsolicited telephone marketing & junk faxes:**

Over 1,200 calls were received on the subject of unsolicited telephone marketing and junk faxes. The complaint is normally that the enquirer has informed the marketing organisation that they do not want to receive such approaches, however, despite their request the approaches continue. One area of contention is where the call being received is a fax call and the subscriber does not have a fax machine. The banshee screech of a fax call at 2 o’clock in the morning provokes the most furious response from individuals. This is not calmed when we have to inform them that the Telecommunications (Data Protection & Privacy) Regulations 1999 refers to unsolicited marketing faxes and, with no fax as evidence, our ability to take action is frustrated.



## Chapter 7:

# Financial matters



### Financial Position to 31 March 2001

Year ended 31 March	Office Expenditure	Other Expenditure	Receipts	Cumulative Financial Position	Cumulative Financial Position	Accrued Fees
	<i>In Cash Terms</i>	<i>In Cash Terms</i>	<i>In Cash Terms</i>	<i>In Cash Terms</i>	<i>In Accruals Terms</i>	
£'000	£'000	(note 1) £'000	(note 2) £'000	£'000	(note 3) £'000	(note 4) £'000
1985	308	31	–	(339)		
1986	1,696	58	424	(1,669)		
1987	2,422	72	2,757	(1,406)		
1988	2,650	60	930	(3,186)		
1989	2,624	60	1,294	(4,576)		
1990	2,975	67	5,428	(2,190)		
1991	3,153	83	2,068	(3,358)		
1992	3,402	95	2,425	(4,430)	(9,191)	1,503
1993	3,723	78	7,842	(389)	(9,469)	5,903
1994	3,449	83	4,494	573	(7,913)	5,519
1995	3,798	69	3,420	126	(6,417)	3,673
1996	3,975	64	7,072	3,159	(5,526)	5,752
1997	4,025	65	5,173	4,242	(4,471)	5,697
1998	3,660	79	4,913	5,416	(2,527)	4,864
1999	4,190	82	7,586	8,730	(830)	6,538
2000	4,704	94	5,617	9,549	339	9,131
2001	4,970	90	2,076	6,565	1,431	5,047
<b>Totals to 31 March 2001</b>	<b>55,724</b>	<b>1,230</b>	<b>63,519</b>	<b>6,565</b>	<b>1,431</b>	<b>5,047</b>

#### Notes:

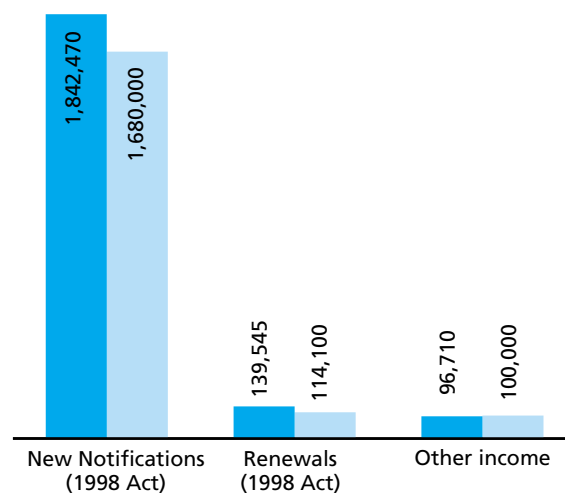
1. 'Other expenditure' includes that incurred in respect of the Information Commissioner, the Information Tribunal and related Home Office costs.
2. 'Receipts' include registration fees and other receipts such as interest on unallocated grant-in-aid in hand.
3. From 1992 onwards, the cumulative position under accruals accounting principles is given, adopting a 'full cost' approach. From 1985 these figures incorporate notional costs and are also subject to the Treasury 'GDP deflator'.
4. Under the accruals method of accounting, fees received have been spread over the three year registration period and notifications over one year, thus providing an 'accrued fees' figure to be carried forward to future years.

## Analysis of actual and forecast income 2000/2001

(in cash terms)

<b>Actual</b>		£
88.6%	New notifications (1998 Act)	1,842,470
6.7%	Renewals (1998 Act)	139,545
4.7%	Other income	96,710
100.0%		<u>2,078,725</u>

<b>Forecast</b>		£
88.7%	New notifications (1998 Act)	1,680,000
6.0%	Renewals (1998 Act)	114,100
5.3%	Other income	100,000
100.0%		<u>1,894,100</u>

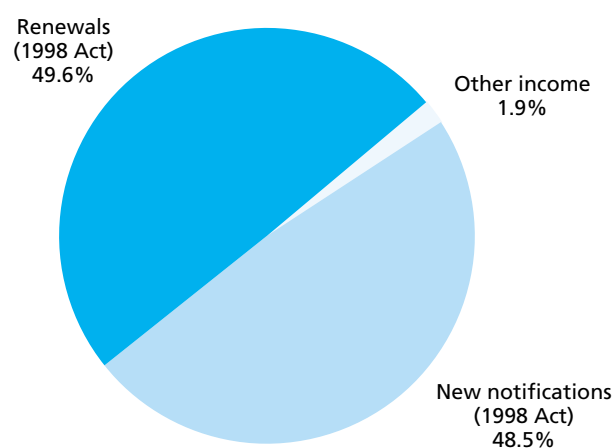


A full statement of account can be found in the Account.

## Analysis of forecast income 2001/2002

(in cash terms)

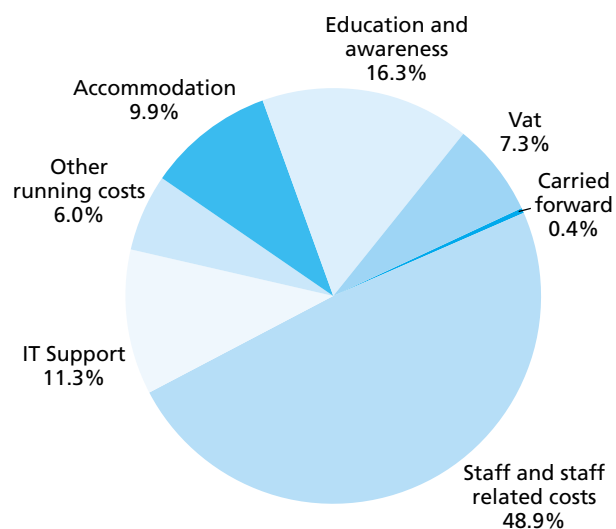
		£
48.5%	New notifications (1998 Act)	1,932,000
49.6%	Renewals (1998 Act)	1,977,500
1.9%	Other income	75,000
100.0%	Total	<u>3,984,500</u>



## How the grant was spent 2000/2001

(in cash terms)

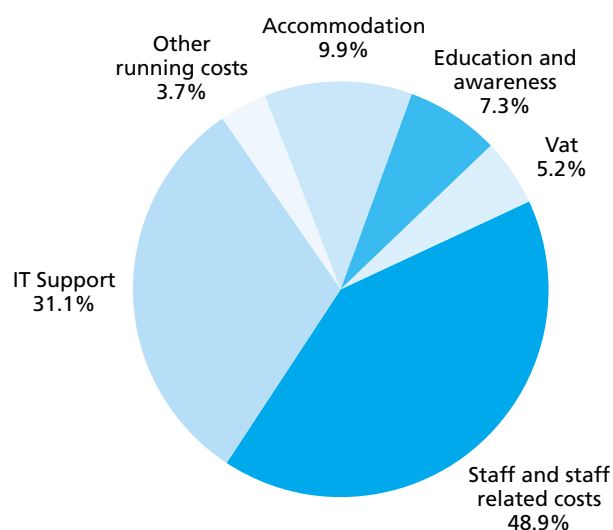
	£
48.9% Staff and staff related costs	2,581,778
11.3% IT Support	595,748
6.0% Other running costs	316,335
9.9% Accommodation	524,253
16.3% Education and awareness	858,781
7.3% Vat	384,274
0.4% Carried forward	19,691
<u>100.0% Total</u>	<u>5,280,860</u>



## Our spending plans for 2001/2002

(in cash terms)

	£
41.2% Staff costs	3,760,675
31.1% IT Support	2,834,000
3.7% Other running costs	334,500
11.5% Accommodation	1,053,500
7.3% Education and awareness	666,325
5.2% VAT	477,000
<u>100.0% Total</u>	<u>9,126,000</u>



## Chapter 8:

# The year ahead



The work of the Office cascades through a series of steps from its mission to each individual's contribution, as shown:

### **Mission Statement**

*What the Office is here to do*

### **Aims**

*How it achieves its **mission***

### **Objectives**

*Progress against **aims** in the next three years*

### **Milestones**

*Progress against **objectives** in the first year*

### **Team Targets**

*Departmental inputs to **milestones***

### **Individual Contributions**

*A work plan agreed in staff development reviews to contribute to **targets***

## Milestones for 2001 – 2002

The Milestones set for the financial year are derived from the Corporate Aims and Objectives:

**We will aim to ensure that the statutory duties placed upon us are met. To do this efficiently and effectively, we aim to be an organisation responsive to change and ready to manage risk in a way which will allow the resources available to us to be best used.**

Objectives	Milestones
1 Transform the Office to take account of increased statutory responsibilities and a changed constitutional framework; and the “Modernising Government” targets.	1 Devolution strategy decided. 2 Accommodation needs determined. 3 Investors-in-People accredited. 4 Pay, grading and rewards strategy reviewed in line with expanded requirements. 5 First stage of growth completed.
2 Develop costing, accounting and monitoring procedures and agree with the Home Office a change to our funding regime to allow an element of net funding.	1 Some recovery and retention of income agreed with the Home Office. 2 Whole Government accounts ‘dry run’ underway. 3 Improved workload and unit cost measures devised from ICT spend.
3 Formalise our risk-based approach to maintain a sound system of internal control. To ensure that this approach is embedded within our normal management processes, and becomes an ongoing procedure.	1 Risk strategy in place and responsibilities allocated.

**We will aim to ensure that policy makers give appropriate weight to individuals’ rights.**

Objectives	Milestones
1 Develop existing and new channels of communication with policy makers and educate them to ensure early consideration of information issues in the development of policy across government and at all levels.	1 Strategy to systematise contact with policy makers designed and developed.
2 Participate in and contribute to European and international discussions that affect the work of the Office.	1 Model data protection law for use in an international environment produced.



We will aim to ensure that those who handle information both in the public sector and in the private sector are aware of their obligations and act accordingly.

Objectives	Milestones
1 Raise awareness amongst: <ul style="list-style-type: none"> <li>• data controllers of their obligations under the Data Protection Act 1998 above the level achieved under the Data Protection Act 1984; and,</li> <li>• public authorities of their obligations in relation to the Freedom of Information Act 2000.</li> </ul>	1 “Large” data controllers to 82.0%. “Small” data controllers to 52.0%.  2 ‘Model’ Publication Scheme produced. 3 Initial level of awareness in public authorities of 14.0%.
2 Use, where necessary, the powers provided by the legislation to enforce the Commissioner’s duties in this aspect of compliance.	1 Commissioner’s revised Enforcement Strategy published.
3 Promote the adoption of self-regulatory tools that integrate with statutory enforcement, (particularly in providing remedies for individuals), and the development of new information systems.	1 Compliance related products provided and approved.

We will aim to ensure that individuals are aware of their rights to information, and feel confident that those rights are respected and can be exercised.

Objectives	Milestones
1 Achieve and sustain a high level of awareness of rights and how to use them, under the Data Protection and Freedom of Information Acts.	1 For data protection 25.0%. For freedom of information 11.0%.
2 Underpin those rights by providing: <ul style="list-style-type: none"> <li>• an effective level of support to enable individuals, as far as possible, to help themselves;</li> <li>• an effective service to process requests for decisions, for information and for assessments as required by the Acts.</li> </ul>	1 ‘Self-help’ initiative launched.  2 Proposals for revised service delivery targets utilising ICT spend agreed and in production.

Our Policy Issues Board (PIB) identifies and prioritises the projects that should be undertaken over the year to achieve these milestones. Agreed projects included on the PIB programme for the 2001–2002 financial year are as follows:

- Data Protection “Lite”. The production of model “bare-bones” data protection standards, aimed primarily at emerging Commonwealth nations, to address key areas such as adequacy of transfers. The legal work involved is to be undertaken by the Information and Privacy Commissioner’s Office, Ontario. The standards will fit in with the Commissioner’s comments relating to the review of the DP Act 1998 and EU Data Protection Directive.
- A study of various websites to assess compliance with data protection requirements dealing with areas such as whether the appropriate notifications are being provided or consents sought, whether privacy/fair obtaining notices are provided and if so whether such notices are “real”. This is intended to be more “in depth” than other similar studies and will involve contact with website operators. External assistance will be sought to undertake the study, which will initially be confined to websites that are clearly UK based.
- Human Issues in Security and Privacy for E-Commerce. UMIST has bid for a project under the Management of Information (MI) Programme. The programme is established between the DTI, the Engineering and Physical Sciences Research Council (EPSRC), and the Economic and Social Research Council (ESRC). The objectives of the project are to better promote e-commerce through innovative social marketing campaigns, guidance of e-commerce system design, and the next generation of privacy enhancing techniques. Our contribution to the project will be that of a research collaborator, which will involve reviewing proposals and contributing our views, as well as providing expert knowledge and contacts.
- Core health sector guidance, which will pull together much of the existing office guidance.
- A review of our enforcement policy and procedures.

# Information Commissioner's Accounts for the year ended 31 March 2001



## Index

	Page
Foreword	52
Statement of Responsibilities	55
Statement on the System of Internal Financial Control	56
The Certificate and Report of the Comptroller and Auditor General	58
Income and Expenditure Account	60
Balance Sheet	61
Cashflow Statement	62
Notes to the Accounts	63
 <b>Appendix A</b>	
Accounts Direction	73

# Foreword



## Introduction

The annual accounts have been prepared in a form directed by the Secretary of State for the Home Office as set out in the Accounts Direction which is reproduced in Appendix A.

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.

## History

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

## Principal Activities

The 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)

- allow individuals to claim compensation for damage and any associated distress arising from lack of security surrounding personal data which concern them and from inaccuracies in such data.

During the year the Office has assumed the responsibility of implementing the Freedom of Information Act 2000.

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 Office 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. She 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 her decisions are subject to the supervision of the Courts and the Information Tribunal.

The Commissioner is responsible for setting the priorities for her 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 Commissioner also has responsibilities in relation to consumer credit, access to personal files, the Telecommunications Directive and Europol.

Fuller details of the Commissioner's activities, and progress on her objectives during the year, are given elsewhere in the annual report.

## Results for the Period

The results for the year are set out on pages 60 to 71.

The Information Commissioner's Office has been financed by a grant-in-aid from the Home Office Vote (Class IV Vote 1 Section G).

## Fees

Schedule 5, paragraph 9(1) of the Data Protection Act 1998 provides that all fees and other sums received by the Commissioner in the exercise of her functions under the Act or section 159 of the Consumer Credit Act 1974 shall be paid by her to the Secretary of State.



### **Changes in Fixed Assets**

No significant changes in fixed assets were made in the year.

### **Future Developments**

A £5 million programme to modernise the Office IT systems will be undertaken over the next two years. In addition, as the implementation of the FOI Act proceeds, the Office will expand accordingly.

### **Charitable Donations**

No charitable donations were made in the year ended 31 March 2001 (1999/2000 – £nil).

### **Post Balance Sheet Events**

There are no significant events to report.

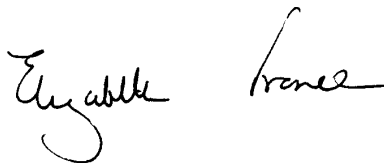
### **Compliance with Public Sector Payment Policy**

The Office has adopted a policy on prompt payment of invoices which complies with the 'Better Payment Practice Code' as recommended by Government. In the year ending 31 March 2001, 96.4 % (1999/2000 – 84%) 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%.

### **Employee Policies**

The Commissioner's Equal Opportunities policy aims to ensure that no potential or actual employee receives more or less favourable treatment on the grounds of race, colour, ethnic or national origin, marital status, sex, sexual orientation, disability or religious belief. An Employment Service Disability Advisor has commented on the Commissioner's "positive attitude and commitment" in the employment of people with disabilities.

The Commissioner is committed to obtaining accreditation under Investors in People and as such places importance on ensuring priority is given to the provision of appropriate training to enable staff to develop skills and understanding of their roles in line with the aims and objectives of the Office.



*Elizabeth France*

**Information Commissioner**

**13 June 2001**

# Statement of the Information Commissioner's Responsibilities



Under paragraph 10(1)(b) of schedule 5 to the Data Protection Act 1998 the Commissioner is required to prepare in respect of each financial year a statement of account in such form as the Secretary of State 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 her income and expenditure, total recognised gains and losses and cash flows for the financial year.

In preparing the accounts the Commissioner is required to:

- observe the Accounts Direction issued by the Secretary of State 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's Office will continue in operation.

As the senior full-time official, the Commissioner carries the responsibilities of an Accounting Officer. Her relevant responsibilities as Accounting Officer, including her responsibility for the propriety and regularity of the public finances and for the 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.

*Elizabeth France*

**Information Commissioner**

**13 June 2001**

# Statement on the System of Internal Financial Control



As Accounting Officer, I acknowledge my responsibility for ensuring that an effective system of internal financial control is maintained and operated by the Information Commissioner.

The system can provide only reasonable and not absolute assurance that assets are safeguarded, transactions authorised and properly recorded, and material errors or irregularities are either prevented or would be detected within a timely period.

The system of internal financial control is based on a framework of regular management information, administrative procedures, including the segregation of duties, and a system of delegation and accountability.

In particular, it includes:

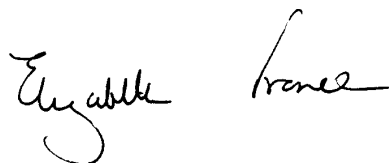
- comprehensive budgeting systems with an annual budget which is reviewed and agreed by a meeting of the corporate management members;
- regular reviews by the senior management of periodic and annual financial reports which indicate financial performance against the forecasts;
- setting targets to measure financial and other performance;
- a system of delegated authority in respect of commitment to spend and actual expenditure which provides overall control assurance.

Internal audit of the Information Commissioner is conducted on its behalf by the Home Office Audit and Assurance Unit (AAU) which operates to standards defined in the Government Internal Audit Manual. The work of the AAU is informed by an analysis of the risk to which the Information Commissioner is exposed, and annual internal audit plans are based on this analysis. The analysis of risk and the internal audit plans are endorsed by the Information Commissioner's Audit Committee and approved by me. At least annually AAU provides me with a report on internal audit activity in the

Office. The report includes the AAU's independent opinion on the adequacy and effectiveness of the Office's systems reviewed during the year.

My review of the effectiveness of the system of internal financial control is informed by the work of the internal auditors, the Audit Committee which oversees the work of the internal auditors, the executive managers within the Office who have responsibility for the development and maintenance of the financial control framework, and comments made by the external auditors in their management letter and other reports.

As Accounting Officer, I am aware of the recommendations of the Turnbull Committee and I am taking reasonable steps to comply with the Treasury's requirement for a statement of internal control to be prepared for the year ended 31 March 2002, in accordance with guidance issued by them.

A handwritten signature in black ink, appearing to read 'Elizabeth France', with a stylized, cursive script.

*Elizabeth France*

**Information Commissioner**

**13 June 2001**

# 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 60 to 71 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 set out on pages 63 and 64.

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

As described on page 55, the Information Commissioner is responsible for the preparation of the financial statements 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 guided by the Auditing Practices Board and the auditing profession's ethical guidance.

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, 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 contained 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 page 56 reflects the Commissioner's compliance with Treasury's guidance 'Corporate governance: statement on the



system of internal financial 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.

## **Basis of Opinion**

I conducted my audit in accordance with 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 2001 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; 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**

**Date 21 June 2001**

**National Audit Office**

157-197 Buckingham Palace Road

Victoria London SW1W 9SP

## Income and Expenditure Account for the year ended 31 March 2001

		2000/2001		1999/2000	
	Note	£	£	£	£
<b>Income</b>					
Grant-in-aid	2	5,258,686		4,694,240	
Other Income	6	46,755		84,220	
			5,305,441		4,778,460
<b>Expenditure</b>					
Staff Costs	5	2,183,898		2,028,953	
Other Operating Costs	7	3,214,624		2,675,107	
Depreciation of Tangible Fixed Assets	8	17,207		17,606	
			(5,415,729)		(4,721,666)
<b>Operating (Deficit)/Surplus</b>			(110,288)		56,794
Fee Income	3		6,066,385		5,837,495
Interest Receivable			49,561		56,037
Notional Cost of Capital			2,411		3,250
<b>Surplus for the year before appropriations</b>			6,008,069		5,953,576
Notional Cost of Capital Reversal			(2,411)		(3,250)
Appropriations due to the Home Office			(6,162,701)		(5,977,752)
<b>Retained Deficit for the year</b>			(157,043)		(27,426)

## Statement of Total Recognised Gains and Losses for the Year Ended 31 March 2001

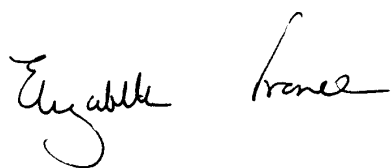
		2000/2001	1999/2000
	Note	£	£
Retained deficit for the year		(157,043)	(27,426)
Unrealised (deficit)/surplus on revaluation of assets	12	(3,124)	3,349
Total recognised losses relating to the year		(160,167)	(24,077)

The notes on pages 63 to 71 form part of these accounts

## Balance sheet as at 31 March 2001

	Note	31 March 2001		31 March 2000	
		£	£	£	£
<b>Fixed Assets</b>					
Tangible fixed assets	8		57,963		55,345
<b>Current Assets</b>					
Debtors and prepayments	9	5,136,363		9,213,851	
Cash at bank and in hand	14	102,836		77,555	
		5,239,199		9,291,406	
<b>Creditors – amounts falling due within one year</b>	10	(4,523,172)		(5,230,531)	
<b>Net Current Assets</b>			716,027		4,060,875
<b>CREDITORS – amounts falling due after one year</b>	11		(890,727)		(4,078,532)
<b>Net Assets</b>			(116,737)		37,688
<b>Capital and Reserves</b>					
Income and Expenditure Reserve	12		(174,700)		(17,657)
Other Reserves	12		57,963		55,345
			(116,737)		37,688

The notes on pages 63 to 71 form part of these accounts



**Elizabeth France**

**Information Commissioner**

13 June 2001

## Cashflow Statement for the year ended 31 March 2001

		2000/2001		1999/2000	
	Note	£	£	£	£
<b>Net cash inflow from operating activities</b>	13		60,087		84,933
<b>Returns on investments and servicing of finance</b>					
Interest Received			49,561		56,037
<b>Investing activities</b>					
Payment to acquire tangible fixed assets			(33,021)		–
<b>Net cash inflow before Financing</b>			76,627		140,970
<b>Financing</b>					
Grant-in-aid for capital expenditure		33,021		–	
Fee Income received	3	1,982,409		5,477,125	
Less: Income Appropriated to the Home Office	4	(2,066,776)		(5,786,607)	
			(51,346)		(309,482)
<b>Increase/(Decrease) in cash</b>			25,281		(168,512)

The notes on pages 63 to 71 form part of these accounts.

# Notes to the Accounts



## 1. Statement of Accounting Policies

### 1.1 Accounting Convention

This Account has been prepared in a form directed by the Secretary of State for the Home Office. The Accounts Direction is reproduced in Appendix A.

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

### 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.

### 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 £2000 or more. Fixed Assets are valued at net current replacement cost by using the **Price Index Numbers for Current Cost Accounting** published by the Office for National Statistics.

### 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



## 1.5 Software and Development Costs

Software and system development expenditure on Information Technology systems is written off in the period in which it is incurred.

## 1.6 Income Recognition

Fee income comprises notification fees in respect of notifications by data-controllers, under the Data Protection Act 1998 (implemented on 1 March 2000) and registration fees in respect of registrations by data-users under the Data Protection Act, 1984.

The notification fee is paid in advance for a period of 1 year, until 29 February 2000 registration fees were paid in advance for a period up to 3 years. 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, and thus a prepayment is included within the Account in respect of income appropriated to the Home Office in advance of recognition of the income in the Income and Expenditure Account.

## 1.7 Notional Charges

In accordance with the Treasury guidance, **Executive Non-Departmental Public Bodies: Annual Reports and Accounts**, a notional charge for the cost of capital employed in the period is included in the Income and Expenditure Account along with an equivalent reversing notional income to finance the charge. The charge for the period is calculated using the Treasury's discount rate of 6% applied to the mean value of capital employed during the period.

## 1.8 Operating Leases

Payments made under operating leases on Land and Buildings and Equipment are charged to the Income and Expenditure Account as incurred.

## 1.9 Value Added Tax

The Information Commissioner is only eligible to register for VAT in respect of office accommodation sublet back to the landlord.

## 2. Grant-in-aid

	2000/2001	1999/2000
	£	£
Grant Received from Class IV Vote 1 (Section G)	5,274,500	4,681,000
Transfer to Deferred Government Grant Reserve in respect of fixed asset additions	(33,021)	—
Release of Deferred Government Grant in respect of depreciation charged	17,207	13,240
	<u>5,258,686</u>	<u>4,694,240</u>

## 3. Fee Income

Fees received in respect of notification fees are paid over to the Secretary of State for the Home Office

Receipts in the period were as follows:

	Data Protection Act 1984	Data Protection Act 1998	2000/2001	1999/2000
	£	£	£	£
Deferred income at 1 April 2000	9,021,623	109,346	9,130,969	9,491,339
Cash received for fees	—	1,982,409	1,982,409	5,477,125
Deferred income at 31 March 2001	<u>(3,969,186)</u>	<u>(1,077,807)</u>	<u>(5,046,993)</u>	<u>(9,130,969)</u>
Fee Income from external fees	<u>5,052,437</u>	<u>1,013,948</u>	<u>6,066,385</u>	<u>5,837,495</u>

## 4. Appropriations

	2000/2001	1999/2000
	£	£
Cash received for fees (note 3)	1,982,409	5,477,125
Interest receivable	49,561	56,037
Other income	46,755	84,220
Home Office creditor at 1 April 2000	71,195	240,420
Less Home Office creditor at 31 March 2001	<u>(83,144)</u>	<u>(71,195)</u>
	<u>2,066,776</u>	<u>5,786,607</u>

## 5. Salaries

The average number of persons employed by the Commissioner during the year was as follows:

	2000/2001	1999/2000
	No.	No.
Corporate management	5	5
Senior Staff	6	6
Other Staff	112	101
Occasional Casuals	3	2
	<u>126</u>	<u>114</u>

The aggregate payroll costs of these persons were as follows:

	£	£
Wages and salaries	2,013,973	1,835,935
Social Security costs	130,190	124,023
Pension Costs	39,735	68,995
	<u>2,183,898</u>	<u>2,028,953</u>

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

The Commissioner and Deputy Commissioners have consented to the disclosure of the salary and pension entitlements below.

	Salary	Real Increase in pension at 60	Total Accrued Pension at 60 at 31 Mar 2001
	(£'000)	(£'000)	(£'000)
Elizabeth France <i>Information Commissioner</i>	70–75	5.0–7.5	25–30
Francis Aldhouse <i>Deputy Commissioner</i>	55–60	0–2.5	10–15
John Woulds <i>Deputy Commissioner</i>	50–55	0–2.5	10–15

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

Pension benefits are provided through the Principal Civil Service Pension Scheme. This is a statutory scheme which provides benefits on a “final salary” basis at a normal retirement age of 60. Benefits accrue at the rate of 1/80th of pensionable salary for each year of service. In addition a lump sum equivalent to 3 years’ pension is payable on retirement. Members pay contributions of 1.5% of pensionable earnings in respect of widows/widowers/dependents benefits.

Pensions increase in line with the Retail Prices Index. On death, pensions are payable to the surviving spouse at a rate of half the member’s pension. On death in service, the schemes provide a lump sum benefit of twice the pensionable pay and also provide a service enhancement on computing the widow(er)’s pension. The enhancement depends on length of service and cannot exceed 10 years. Medical retirement is possible in the event of serious ill-health. In this case pensions are brought into payment immediately without actuarial reduction and with service enhanced as for widow(er) pensions.

Agreement was reached to transfer the staff within The Data Protection Registrar's Staff Pension Scheme into the Principal Civil Service Pension Scheme with effect from 1 April 2000. The Data Protection Registrar's Staff Pension Scheme is a by-analogy scheme to the PCSPS and paid pension benefits, funded from grant-in-aid, to scheme members of £19,778 (1999/2000 – £16,454).

Contributions were paid directly to PCSPS by the Home Office and do not form part of this account. The total amount of such contributions for the year ended 31 March 2001 was £238,622. (1999/2000 – £229,557).

## 6. Other Income

	2000/2001	1999/2000
	£	£
Legal Fees Recovered	10,040	22,712
Pension contributions and transfers	225	14,713
Rents refunded	27,744	–
Refund of Business Rates following appeal	–	45,325
Other Income	8,746	1,470
	<u>46,755</u>	<u>84,220</u>

## 7. Other Operating Costs

	2000/2001	1999/2000
	£	£
Rent and rates	445,944	437,176
Maintenance, cleaning, heating and lighting	78,530	67,684
Office supplies, printing and stationery	93,474	83,795
Carriage and telecommunications	66,150	75,685
Travel, subsistence and hospitality	164,689	162,490
Staff recruitment	72,505	19,474
Specialist assistance	70,964	91,693
Education and awareness	956,423	506,386
Legal costs	40,710	65,826
Staff training, health and safety	80,441	16,739
Computer bureau	751,220	818,779
Vehicle expenses	914	1,058
Audit fee	12,700	15,000
VAT	379,960	313,322
	<u>3,214,624</u>	<u>2,675,107</u>

Included in the above are operating lease payments for land and buildings totalling £333,450 (1999/2000 – £295,254).

VAT is not allocated across individual expenditure headings in order to show more meaningful comparisons within each category of expenditure.

## 8. Tangible Fixed Assets

### Equipment & Furniture

£

#### Cost or Valuation

At 1 April 2000	123,496
Additions	33,021
Disposals	(20,145)
Revaluations in the year	(6,783)
At 31 March 2001	129,589

#### Depreciation

At 1 April 2000	68,151
Revaluations	(3,659)
Charged in year	17,207
Disposals	(10,073)
At 31 March 2001	71,626

#### Net Book Value

At 31 March 2001	57,963
At 31 March 2000	55,345

## 9. Debtors

	31 March 2001	31 March 2000
	£	£
Fee income prepaid to the Home Office	5,046,993	9,130,969
Other prepayments	77,855	80,117
Other debtors	11,515	2,765
	5,136,363	9,213,851
Amounts falling due after more than one year included above are:		
Fee income prepaid to the Home Office	890,727	4,078,532

**10. Creditors – amounts falling due within one year**

	31 March 2001	31 March 2000
	£	£
Trade creditors	255,136	58,034
Payroll	15,926	33,865
Accruals	12,700	15,000
Home Office creditor	83,144	71,195
Deferred income	4,156,266	5,052,437
	<u>4,523,172</u>	<u>5,230,531</u>

**11. Creditors— amounts falling due after one year**

	31 March 2001	31 March 2000
	£	£
Deferred income	890,727	4,078,532

**12. Reserves**

	Income & Expenditure Reserve	Deferred Government Grant Reserve	Revaluation Reserve	Total
	£	£	£	£
Balance at 1 April 2000	(17,657)	51,996	3,349	37,688
(Deficit) in year	(157,043)	–	–	(157,043)
Revaluation of assets	–	–	(6,783)	(6,783)
Depreciation due to revaluation		–	3,659	3,659
Grant deferred for additions		33,021	–	33,021
Release for depreciation	–	(17,207)	–	(17,207)
Loss on disposals	–	(10,072)		(10,072)
Balance at 31 March 2001	<u>(174,700)</u>	<u>57,738</u>	<u>225</u>	<u>(116,737)</u>



### 13. Reconciliation of Operating Surplus to Net Cash Inflow from Operating Activities

	2001	2000
	£	£
Operating (deficit)/surplus for the year	(110,288)	56,794
Depreciation provided in year	17,207	13,240
Additional depreciation provided due to revaluation	–	4,366
Release of deferred government grant	(17,207)	(13,240)
Increase in debtors relating to operating activities	(6,488)	(2,972)
Increase in creditors relating to operating activities	176,863	26,745
Net cash inflow from operating activities	60,087	84,933

### 14. Cash at Bank and in Hand

	2001	2000
	£	£
Balance at 1 April 2000	77,555	246,067
Increase/(Decrease) in Cash	25,281	(168,512)
Balance at 31 March 2001	102,836	77,555
Commercial banks	102,548	77,375
Cash in hand	288	180
	102,836	77,555

### 15. Commitments under Operating Leases

At 31 March 2001 the Information Commissioner was committed to make the following annual payments in respect of operating leases expiring:

	Land and Buildings	
	31 March 2001	31 March 2000
	£	£
within one year	–	3,156
between two to five years	25,700	–
after five years	322,706	322,706
	348,406	325,862

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

## 16. Contingent Liabilities

The Information Commissioner has entered into a contract (which is not an operating lease) for the provision of IT Services. The cost of cancelling the contract at 31 March 2001 would be £131,433 (31 March 2000 – £192,078).

## 17. Capital Commitments

At 31 March 2001 no capital commitments were contracted for (31 March 2000 – £nil)

## 18. Losses and Special Payments

There were no losses or special payments to report for the year (31 March 2000 – £nil)

## 19. Post Balance Sheet Events

There were no post balance sheet events to report for the year (31 March 2000 – £nil)

## 20. Related Party Transactions

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

The Home Office is a related party to the Information Commissioner. During the year ending 31 March 2001 no related party transactions were entered into, with the exception of the Home Office providing the Information Commissioner with grant-in-aid, and internal audit services.

In addition, the Information Commissioner has had various material transactions with other central Government bodies. Most of these transactions have been with the Central Office of Information (COI), Property Advisers to the Civil Estate (PACE) and the Central Computer Telecommunications Agency (CCTA).

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



## Appendix A to the Accounts

# Information Commissioner



**Accounts direction given by the Secretary of State for the Home Department, with the approval of the Treasury, in accordance with paragraph (10)(1)(b) of schedule 5 to the Data Protection Act 1998.**

The annual accounts shall give a true and fair view of the income and expenditure and cash flows for the financial year, and the state of affairs as at the year-end. Subject to this requirement the Information Commissioner shall prepare accounts for the financial year ended 31 March 2001 and subsequent financial years in accordance with:

- a. Executive Non-Departmental Public Bodies Annual Reports and Accounts Guidance;
- b. other guidance which the Treasury may issue from time to time in respect of accounts which are required to give a true and fair view;
- c. any other specific disclosures required by the Secretary of State;

except where agreed otherwise with the Treasury, in which case the exception shall be described in the notes to the accounts.

Signed by authority of the Secretary of State of the Home Department.

L Hughes  
Head of Freedom of Information and Data Protection Unit  
Constitutional and Community Policy Directorate  
Home Office

3 May 2001



# Appendix





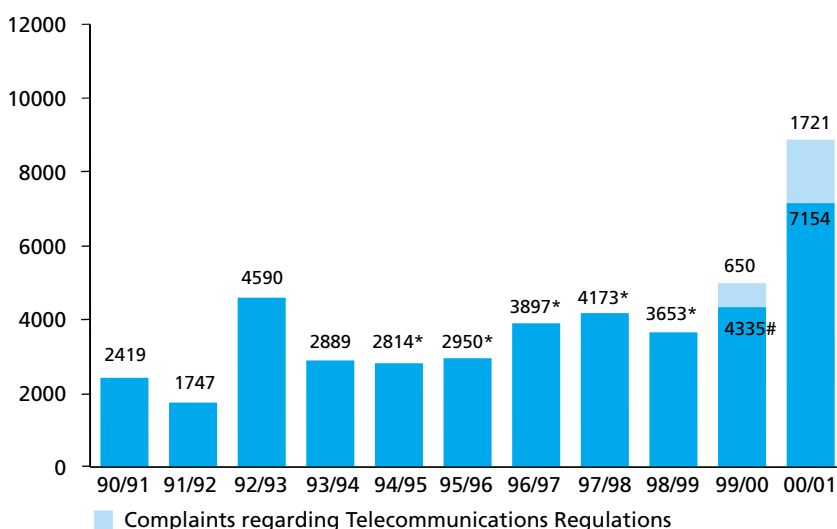
## Our Annual Caseload

### Requests for assessment

Section 42 of the DP Act 1998 provides that persons who believe they are directly affected by any processing of personal data may request the Commissioner to make an assessment whether the processing is likely or unlikely to have been carried out in compliance with the Act. In practice most requests for assessment are complaints from individuals who believe that their personal data have not been processed in compliance with the Act. In a considerable number of cases, though it is clear the person making the request has concerns regarding the processing in question, we are not provided with sufficient information to enable us to make an assessment but are able to provide authoritative advice. Such cases, where we provide written advice, are counted as enquiries. These are to be distinguished from requests from data controllers for advice regarding their own compliance. Alleged breaches of the Telecommunications Regulations are not technically requests for assessment but are included in our caseload figures.

The total of requests for assessment, and those ‘complaints’ where an assessment is not made but which are recorded as enquiries, may be broadly compared with the annual totals of complaints received under the DP Act 1984. The annual total of some 8,875 requests for assessment and enquiries the office had dealt with by the 31 March 2001 (including 1,721 complaints of breaches of the Telecommunications Regulations), therefore indicate a very significant increase in casework for compliance staff. Especially as this is in addition to work undertaken in closing 1,121 complaints received under the DP Act 1984.

### Complaints/requests for assessment received 1990 to 2001



\* Figures since 1994/95 refer to the financial year commencing 1 April and ending 31 March rather than using the previous reporting period for the Data Protection Registrar's Annual Report, which ran from 1 June to 31 May.

# This figure for the financial year 1999/2000 is based on the number of complaints received for the eleven months to 29 February 2000, adjusted to provide a twelve month estimate.

### Requests were received about

Consumer Credit	24.5%
Telecommunications	16.6%
Direct Marketing	4.0%
Other	47.9%

A proportion of requests for assessment from individuals require our compliance teams to ask for further information from the individual and from the organisation concerned. This, along with the varying complexity of the cases themselves, results in the time taken to undertake these assessments varying considerably.

Of the number of cases closed:

were open for 6–12 months	1.3%
were open for 3–6 months	3.2%
were open for 0–3 months	95.5%

### Outcome of cases

advice given	27.4%
request for assessment declined	3.9%
assessment criteria not met*	4.0%
unverified assessment suggesting compliance unlikely	2.5%
verified assessment suggesting compliance unlikely	1.3%
unverified assessment suggesting compliance likely	6.4%
verified assessment suggesting compliance likely	3.4%

\* The threshold criteria are:

- whether the request is made by or on behalf of a person who is, or who believes themselves to be directly affected by the processing in question;
- whether we are satisfied as to the identity of the person making the request;
- whether we can identify the processing in question;
- whether the processing is of personal data.

In deciding whether to make an unverified or verified assessment we will have regard to whether:

- the request raises, on the basis of the impact on the person making the request or on whose behalf the request is made and the wider impact, what we consider to be a matter of substance;
- the request is made without undue delay;
- the request is from a person who is entitled to make a subject access request in respect of the personal data in question;
- an assessment has previously been carried out in respect of the processing in question;
- the matters to which the request relates are being or could better be dealt with by another body or alternative mechanism;

- the matters to which the request relates have already been resolved;
- the issues raised by the request are fundamentally about data protection (rather than data protection being merely incidental to the main issues);
- an investigation by the Commissioner is likely to require resources disproportionate to the value of the assessment.

### **Assessments outstanding**

As of the 31 March 2001 there were over 750 cases received during the year in which action had been taken but not completed. In addition there were a further 700 cases in which no substantive action had, at that point, been taken. This backlog arose because during the year staff have had to deal with new legislation, following the coming into force of the DP Act 1998, and were at the same time faced with an increase in enquiries and requests for assessment. The oldest case awaiting attention at 31 March had been received about five months earlier. We are taking action to reduce delays and inconvenience, but there will continue to be delays in dealing with some cases while this takes effect.

### **Complaints outstanding**

There remain some 400 complaints made under the DP Act 1984 that remain under consideration. Some of these are with our investigation and legal departments for follow up action. During the year we closed 1,121 cases.

### **Investigations**

Depending on the outcome or where a criminal offence is alleged, complaints may be passed to our Investigations Department for further action. Our Investigators have made 715 visits to premises this year in the course of their investigations into alleged criminal breaches of the Act.

### **Search Warrants**

Applications were made, and no-notice search warrants granted, in respect of nine premises. Once again, the investigations concerned the unlawful procurement of information mainly by private investigators and tracing agents.

Investigations	Year	Year	Year
	98/99	99/00	00/01
Visits to business premises	700	388	480
Visits to dwellings	319	199	235
Witness statements obtained	433	346	355
Interviews under caution conducted	216	098	144
Cases considered for prosecution	215	125	129
Cases convicted	055	130	021
Cases acquitted		001	001
Cases withdrawn		009	001
Cases discontinued		005	–
Cases cautioned	002	002	012
Demands for access to premises	002	002	–
Search warrants obtained	010	011	009
Regional Investigators	006	005	007
HQ Investigators	004	002.5	003

### Prosecutions

129 cases were submitted to the Legal Department for consideration of prosecution, 23 cases were put before the courts and 21 of them resulted in conviction.

Those convictions comprised:

- 13 unregistered data users
- 04 cases of unlawfully procuring information
- 03 cases of employee of data user ‘disclosing’ data
- 01 case of employee of data user ‘using’ data for unregistered purpose

### Cautions Administered

- 06 unregistered data users
- 04 cases of unlawfully procuring information
- 02 cases of employee of data user ‘using’ data for unregistered purpose

The reduced number of convictions reported this year is not a reflection of a lower priority being put on investigations and prosecutions or a reduction in our investment in this area- indeed the opposite is true. The figure reported last year (99/00) of 130 convictions showed an increase on the figure of 55 recorded the previous year (98/99). This was largely due to one individual having 81 offences taken into consideration upon conviction.

The figure of 21 convictions for this year reflects three changes that have taken place:

1. The Commissioner's policy to reduce the priority in pursuing those unregistered data users who would not need to notify under the new Act.
2. The increased use of administering 'Cautions' as an alternative to prosecution (i.e. 12 this year as opposed to two last year).
3. The inception of, and work carried out in respect of, the BAIRD Project.

Prosecutions	1996/97	1997/98	1998/99	1999/00	2000/01
Number of offences brought to Court	67	38	59	145	23
Number of offences resulting in acquittal or withdrawn	8	0	4	15	2
Number of offences resulting in a finding of guilty	58	38	55	130	21
Number of cases resulting in caution	–	–	–	–	12

Convictions	2000/01
Unregistered data controllers	13
Cases of unlawfully procuring information	4
Cases of selling unlawfully procured information	–
Cases of data controllers using data for unregistered purposes	1
Employee for using data for an unregistered purpose	–
Data controller for disclosing data	3
Employee for disclosing data	–
Directors conniving offences by company	–

Enforcement	1996/97	1997/98	1998/99	1999/00	2000/01
Preliminary Enforcement Notices	6	19	7	5	5
Preliminary Enforcement Notices leading to Enforcement Notice	0	3	2	0	1
Enforcement Notices	2	5	5	1	4
Information Notices	–	–	–	0	0

**Prosecutions 1 April 2000 – 31 March 2001**

Defendant	Offence	Magistrates Court	Date of Hearing	Result	Sentence	Costs
Generic Software Consultants Ltd	5(1)	Milton Keynes	14/04/00	Guilty	£3000.00	£848.77
Xerox Imaging Systems UK Ltd	5(1)	Uxbridge	17/04/00	Guilty	£1000.00	£856.41
Baljinder Singh Dhand	5(2)(d)(3) x3	Highbury	19/05/00	Guilty	£1400.00	£646.25
Keith Hill	5(1)	Horseferry	25/05/00	Guilty	£200.00	£500.00
Digital Cellphones Plc	5(1)	Enfield	25/05/00	Guilty	£750.00	£352.50
Oluyemisi Akindele	5(6)	Highbury Corner	26/05/00	Guilty	£200.00	£400.00
Anthony Dunne	5(6)	Liverpool	07/06/00	Guilty	£250.00	£250.00
DataMirror UK Ltd	5(1)	Kingston N. Surrey	27/06/00	Guilty	£1000.00	£645.00
Research & Marketing Services Ltd	5(1)	Maidstone	11/07/00	Guilty	£2000.00	£500.00
Total Assist Recruitment Ltd	5(1)	Redbridge	18/07/00	Guilty	£100.00	£481.75
Robert Beecher	5(6)	Northampton	04/08/00	Guilty	Conditional Discharge 2 years	£250.00
Gregory Edward Fickert	5(1)	Birmingham	25/08/00	Guilty	Absolute Discharge	£500.00
UK Property Gold	5(1)	Cheltenham	09/10/00	Guilty	Conditional Discharge 12 months	£350.00
Reeds Rains Limited	5(1)	Trafford	12/10/00	Guilty	£800.00	£250.00
Training Direct UK Ltd	5(1)	Trowbridge	10/11/00	Guilty	£450.00	£300.00
Greenstone Sales Marketing Ltd	5(1)	Bromley	14/12/00	Guilty	£250.00	–
Paul Kilikita	5(2)(b)	Bromley	14/12/00	Guilty	£250.00	£1000.00
Sterling Travel Insurance Services Ltd	5(1)	Stockport	10/01/01	Guilty	£1000.00	£250.00
Sandra Cox	5(6)	Redditch	13/03/01	Guilty	Conditional Discharge 12 months	£250.00

In addition one case was discontinued on the administering of a caution.

In another case the defendant was acquitted upon trial.



## Notification Department Statistics

The Data Protection Register	1999 –2000	2000–2001
Registrations under the 1984 Act	–	
Notifications under the 1998 Act	–	
Total Register Entries	243,681	220,455
Registered Data Users	237,146	–
New Applications	25,012	52,642
<b>Renewals</b>		
Requests under the 1984 Act	38,354	3,987
Requests under the 1998 Act	–	
<b>Re-applications Submitted</b>		
Under the 1984 Act	8,220	–
Under the 1998 Act	–	–
<b>Requests for Amendment</b>		
Under the 1984 Act	25,047	17,863
Under the 1998 Act	–	2,351

## Output Measures and Performance Indicators

### Financial Years 1999/2000 to 2002/2003

#### Notification

	Actuals		Estimates and Targets	
	1999/2000	2000/2001	2001/2002	2002/2003
Number of weighted transactions processed	212,033	201,266	283,922	314,548
Number of weighted transactions processed per officer day	47.02	52.48	69.58 *	70.38 *

\* Dependent on increased staffing to handle current level of telephone calls.

There are three notification ‘products’ – new applications, and transformations (from DP Act 1984 renewals), renewals and changes. Each product is weighted in accordance with its processing time to year-on-year comparisons of performance to 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.

#### Assessments and Complaints

	Actuals		Estimates and Targets	
	1999/2000	2000/2001	2001/2002	2002/2003
Total requests for Assessment received	5,166	8,875	9,000	9,000
Not Investigated	2,227	57	–	–
Enquiries handled	–	4,408	4,750	4,750
No Assessment made	–	680	712	712
Sub-total	2,227	5,145	5,462	5,462
Investigated and Closed	1,812	1,063	350	80
Assessments completed	–	2,462	2,350	2,620
Sub-total	1,812	3,525	2,700	2,700
Number closed per Officer day	0.74	0.87	0.87	0.88

Currently there are still complaints being investigated (made under the provisions of the DP Act 1984).

Requests for assessment made under the DP Act 1984 are processed differently from complaints. From 2000/2001 the number closed per officer day figure encompasses complaints closed and assessments completed.

## Contact with our customers

	Actuals		Estimates and Targets	
	1999/2000	2000/2001	2001/2002	2002/2003
Telephone Enquiries received by the Information Line	55,070	55,125	55,250	55,500
Calls received per line hour	8.72	9.06	9.08	9.12

Contact is to all areas of the Office. Notification has its own dedicated enquiry line and media enquiries are initially dealt with by Marketing. Sector teams receive calls from data controllers and individuals with whom they have had previous contact. The Information Line handles all general calls, from controllers and individuals, and calls that have been transferred by the switchboard, currently these represent approximately 35% of the total calls received by the Office. Telephone enquiry figures represent the calls received by the Information Line. It is anticipated that the gradual implementation of the Freedom of Information Act 2000 will further increase workloads in 2001/2002 and 2002/2003. 'Line hours' are the hours spent by staff dealing with enquiries on the Information Line. The target figures for the 'calls received per line hour' are based on efficiency improvements being achieved year on year. An increasing number of enquiries are now received by e-mail, and 9% continue to be received as letters.

## Data Protection – Public Awareness

	Actuals		Estimates and Targets	
	1999/2000	2000/2001	2001/2002	2002/2003
% large data controllers aware of subjects' rights	77	85	82.0	83.0
% small data controllers aware of subjects' rights	58	63	52.0	54.0
% data subjects aware of own rights	14	27	25.0	25.0

## Freedom of Information – Awareness of Rights

	Actuals		Estimates and Targets	
	1999/2000	2000/2001	2001/2002	2002/2003
Amongst the public (percentage)	–	11	11	12
Within public authorities (percentage)	–	14	14	16

Notes:

Public Awareness and Awareness of Rights

The figures are based on annual tracking research in the spring of each year.

Freedom of information will begin to be phased in during FY 2002/2003 and will have a significant impact on the OMPs devised and set for that year. Anyone requiring more detailed statistics and information is welcome to apply to the Office.