Information Commissioner's Office

Information Commissioner's Annual Report and Financial Statements 2018-19

Report Presented to Parliament pursuant to Section 139(1) of the Data Protection Act 2018 and Section 49(1) of the Freedom of Information Act 2000 and Accounts Presented to Parliament pursuant to paragraph 11(4) of Schedule 12 to the Data Protection Act 2018.

Ordered by the House of Commons to be printed on 8 July 2019.

HC 2299

This publication is available at at www.gov.uk/official-documents

Any enquiries regarding this publication should be sent to us at

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

ISBN 978-1-5286-1409-2

CCS0619358894 07/19

Printed on paper containing 75% recycled fibre content minimum

Printed in the UK by the APS Group on behalf of the Controller of Her Majesty's Stationery Office

A Performance report

B Accountability report

C Financial statements

A Performance report

Information Commissioner's foreword

This report covers what has been an unprecedented year for the ICO. It is my third annual report as the United Kingdom's Information Commissioner, and covers an enormous amount of ground, from the introduction of a new data protection law, to our calls to change the freedom of information law, from record-setting fines to a record number of people raising data protection concerns. And all while we continue to grow an ICO that is efficient, focused and effective.

The biggest moment of the year was the General Data Protection Regulation coming into force. GDPR brings enhanced rights for the public, and the past year has been pivotal in public awareness of data protection rights. The doubling of concerns raised with our office reflects that.

The GDPR also brought in a step change in how organisations approach data protection. It increased the onus on organisations to take a proactive approach to data protection, identifying what risks they were creating through their use of data, and working to reduce and mitigate those risks. The greater enforcement powers granted to regulators helped to establish compliance as a board level issue.

The ICO responded to the new law with a comprehensive package to support organisations through the change. We published detailed guidance on our website. We had close to half a million conversations through our helpline, live chat and written advice service. We shared best practice at our annual Data Protection Practitioners' conference. Throughout the year, the ICO's experienced and expert team worked incredibly hard to provide the support we knew organisations needed. I am, as ever, enormously grateful to have such committed and capable colleagues.

So many of our conversations are around the use of personal data in digital services. It is early stages, but the GDPR has so far demonstrated that it is a law that can work alongside emerging technologies and creative approaches. There's no dichotomy between digital innovation and data protection. But progress relies on consumers trusting organisations with their data, and organisations stand at the front line on this. For our part, we are working on key guidance and codes, notably around internet harms and age appropriate design online, that we believe will increase this trust.

Our investigative work continues to hit the front pages. Over the year, we issued a record breaking total of monetary penalties – 22 fines totalling over £3m – as investigations continued into organisations breaching the Data Protection Act 1998. Our investigation into the use of data analytics for political purposes made the workings of Cambridge Analytica and Facebook a topic of conversation across the world, and prompted our report, Democracy Disrupted? calling for fundamental changes to how political parties lobby for your vote.

Our work combatting nuisance calls and texts continues to interest the public. We issued 23 monetary penalties under the Privacy and Electronic Communications Regulation, totalling over £2m. We also worked closely with the insolvency service, prompting the disqualification of would-be directors who may otherwise have looked to break the law again with new businesses.

Our work around the Freedom of Information Act also followed the trend of more interest from the public, and more action from us as a regulator. The number of cases we receive continues to grow, up to almost 6,500 cases over the past twelve months. We made improvements in the time it takes us to resolve cases, with almost two-thirds now closed within 30 days. And we laid an important report to Parliament setting out the case to extend the scope of freedom of information law to cover the work of private organisations providing a public function.

An unprecedented year, covering so much ground, requires an efficient and effective Information Commissioner's Office. We have grown in size, capability and ambition over the past year, our workforce grew from 505 to more than 700, with particular increases in the parts of the organisation handling data protection complaints and customer contact. We've increased our ability to deal with more complex areas, with a Technology Strategy supported by a new Executive Directorate for Technology Policy and Innovation.

I would, as I did in last year's foreword, express my appreciation for the continuing support and guidance of my Management Board – both executive and non-executive members. As Commissioner, I value their continual willingness to give me advice on topical issues.

I am grateful too, every day, for the commitment to quality public service from my staff, here in our headquarters in Wilmslow, and our offices in Edinburgh, Belfast, Cardiff and London. It is an honour to work with such dedicated staff. You may recall last year I spoke about the importance of pay flexibility in ensuring that we can retain our high performing staff while recruiting new talent, and I'm pleased to say we have been able to implement the first part of that work, followed by a career progression framework beginning in April 2019.

We have come to an end of a busy and crucial year for the ICO, and for information rights, but we look ahead to similar in the year ahead. I believe the wealth of valuable information and data in this report demonstrates the ICO's ongoing commitment to meet those challenges. We continue to be an effective information rights regulator for the UK.

Elizabeth Denham
1 July 2019

Our mission, vision, strategic goals and values

Our Mission

To uphold information rights for the UK public in the digital age.

Our Vision

To increase the confidence that the UK public have in organisations that process personal data and those which are responsible for making public information available.

Our Strategic goals

1. To increase the public's trust and confidence in how data is used and made available.
2. Improve standards of information rights practice through clear, inspiring and targeted engagement and influence.
3. Maintain and develop influence within the global information rights regulatory community.
4. Stay relevant, provide excellent public service and keep abreast of evolving technology.
5. Enforce the laws we help shape and oversee.
6. To be an effective and knowledgeable regulator for cyber-related privacy issues.

Our Values

Ambitious – Working boldly, ready to test boundaries and take advantage of new opportunities; working with a sense of genuine urgency, continuously improving when striving to be the very best we can be.

Collaborative – Working towards achieving our goals, supporting one another whilst seeking and sharing information and expertise and working effectively with a range of partners to achieve our collective objectives.

Service focused – Working impartially and ethically to provide excellent services – continuously innovating to remain relevant to the environment we regulate.

The legislation we regulate

Until 25 May 2018, the **Data Protection Act 1998** (DPA 1998) was in place and was therefore the data protection legislation the ICO regulated during the start of 2018-19.

As of 25 May 2018 the new **Data Protection Act 2018** (DPA 2018) and the **General Data Protection Regulation** (GDPR) both commenced, superseding the duties and obligations under the DPA 1998. The DPA 2018 and the GDPR built on and enhanced individuals' rights beyond DPA 1998, including the right to know what information is held about them and the right to correct information that is wrong. It also obliges organisations to manage the personal information they hold in an appropriate way.

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

The **Environmental Information Regulations 2004** (EIR) provide an additional means of access to environmental information. The EIR cover more organisations than the FOIA, including some private sector bodies, and have fewer exemptions.

The **Privacy and Electronic Communications Regulations 2003** (PECR) regulate the use of electronic communications for the purpose of unsolicited marketing to individuals and organisations, including the use of cookies.

The **Network and Information Systems Regulations 2018** (NIS) are derived from the European NIS Directive, which establishes a common level of security for network and information systems. These systems play a vital role in the economy and wider society, and NIS aims to address the threats posed to them from a range of areas, most notably cyber-attacks.

The **Infrastructure for Spatial Information in the European Community Regulations 2009** (INSPIRE) give the Information Commissioner enforcement powers in relation to the pro-active provision by public authorities of geographical or location based information.

The **Re-use of Public Sector Information Regulations 2015** (RPSI) gives the public the right to request the re-use of public sector information and details how public bodies can charge for re-use and license the information. The ICO deals with complaints about how public bodies have dealt with requests to re-use information.

The **Investigatory Powers Act 2016** (IPA) imposes duties on communications service providers in respect of the retention of communications data for third party investigatory purposes where they have been issued with a notice from the Secretary of State. The Information Commissioner has a duty to audit the security, integrity and destruction of that retained data.

The **Electronic Identification and Trust Services for Electronic Regulations 2016** (eIDAS) sets out rules for the security and integrity of trust services including electronic signatures, seals, time stamps and website authentication certificates. The ICO has a supervisory role towards organisations providing these trust services, including being able to grant qualified status to providers who demonstrate compliance with certain areas of the regulations and the ability to take enforcement action.

Introduction

In the first part of this document, we will report on our major work and achievements throughout 2018-19. This is divided into six sections:

- Implementing GDPR and DPA 2018;
- Our regulatory powers and actions;
- Freedom of Information;
- Collaboration;
- Facilitating innovation; and
- Resourcing

Throughout this section of the report, we identify how this work has contributed to achieving our six strategic priorities, set out on page 11.

Following this, we provide statistics covering the full range of our operational performance, followed by summary reports on our financial performance, sustainability and whistleblowing disclosures made to us. We then provide a statement on the ICO's status as a going concern.

In Part B, we report on our accountability, making declarations regarding corporate governance, remuneration and staffing, and parliamentary accountability and audit reporting.

In Part C, we report on our financial performance, through our financial statements.

Our major achievements and work this year

Section 1: Implementing GDPR and DPA 2018

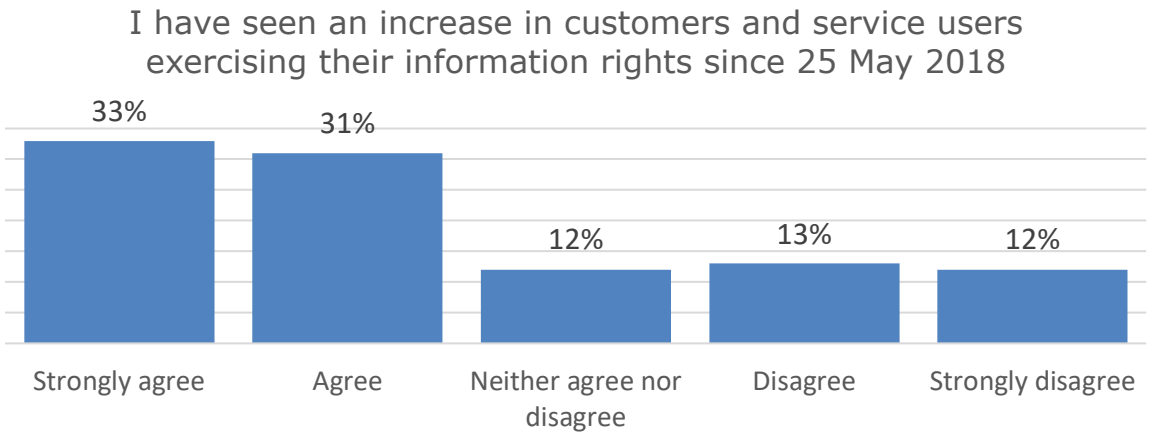
Supporting the public

The first year of GDPR and DPA 2018 saw people wake up to the potential of their personal data. This led to greater awareness of data protection law, in particular the data rights of individuals, and greater awareness of the role of the regulator when these rights aren't being respected.

Goal 1: increase the public's trust and confidence

In July 2018 our research found that one in three (34%) people have high trust and confidence in companies and organisations storing and using their personal information – significantly up from the 21% stating this in 2017. This is a welcome rise, which could be attributed to GDPR and DPA 2018, but further research will be needed over time to assess this. We will be conducting a further survey in July 2019.

In March 2019 we surveyed data protection officers, and 64% stated that they either agreed or strongly agreed with the statement "I have seen an increase in customers and service users exercising their information rights since 25 May 2018."



We supported this increase in awareness through our "Your Data Matters" campaign. This ongoing campaign aims to increase awareness of the enhanced data protection rights individuals have under the GDPR and DPA 2018, highlighting how people can exercise these rights and promoting our online guidance products. This campaign, along with the increased awareness of GDPR and DPA 2018, has led to a significant increase in visits to our website: during 2018-19 we had 17.5m sessions on our website (a 58% increase on 2017-18) from 9.5m users (a 72% increase). The most viewed products were our guide to GDPR and data protection self-assessment toolkit.

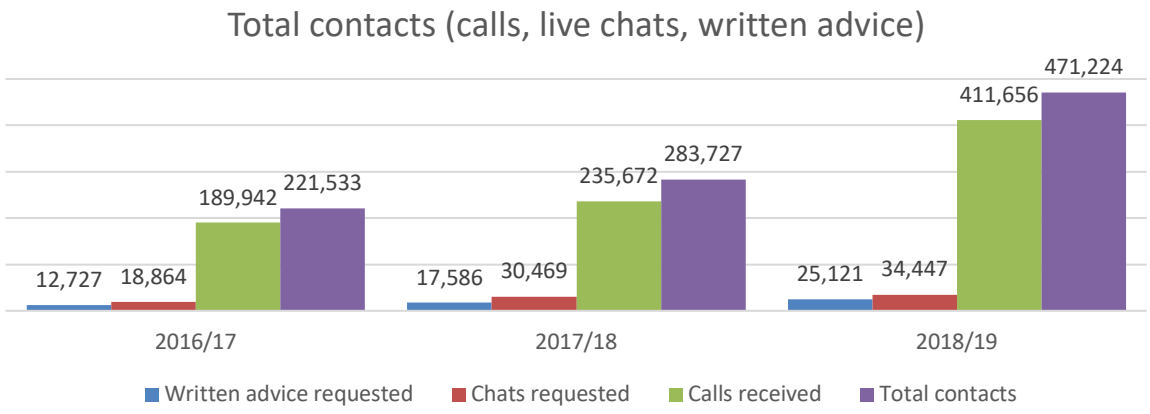
We've been working to support the public throughout the year. We support the public directly through our many expanded public-facing services (like our helpline and live text service), as well as providing organisations with indirect support through the various tools we have made available for companies, small or large, to explain the new laws and rights. We have also launched a number of 'own motion' investigations, which help the public to become more aware of how their data is being used. These allow us to, for example, highlight and address otherwise opaque or invisible processing of personal information. We have used these 'own motion' investigations to look into data protection practices which concern us as a regulator, but which have not yet been the subject of significant public complaints.

Supporting Data Protection Officers (DPOs)

The big push to be ready for GDPR and DPA 2018 prompted organisations to make significant changes. They determined the legal basis under which they collected personal data, inventoried the data they held, examined how data was used in their supply chains and refreshed their consents.

Goal 1: increase the public's trust and confidence

The volume and nature of our contact and engagement with businesses, organisations and individuals reflected this heightened engagement with the rights and responsibilities in the new regime. Our helpline, live chat and written advice services received 471,224 contacts in 2018-19, a 66% increase from 2017-18 (283,727 contacts).



We recognise that GDPR and DPA 2018 have placed a significant responsibility on DPOs, bringing with it the ongoing challenge of normalising the new regulations and embedding them as "business as usual" in their organisations.

Goal 2: improve standards of information rights practice

One avenue through which we do this is through our Data Protection Practitioners' Conference (DPPC), held each April in Manchester. Each year at the conference, we recognise exceptional performance by DPOs through our ICO Practitioner Award for Excellence in Data Protection. The nominations this year demonstrated the creative and dynamic way this community of privacy professionals have responded to the challenges of GDPR and DPA 2018.

We presented our 2019 Practitioner Award for Excellence in Data Protection to Mikko Niva, of Vodafone Group Services Ltd. Mr Niva delivered a pioneering privacy compliance programme for Vodafone, not just in the UK, but across 21 different countries. He also took a leadership role outside of Vodafone, speaking on privacy at a range of conferences during the year. The award to Mr Niva followed on from the 2018 winner, Esther Watt, Data Protection Officer at North Kesteven Council. Ms Watt led a programme for the council to ensure a smooth and positive transition towards GDPR and DPA 2018 compliance.

The Practitioner Award for Excellence in Data Protection helps to demonstrate some of the great work being done throughout the UK to embed the principles of GDPR and DPA 2018 into organisations. We hope to continue to receive such high quality nominations in 2019-20 and beyond.

The Award also shows the benefits of organisations having an embedded DPO with the right support. The challenges which DPOs face every day means that having the seniority and engagement from board level is critical to their success. Resourcing these roles needs to be a key priority for all organisations.

When we surveyed DPOs as part of our Data Protection Practitioners Conference, the responses showed that the majority of DPOs felt that they received support from within their organisation. The key findings of this survey were:

- 74% of DPOs said they were satisfied or very satisfied with the airtime they get with the senior leadership at their organisation with data protection issues. This is particularly encouraging as culture was considered to be one of the biggest issues for implementing the GDPR and DPA 2018.
- 90% of DPOs either agreed or strongly agreed that their organisation had an accountability framework in place.
- 61% of DPOs reported that the accountability framework was well understood within their organisation.

Clearly this is positive progress in under a year, but maintaining momentum will be key. There is still a long way to go to truly embed GDPR and DPA 2018 and to truly understand the impact of the new legislation – in our survey nearly 50% of respondents reported that they had faced unexpected consequences as a result of GDPR and DPA 2018. In 2019-20 we will continue to work to support organisations in dealing with all aspects of GDPR and DPA 2018.

Supporting small and medium-sized enterprises (SMEs)

Goal 2: improve standards of information rights practice

Beyond the data protection officer community, we recognise that it hasn't been easy for small organisations to become compliant with GDPR and DPA 2018. Legal bases for processing, data auditing and privacy policies take time to understand and there are no quick fixes for making sure people's personal data is being processed legally. This has been particularly difficult for sole traders.

To help this vital community to understand their data protection responsibilities, we provided a suite of resources, support and guidance on our website, tailored to the needs of sole traders and small organisations including toolkits and checklists, podcasts and FAQs. We offered a dedicated helpline and live chat service for further help and advice, and held advisory sessions attended by hundreds of SMEs.

In addition to these services, we are currently exploring establishing a "one-stop shop" for SMEs within the ICO. This department will draw together expertise from across our regulatory teams to help us better support all SMEs, particularly those without the capacity or obligation to maintain dedicated in-house compliance resources.

Helping organisations to embed GDPR and DPA 2018

Goal 2: improve standards of information rights practice

During 2018-19 we put comprehensive guidance in place, the Guide to GDPR, which helped organisations with the process of embedding GDPR and DPA 2018 into their work. This guide was supported by blogs, building on the success of our early 'myth busting' advice. We continued to add significant content to this guide throughout 2018-19, on areas such as contracts, DPA exemptions and encryption. We also produced an interactive tool for organisations to understand the lawful bases for processing.

Our GDPR guidance has been heavily used by organisations around the world throughout 2018-19. During 2018-19, it has had over 15 million views on our website.

We also continue to engage with trade bodies and other sector groups throughout the UK, to provide input into specific advice and guidance they produce and provide policy input into strategic data protection issues.

Goal 3: influence the global information rights community

Later in the year, we produced a tool to assist with the continued flow of data in the event of a no-deal EU Exit. This tool will be helpful to UK organisations, as well as organisations outside of the UK who deal with UK organisations. The tool has received good feedback from international counterparts within the European Data Protection Board (EDPB) and was the basis for the EDPB's own UK EU Exit guidance. This tool is still available to help organisations to prepare for the UK's exit from the EU, whenever and under whatever circumstances that happens.

We also produced an in-depth Guide to Law Enforcement Processing for those who have day-to-day responsibility for data protection in organisations with law enforcement functions. It was important to support those covered by the new EU Law Enforcement Directive in the year after the implementation of that Directive.

In 2019-20, our focus in this area will be to update existing guidance and ensure we continue to provide a clear and comprehensive guide to the law. We will also continue to provide new areas of support for organisations and continue our series of 'myth busting' blogs.

Drafting statutory codes

Goal 1: increase the public's trust and confidence

Goal 2: improve standards of information rights practice

During 2019-20 we will deliver the four statutory codes of practice which we are required to produce under the DPA 2018. These codes will focus on age appropriate design, data sharing, direct marketing, and data protection and journalism. During 2018-19, significant work went into the preparation of these codes.

These statutory codes are vital, because the Information Commissioner, courts and tribunals are required to take account of any relevant provisions within the statutory codes in any matters brought before them.

Code 1: Age Appropriate Design Code

A key concept of the GDPR is that children merit special protection. This code will help to achieve that by setting out the standards of age-appropriate design which we expect providers of online services and apps to meet when their services are likely to be used by children or when they process children's personal data. This is a key example of how important and effective data protection by design can be. The code builds on a set of minimum standards to be taken into account, which were provided by Parliament.

We consulted on this code during April and May 2019 and received over 400 responses. This followed on from an initial call for views from June 2018 to September 2018. We also engaged with parents, carers and children to better understand their views. The code will be laid before Parliament after the comments from the consultation have been reviewed and carefully considered.

Code 2: Data Sharing Code

Goal 2: improve standards of information rights practice

The Data Sharing Code will update our existing data sharing code of practice, which was published in 2011 under the DPA 1998. Data sharing brings important benefits to organisations, citizens, residents and consumers, making their lives easier and helping with the delivery of efficient services.

One of the myths of GDPR is that it prevents data sharing. This isn't true. The GDPR and DPA 2018 aim to ensure that there is trust and confidence in how organisations use personal data and ensure that when organisations share data they do so securely and fairly. Clear guidance for data controllers is vital for this, so that individuals can be confident that their data is shared securely and responsibly.

A call for views on the data sharing code closed in September 2018. We are currently considering the views presented to develop a draft code for formal consultation. We expect to launch that consultation in summer 2019 and for the code to be laid before Parliament in the autumn.

Code 3: Direct Marketing Code

Goal 2: improve standards of information rights practice

The Direct Marketing Code aims to ensure that direct marketing continues to be a useful tool for organisations to engage with customers in order to grow their business or publicise and gain support for causes, while avoiding it being intrusive and ensuring that all activities are compliant with the GDPR, DPA 2018 and the PECR.

We are currently considering feedback from the call for views, which closed in December 2018. This will inform a draft code, which we expect to consult on in summer 2019 and finalise by the end of October. Once the new European Union e-privacy regulation is completed, we may also produce an updated version of the code, if appropriate, to ensure that UK organisations have the best possible guidance on how to comply with the GDPR and DPA 2018.

Code 4: Data Protection and Journalism Code

Goal 1: increase the public's trust and confidence

Goal 2: improve standards of information rights practice

The Data Protection and Journalism Code aims to help the media to strike a balance between privacy, respect of individuals' rights, and freedom of expression. The code aims to provide clear and practical guidance on what data protection law requires to achieve this. This builds on guidance we produced under the DPA 1998 in response to the Leveson Inquiry. We will also be working collaboratively with the press regulators to ensure that the code fits within the wider framework for the industry.

A call for views on this code took place in April and May 2019. We are currently in the process of reviewing the views presented and developing a draft code for formal consultation. We expect to launch that consultation in the summer and lay the code before Parliament later in the year.

Under section 177 of the DPA 2018, we were required to produce and publish guidance about how an individual may seek redress against a media organisation where they consider that their personal data has been misused in the course of journalism. We made our redress guidance publicly available in May 2019 as part of our "Your Data Matters" resources.

Guidance: Use of personal data in political campaigns

In addition to the four statutory codes set out in the DPA 2018, we are developing guidance for the use of personal data in political campaigns. This work emerged from our Democracy Disrupted? report, which was published in July 2018, following our investigation, under the DPA 1998, in to the use of personal data in political campaigns. While we have previously produced guidance on political campaigning, the investigation demonstrated the need for stronger guidance, as parties and campaign groups now increasingly use personal information and data analytics to target and influence voters.

Goal 1: increase the public's trust and confidence

Goal 2: improve standards of information rights practice

Goal 5: Enforce the laws we oversee

Our position is that this guidance should be given statutory footing as a code of practice under the DPA 2018, so that it has the same legal status as the other four codes. We have called on Parliament to legislate to this end, and continue to do so.

The guidance is vital to retain the trust and confidence of the electorate in the democratic process, ensuring that all personal data used in political campaigns is used in a way which is transparent, understandable and lawful. The guidance will explain how to do that; giving it the statutory footing of a code of practice will increase its power.

The guidance will apply to all organisations who process personal data for the purpose of political campaigning (activity relating to elections or referenda, in support of, or against, a political party, a referendum campaign, or a candidate standing for election).

A call for views on this guidance closed on 21 December 2018. We are currently considering the views presented to develop draft guidance for formal consultation. We expect to launch that consultation in the summer.

Section 2: Regulatory powers and actions

Regulatory Action Policy

Goal 5: Enforce the laws we oversee

Raising awareness and providing support and guidance to organisations is a key part of our role, but we have not hesitated to act in the public interest when organisations wilfully or negligently break the law. Enforcing the GDPR and DPA 2018 is not just about big fines. It is about using all the tools set out in our Regulatory Action Policy. We laid this policy before Parliament in July 2018 and received approval in November 2018. The objectives for our regulatory action, which we set out in the policy, are:

- We will respond swiftly and effectively to breaches, focusing on those involving highly sensitive information, adversely effecting large groups of individuals, or those impacting vulnerable individuals.
- We will be effective, proportionate, dissuasive and consistent in our application of sanctions, targeting our most significant powers on organisations and individuals suspected of repeated or wilful misconduct or serious failures to take proper steps to protect personal data.

- We will support compliance with the law, including sharing information in relation to and otherwise contributing to the promotion of good practice and providing advice on how to comply with all aspects of legislation.
- We will be proactive in identifying and mitigating new or emerging risks arising from technological and societal change.
- We will work with other regulators and interested parties constructively, at home and abroad, recognising the interconnected nature of the technological landscape in which we operate and the nature of data flows in the expanding digital economy.

In this policy we set out how we will use our enhanced powers to pull back the curtain on processing where the public have concerns, for example social media companies, political parties, data brokers and the use of new technologies by law enforcement agencies. We also explained the factors which we will consider when deciding the extent of regulatory action to take.

Goal 1: increase the public's trust and confidence

Our regulatory powers and actions

We are increasingly using our powers to change behaviours. We have tools at our disposal and will use these to ensure that individual rights are upheld and that organisations comply with the law.

Goal 2: improve standards of information rights practice

Under the GDPR and DPA 2018, we are able to issue formal assessment notices to any organisation, either public or private. Under the DPA 1998 the Commissioner only had compulsory audit powers in respect of central government and health organisations. Otherwise companies had to agree to an audit. Now we have the power to issue assessment notices. With these new powers of inspection, we have been able to proactively respond to complaints from the public about unsolicited marketing communications and unfair and unlawful processing. We have issued 11 assessment notices under the new law, in conjunction with our investigations into data analytics for political purposes, political parties, data brokers, credit reference agencies and others.

We have also taken significant action through enforcement notices, particularly in two priority investigations. Enforcement notices compel the data controller in question to comply with data protection laws within a specified time. The first of these investigations started in October 2017, when we began an investigation in relation to the Metropolitan Police Service's (MPS) 'Gangs matrix'. We understood the policing requirement for the matrix, but our investigation found a range of serious infringements of data protection law that would undermine public confidence in the matrix and how the data was being used. For example, we had serious concerns about the way data was being shared with other organisations and about data that should not have been on the matrix at all. MPS responded positively to the requirements of the enforcement notice, working to provide safeguards for sharing information, taking the steps we required to increase security and accountability and to ensure that the data was used proportionately. The enforcement notice provided a clear incentive and way forward for MPS to become compliant, increasing its transparency and improving public confidence in this challenging area of policing.

Goal 5: Enforce the laws we oversee

Goal 1: increase the public's trust and confidence

The second investigation was in relation to Her Majesty's Revenue and Customs (HMRC) and their Voice ID service for customer identification. Our investigation found that HMRC had failed to give customers sufficient information about how their biometric data would be processed and failed to give them the chance to give or withhold consent, breaches of GDPR and DPA 2018. The enforcement notice required HMRC to delete all biometric data held under the Voice ID service for which they did not have explicit consent. New technologies, including biometric technology, can bring substantial benefits to organisations and the public, but the enforcement notice showed that they must be used appropriately and in a way that the public can be clear and confident about.

Goal 2: improve standards of information rights practice

We have also issued organisations with warnings and reprimands across a range of sectors including health, central government, criminal justice, education, retail and finance. We have issued 11 information notices which have allowed us to progress our investigations and inform our action. We now have the ability to issue urgent information notices, which will assist fast-moving investigations.

Goal 5: Enforce the laws we oversee

As part of our investigation into the use of personal data in political campaigns (launched under the DPA 1998), we requested a warrant, which meant it took 17 days from the outset to gain access to Cambridge Analytica's premises. With GDPR and DPA 2018, our powers have broadened and we now have greater control and flexibility over powers to help this type of situation. 'No-notice' assessment notices mean we are now able to have access to companies' data protection practices faster than under the previous legislation.

While GDPR and DPA 2018 caught the headlines, the majority of our completed investigations during 2018-19 took place under other legislation. For personal data breaches which pre-dated 25 May 2018, this was the DPA 1998. Many of our investigations are complex and time-consuming, so while there were no monetary penalties under DPA 2018 in 2018-19, there were many under DPA 1998.

In fact, 2018-19 was a record-breaking year of monetary penalties under the DPA 1998. We issued 22 monetary penalty notices (MPNs) for breaches of the DPA 1998, with fines totalling £3,010,610, including two fines of £500,000 (the maximum permitted under DPA 1998 and our highest ever fines). Some of the largest MPNs issued during 2018-19 were:

- £500,000 fine against Equifax Ltd, relating to a cyber security incident which effected the personal data of up to 15m UK citizens and residents.
- £500,000 fine against Facebook Ireland Ltd, relating to a serious data incident affecting the personal data of an estimated 87m Facebook users worldwide. This is currently being appealed.
- £385,000 fine against Uber, relating to a cyber security incident effecting the personal data of 2.7m UK Uber users and 82,000 UK Uber drivers.
- £325,000 fine against the Crown Prosecution Service, for losing unencrypted DVDs containing recordings of police interviews.

- £250,000 fine against Yahoo! UK Services Ltd, relating to a cyber security incident effecting the personal data of approximately 500m Yahoo! users worldwide.

Fines received by the ICO as a result of its MPNs are returned to the Treasury Consolidated Fund, rather than being retained by the ICO.

Protecting democracy

Goal 1: increase the public's trust and confidence

Goal 4: relevant; excellent service; abreast of evolving technology

As mentioned earlier in this report, in May 2017 we launched a formal investigation into the use of data analytics for political purposes, after allegations were made about the 'invisible processing' of personal data and the micro-targeting of political adverts during the 2016 EU referendum.

The investigation eventually broadened and has become the largest investigation of its type by any data protection authority. It has involved social media online platforms, data brokers, analytics firms, academic institutions, political parties and campaign groups. As a result of the investigation, in July 2018 we published 'Democracy Disrupted?', a ground-breaking policy report into the use of data analytics in political campaigns. At the same time, we published a progress report setting out the findings, recommendations and actions from our investigation into data analytics in political campaigns. We published a further update report into this investigation in November 2018.

Goal 5: Enforce the laws we oversee

We issued a fine of £500,000 against Facebook, the maximum possible fine under the DPA 1998 and the largest fine that we have issued to date. When issuing the fine, we stated that the fine could have been higher under the new legislation. This fine is currently being appealed by Facebook.

As part of this investigation, we issued the first enforcement notice under DPA 2018 to Aggregate IQ, a Canadian data broker. In the enforcement notice we ordered the company to delete certain personal data it held about UK citizens and residents.

Goal 1: increase the public's trust and confidence

Alongside this action, in the Democracy Disrupted? report we made a series of recommendations that, through their implementation, were designed to restore the trust and confidence of electorates and the integrity of the election process. As mentioned earlier in the report, one of the key recommendations was the need for a statutory code of practice on the use of personal data in political campaigns. Through the other recommendations, we sought to improve transparency and protect personal data and information rights in political campaigning.

We have continued to promote these messages throughout the year, particularly in some of the Information Commissioner's speaking engagements, including a speech at the European Political Strategy Centre on election interference in the digital age, presenting evidence to the International Grand Committee on disinformation and "fake news", and speaking at the European Data Protection Supervisor's Europe Votes event on unmasking and fighting online manipulation.

We have also engaged with the major social media companies to help them to comply with the relevant data protection legislation. We have also engaged with universities on the appropriate use of personal data in research projects.

Other major investigations

Goal 5: Enforce the laws we oversee

The investigation into the use of data analytics for political purposes was not our only major investigation during 2018-19. We devoted considerable resources to some wide ranging investigations, led by our new High Priority Investigations and Intelligence Directorate. Case studies of some of these investigations are set out below. We expect to provide further information on a variety of ongoing investigations as they are completed.

Case Study One: Use of Mobile Phone Extraction for Policing Purposes

We initiated an investigation after receiving a complaint from Privacy International. Privacy International raised their concerns about the policing practice of extracting data from mobile phones and whether it was compliant with Data Protection legislation. The complaint sought action from the ICO, including a review of the practice of using mobile phone extraction and using our powers to require the Data Controllers to comply with the Data Protection Act.

Through the investigation we aimed to identify current mobile phone extraction practices, focussing on lawfulness and fairness of the data processing of individuals' data, whether from suspects, victims or witnesses. The investigation used a multi-disciplinary approach, combining expertise from technologists, investigators and policy officers in order to effectively investigate across the key themes of this case. The investigation has benefitted significantly from meaningful engagement with key stakeholders, including working with victims' groups and representatives, the police, the Crown Prosecution Service (CPS), and the Attorney General's Office.

The challenges around digital evidence are broader than mobile phone extraction, and we will continue to act to ensure that where these issues extend beyond data protection, they are nevertheless seen through a data protection lens.

Case Study Two: victims' data

We initiated this investigation following complaints from a number of organisations representing victims, who raised concerns that police investigations into rape and serious sexual offences resulted in breaches to the complainants' right to privacy, which was having an effect on complainants' confidence in reporting crimes to the police. The concerns raised indicate that a key contributing factor to this issue is the requirement for victims of rape or serious sexual assault to "consent" to police obtaining copies of medical records, education records, psychiatric records, social service records and family court proceedings records at the start of the investigation.

Whilst this investigation is separate to the mobile phone extraction investigation, many of the concerns and issues that arise are shared across both cases, most central of which is the requirement to maintain and enhance public confidence in how personal data is used in police investigations.

The investigation aims to identify how data of complainants is processed through the criminal justice system in cases where rape and serious sexual offences are being investigated.

The issue under investigation has also been identified by government, policing and support organisations. There are a number of parallel investigations by other government or public bodies being conducted in order to tackle the significant concerns regarding public confidence, and issues relating to the right to privacy and right to a fair trial in prosecuting rape and serious sexual offences. We are working closely with the Victims Commissioner, Association of Police and Crime Commissioners, Attorney General's Office, Ministry of Justice, Home Office, CPS, NPCC and Police Authorities

The aims of the investigation mirror those in the case above but in addition look to work alongside key stakeholders to ensure data protection law is a central consideration in investigative and prosecution decision making.

Case Study Three: live facial recognition technology

We have highlighted our concerns regarding the potential for misuse of facial recognition technology and the need to ensure Data Protection Law is adhered to when using this technology. This issue is one of our regulatory priorities and this investigation seeks to shape our response to the emerging use of this technology by a large volume of law enforcement, public sector and private sector bodies.

Through our investigation we attended a variety of deployments by police forces in pilot stages, in order to identify current practices and how the police envisaged that facial recognition technology capabilities could be used in opportunities in the future. Our investigation findings will enhance our policy in this area and also seeks to increase the public's trust and confidence in how this data is used and made available.

We intervened in the recent judicial review brought by Liberty against South Wales Police to ensure that the data protection issues of this case were appropriately explained and considered by the court: data protection principles provide key safeguards for the police and the public when facial recognition technology is deployed. We are awaiting the judgement and look forward to working with partners on publication.

Intelligence

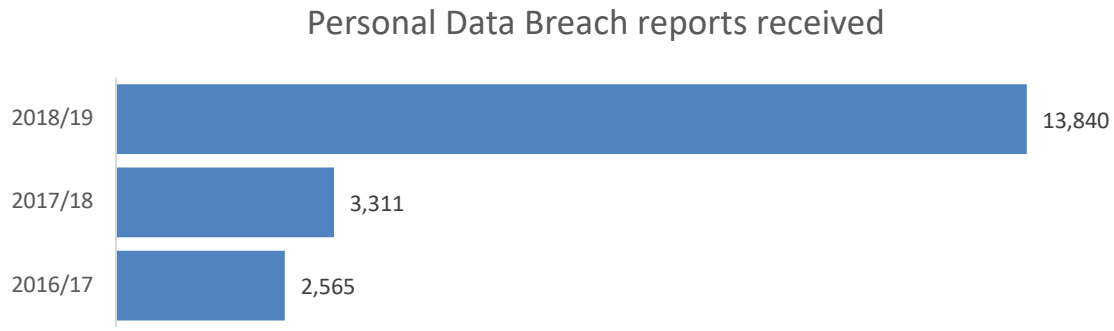
To make sure that our investigation and enforcement work is targeted in the right areas, we developed an Intelligence Strategy to set out how we use the information we gather. One important piece of work in this area is using the information we receive from the public and other sources to inform a strategic threat assessment, which will support all of our work, including investigations, enforcement, guidance, codes of practice and more. This includes information from personal data breach reports, complaints reported to us by the public and working with other regulators. The first iteration of this was completed in May 2019, and we plan to repeat this work at six-monthly intervals, which ensures that we are well-informed of and can respond to any emerging threats to information rights.

Personal data breaches (PDBs)

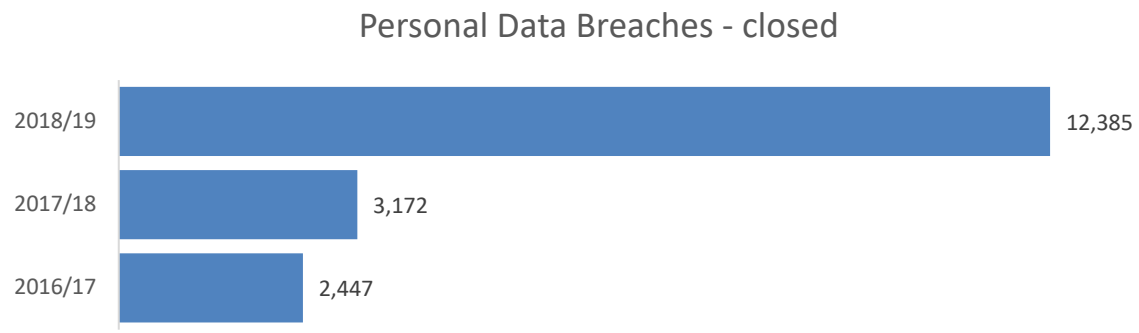
GDPR and DPA 2018 strengthened the requirement for organisations to report PDBs. As a result, we received 13,840 PDB reports during 2018-19, an increase from 3,311 in 2017-18.

Goal 2: improve standards of information rights practice

Some organisations have had to make changes to meet the higher standards required under GDPR and DPA 2018 and the introduction of mandatory breach reporting. This has required increasing staff awareness to enable them to recognise breaches and react appropriately. However, many organisations were already doing this before the introduction of GDPR and DPA 2018 and have not needed to make significant changes. The significant increase in breach reporting demonstrates that organisations are taking the requirements of the GDPR and DPA 2018 seriously and it is encouraging that these breaches are being proactively reported to us.

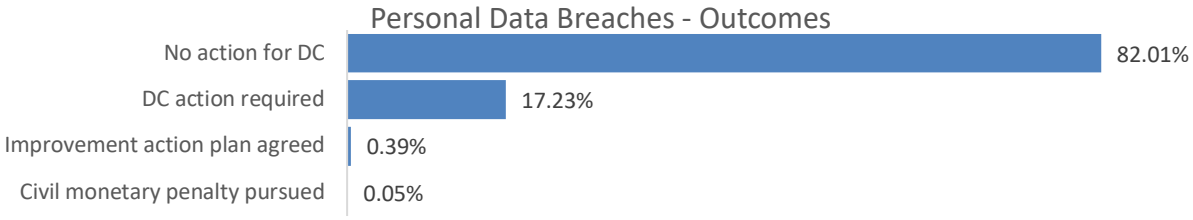


We closed 12,385 breaches during the year, compared to 3,172 in 2017-18. We assess all reported PDBs and will take action in relation to the more serious breaches, in line with our regulatory action policy. When determining what, if anything, should happen next, we consider factors such as the cause of the breach, the detriment to affected individuals, the sensitivity of the data and the remedial measures taken by the controller to address the incident and prevent recurrence.



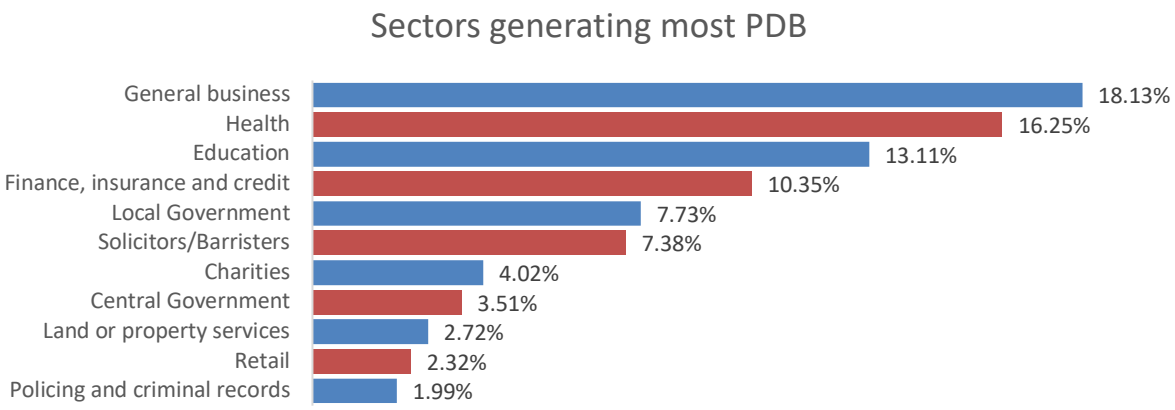
In 82% of the cases we have assessed, we have determined that the organisation had measures in place or was taking steps to address the breach without further action being required by the ICO. Where appropriate, we offer advice and recommendations to help the data controller to improve their information rights practices and prevent a recurrence of a similar breach.

In 17% of cases, we required that data controllers take further action. Only a very small minority of cases (less than 1%) led to action beyond that. That could consist of improvement action plans, further investigations audit visits, or civil monetary penalties being pursued.



*Note: an additional 0.3% of PDBs closed with the following outcomes: investigation pursued, audit visit recommended, DPA 1998/2018 not applicable, or data controller outside the UK.

Many PDB reports come from sectors that handle large volumes of personal data. In some sectors, there is a strong correlation between the volume of reports received, the sensitivity of the data and awareness of reporting thresholds. For example, reporting can be higher where there are dedicated DPOs and well-developed breach reporting processes.

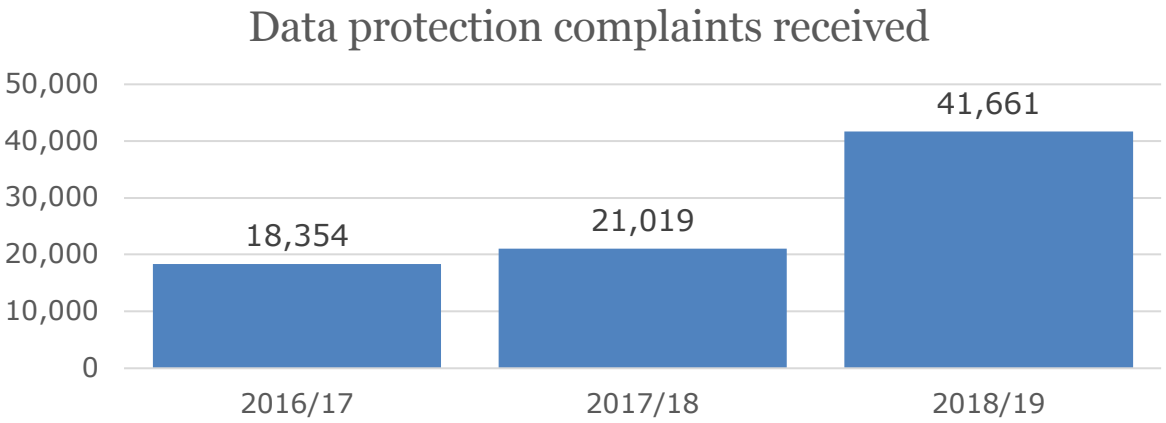


In 2019-20 we will continue to work with data controllers in the UK and with other Data Protection Authorities to understand how best to support organisations to be compliant with the breach reporting requirements of the GDPR and DPA 2018 in a way that best helps protect data subjects.

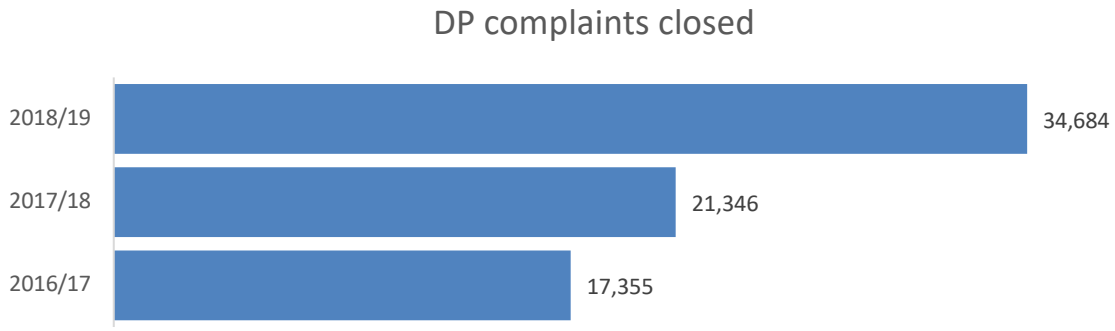
Responding to public complaints

In 2018-19 we saw a significant increase in the number of data protection complaints reported to us by the public. During 2018-19, we received 41,661 data protection complaints from the public. In 2017-18 we received 21,019 data protection complaints.

Goal 1: increase the public's trust and confidence



We closed 34,684 complaints in 2018-19, compared to 21,364 in 2017-18.

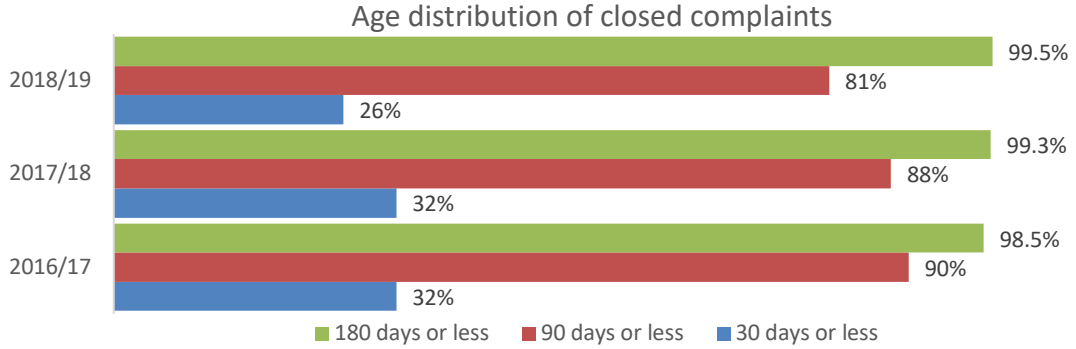


This means that we carried forward a sizeable caseload of 9,503 data protection complaints into our new reporting year, compared to 2,522 complaints at the end of 2017-18.

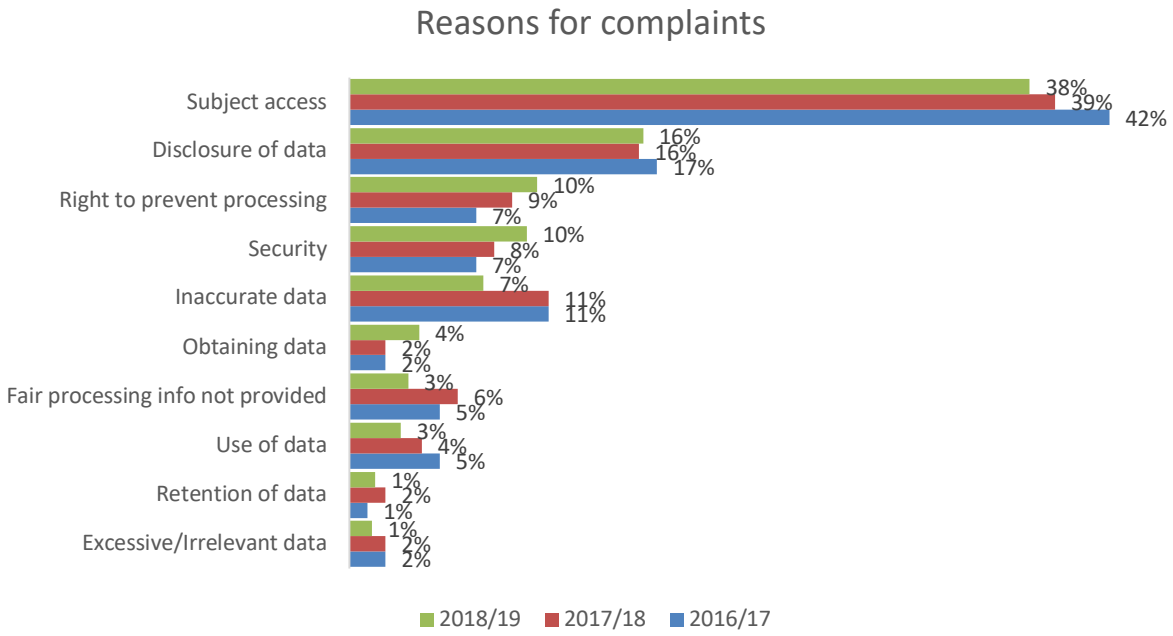
Given the volume of data protection complaints received during 2018-19, delivery against our target of closing 99% of complaints within six months has been a momentous challenge. By redeploying resources from across the ICO and agile working, we have been able to maintain strong performance against our six-month resolution target by closing 99.5% of complaints within six months, up from 99.3% in 2017-18.

The challenge that we face for 2019-20 is sustaining this new, much higher demand for our service. Therefore, to ensure that we can maintain service standards for the public, we have plans in place to reduce our open complaints across 2019-20 to below 5,000 open complaints by the end of the reporting year. We plan to achieve this by working with data controllers to support them to be compliant with data protection legislation, to help them to better understand the GDPR accountability principle and, when appropriate and proportionate to do so, take regulatory enforcement action against data controllers who breach data protection legislation.

We also plan to deliver further improvements to our processes, systems and IT so that the data protection complaints process is as streamlined as possible, enabling us to identify premature complaints at the earliest opportunity and provide an improved customer experience.



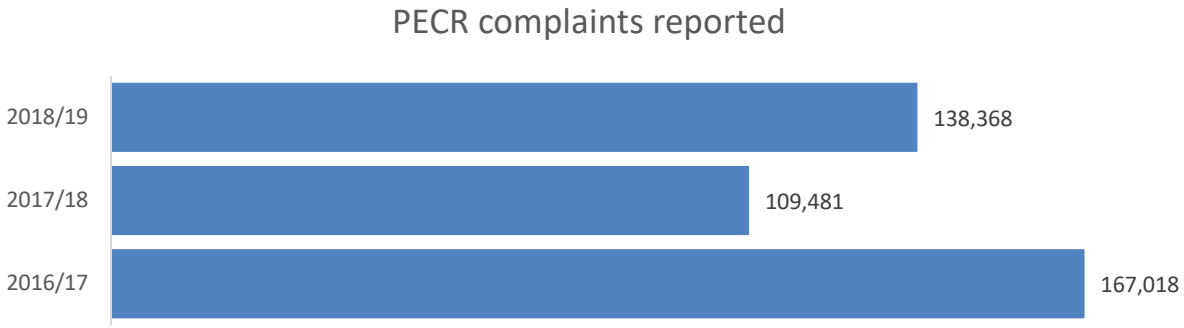
In terms of the types of complaints received, subject access requests (SARs) remain the most frequent complaint category, representing 38% of data protection complaints we received. This is similar to the proportion before the GDPR and DPA 2018 (39%). In fact, the general trend is that all categories of complaints have risen in a similar proportion to the overall number of complaints.



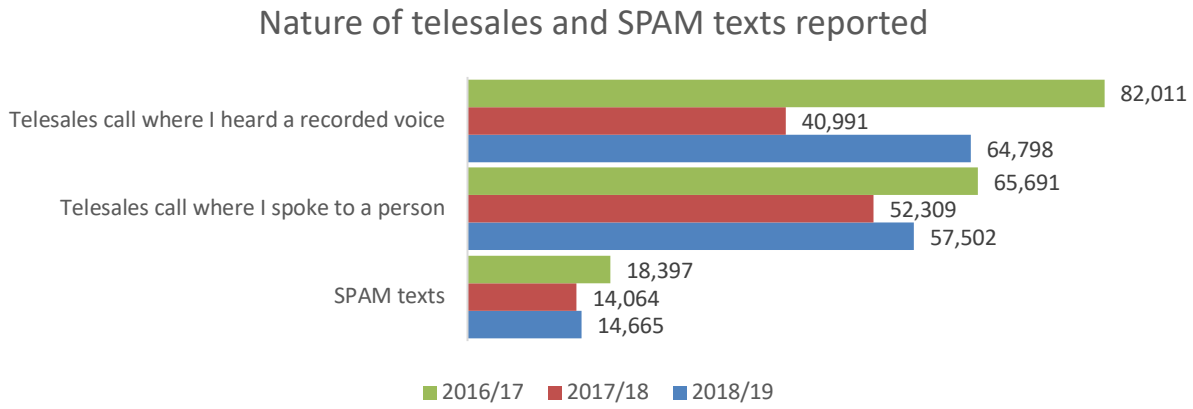
Privacy and Electronic Communications Regulations (PECR)

During 2018-19, we received 138,368 complaints under PECR (up from 109,481 in 2017-18).

Goal 5: Enforce the laws we oversee



14,665 of these complaints related to spam texts, 57,702 to telesales calls with people, and 64,798 to telesales calls with recorded voices.



During 2018-19, we issued 23 monetary penalties for violations of PECR, totalling £2,053,000.

Goal 2: improve standards of information rights practice

Over the last few years we have observed that a common tactic for companies subject to significant fines under PECR has been to liquidate the company to avoid paying a fine, potentially then forming a new company that conducts the same practices. We have worked with the Insolvency Service to disrupt this. So far, as a result of ICO investigations, the Insolvency Service has been able to disqualify 16 people from serving as a director, for a total of 107.5 years. In December 2018 we received further support for this area of our work, through an amendment to the PECR legislation to allow us to make directors personally liable for fines. The legislation did not allow retrospective action to that end, so there have not been any such fines to directors so far. We also welcomed legislation which banned cold calling regarding pensions from January 2019.

Since December 2016 we have had statutory responsibility for the Telephone Preference Service (TPS), the central opt-out register for people to record their preference to not receive unsolicited marketing calls. The service is currently provided by TPSL. Following the completion of a procurement exercise, a new contract for the delivery of the service will be issued later this year.

Goal 1: increase the public's trust and confidence

As at May 2019, there were over 18.5 million numbers on the TPS Register and 2.2 million numbers on the Corporate Register. Over 616,000 people registered with TPS in 2018-19. TPS also provides a way for members of the public to raise a complaint if they have registered their number and subsequently receive unsolicited marketing calls. In 2018-19, TPS received 52,503 complaints.

Under these arrangements, the ICO is able to monitor service delivery to ensure that the TPS is effective in providing members of the public and companies with an accessible way of registering their preference to not receive unsolicited marketing calls. We will be investigating how technology can offer improvements to the scope of services currently available. We currently receive complaint information and information on emerging risks or trends quickly, enabling us to take prompt regulatory action to disrupt organisations and individuals who are involved in making unsolicited direct marketing calls in breach of the requirements of PECR. We will continue to review arrangements for the provision of information to best inform our assessment of risks and threats, and regulatory action that we take in relation to privacy and data marketing.

Providing assurance

Goal 2: improve standards of information rights practice

To improve information rights compliance in both organisations and in specific sectors, during the year we undertook 27 consensual data protection compliance audits and four to assess compliance with PECR, providing advice and recommendations. We also undertook 14 follow-up audits checking that recommendations we had made previously had been acted upon. In addition we undertook 89 advisory visits with a particular focus on SMEs and charities.

We use workshops to promote good practice, in conjunction with partner organisations, to provide advice and guidance based on the findings from our audits. We held three workshops aimed at SMEs and 'Umbrella' bodies engaging with around 150 organisations. We also communicate outcomes based on audit findings in order to ensure wider dissemination of good practice with reports produced on the charities and high education sectors and Central Government departments.

Accountability

Goal 2: improve standards of information rights practice

Promoting accountability is one of our strategic priorities. GDPR introduces the accountability principle into law, making it clear that data controllers are not only responsible for complying with GDPR but demonstrating it as well.

Codes of conduct and certification schemes are two mechanisms that can help organisations evidence their accountability, either by demonstrating how specific processing activities are compliant via certification or by agreeing between categories of controllers what the practical application of GDPR is in particular areas and signing up to adhere to that via a code of conduct. The ICO is charged in the GDPR with encouraging these.

We have carried out work internally to develop the processes to formally receive codes and schemes for consideration from autumn 2019. At the end of April we launched new webpages, inviting organisations to engage with us in both of these areas.

Network and Information Systems (NIS) Regulations 2018

Goal 4: relevant; excellent service; abreast of evolving technology

The NIS Regulations came into force in May 2018. Therefore, 2018-19 was a year of embedding these regulations in to the UK economy. As the competent authority for relevant digital service providers (RDSPs), we commenced a programme of work to ensure we would be able to deliver our regulatory functions under the new legislation.

Goal 2: improve standards of information rights practice

We produced a new piece of guidance, "The Guide to NIS", to assist RDSPs in complying with the requirements of the NIS Regulations. We published this in initial form in May 2018 and in longer, more detailed form in October 2018.

The NIS Regulations require RDSPs to register with the ICO. We established a process to enable this registration to take place. Combined with our outreach and engagement activities, over 120 organisations are now on the register.

We undertook engagement and outreach activities, including workshops held at TechUK, aimed at increasing awareness among RDSPs and relevant stakeholders of the NIS Regulations and our associated guidance.

Goal 3: influence the global information rights community

We also joined the EU NIS DSP Competent Authorities Working Group, which comprises the competent authorities for digital services providers from across the Member States. We have attended a number of meetings of this group and have contributed to a number of key topics and have also presented our investigative experience to other EU regulators.

Cyber-related privacy issues

Goal 6: be a knowledgeable regulator for cyber-related privacy

The NIS regulations are a key strand of our work to be an effective and knowledgeable regulator of cyber-related privacy issues. A key part of this work in 2018/19 was the establishment of a new Technology Policy and Innovation Executive Directorate (further information on this is provided later in the report). Around 2,500 cyber security incidents were reported to us during 2018-19. The most common types of incidents were phishing attacks (44% of incidents) and unauthorised access (29% of incidents).

Cyber-security is at the heart of some of the biggest personal data breaches that we have been investigating during the year. Three of the major fines mentioned earlier in this report (those assessed against Uber, Yahoo! and Equifax) were as a result of failures in cyber security. During 2018-19, some of our major investigations under GDPR and DPA 2018 have also been related to major cyber security failures: the hack of Marriott International, which exposed the personal data of 500m customers worldwide; the hack of British Airways, which exposed the personal data of 380,000 passengers; and the hack of Cathay Pacific which exposed personal data of 9.4m passengers. Investigations into these data breaches are currently ongoing, but they highlight the importance for all organisations of ensuring they have strong cyber security.

Throughout 2018-19, we have worked closely with the National Crime Agency (NCA), National Cyber Security Centre (NCSC) and the Department for Culture, Media and Sport (DCMS) in this area. We have also spoken at CyberUK on data security and data privacy in April 2018 and April 2019 and at techUK's annual Digital Ethics Summit (we plan to speak at this event again in December 2019).

Goal 2: improve standards of information rights practice

Section 3: Freedom of Information

Openness by Design and Outsourcing Oversight

Goal 2: improve standards of information rights practice

In January 2019 we launched our draft access to information strategy, 'Openness by Design' for public consultation. In this draft strategy, we set out our medium-term goals in relation to the freedom of information legislation we regulate. An important part of our approach is to increase our focus on compliance and enforcement. The Information Commissioner launched this consultation with a speech at the Parliamentary Internet, Communications and Technology Forum (PICTFOR).

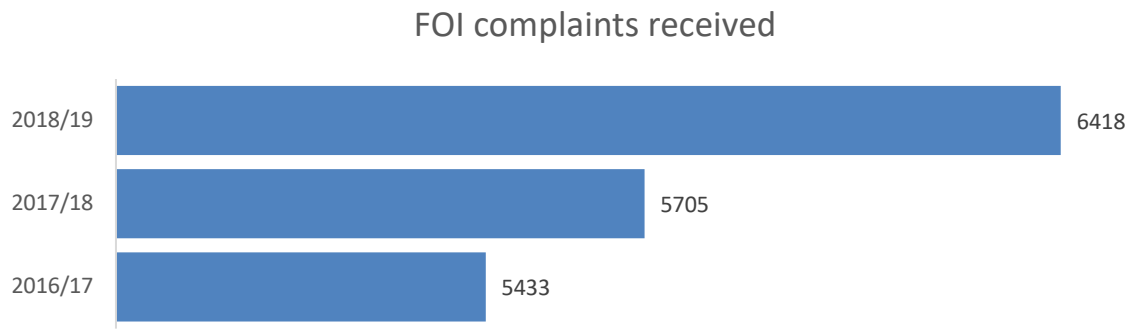
Goal 4: relevant; excellent service; abreast of evolving technology

During 2018-19 we laid an important report before Parliament, 'Outsourcing Oversight?' setting out the case for change to the scope of the FOIA and the EIR. Given the fundamental changes in the way public services are commissioned and delivered, our report makes the case for expanding the scope of FOIA and EIR to cover the work of private organisations providing a public function. Change cannot wait until we see more cases like the collapse of Carillion or the tragedy of the Grenfell fire. In the report we argued that urgent action is now required and we are committed to working with Government and Parliament to achieve this report's vision of more accountable public services, regardless of how they are delivered.

Freedom of Information Act 2000 (FOIA) complaints

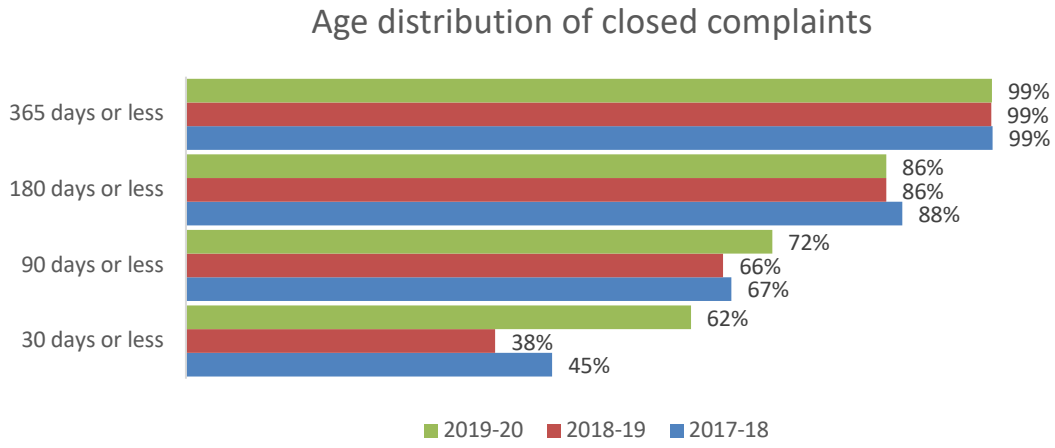
The ICO independently reviews decisions made by public authorities about requests for information under the FOIA and the Environmental Information Regulations 2004 (EIR).

The number of complaints we consider continues to increase, from 5,433 FOIA complaints in 2016/17 to 6,418 in 2018-19.



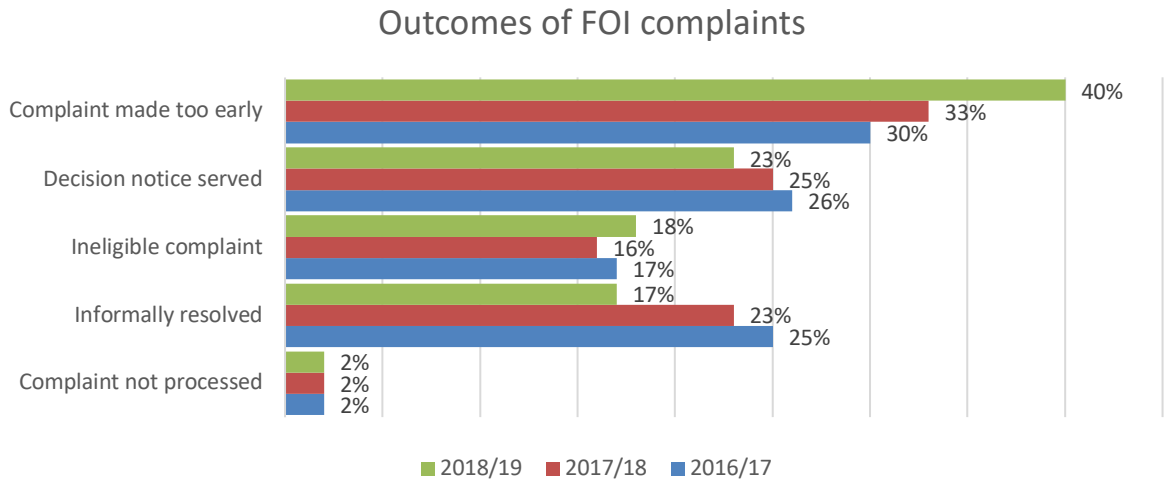
Despite the increasing complaint volumes, we were able to keep pace, closing 6,293 complaints during the year, an 8% increase on last year. We also made improvements in the time it takes to close complaints, with 62% of our FOIA complaints being closed within 30 days or less, compared to 38% in 2017-18.

Goal 1: increase the public's trust and confidence

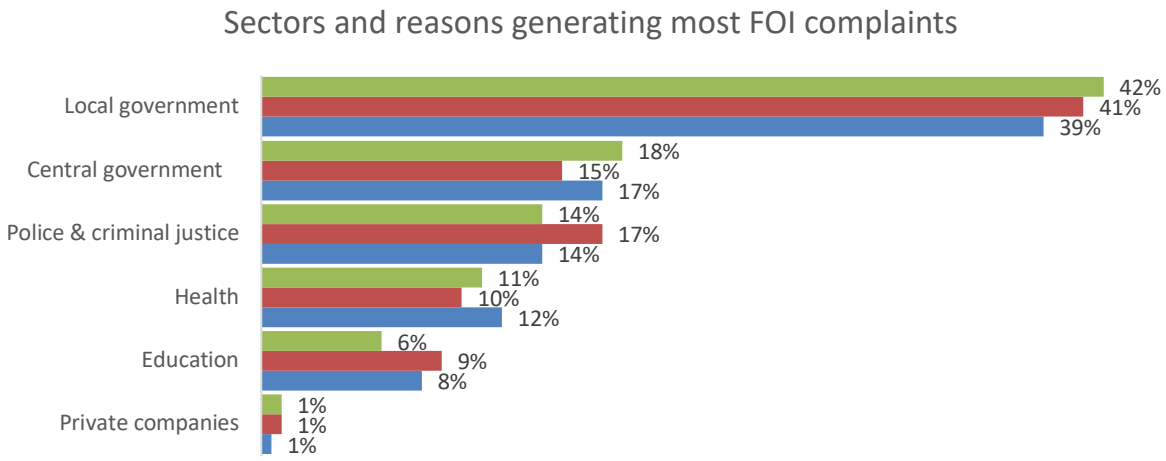


A growing proportion complaints we receive come to us too early. Sometimes this might be because the internal review procedures of a public authority have not been completed, or a complaint may be submitted without all the necessary information for us to progress it. Last year 40% of the queries we received were premature. During 2019-20 we will review our complaint handling processes to make sure people understand what to expect from us when they complain, to ensure that it is as easy as possible for people to bring a complaint to us.

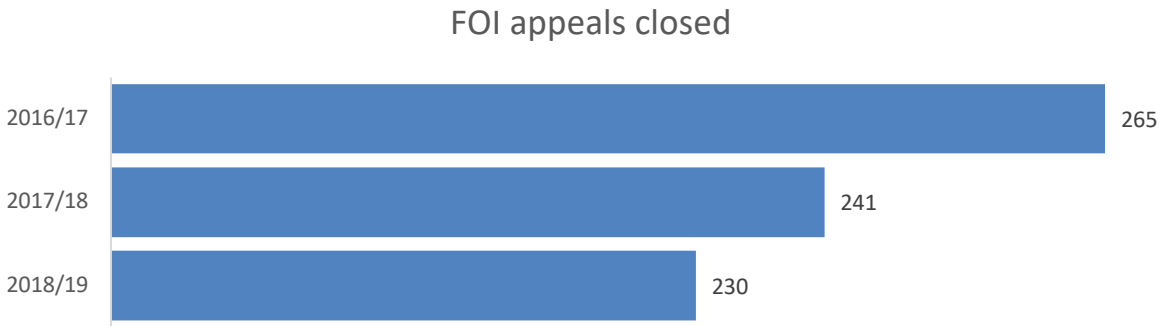
Goal 2: improve standards of information rights practice



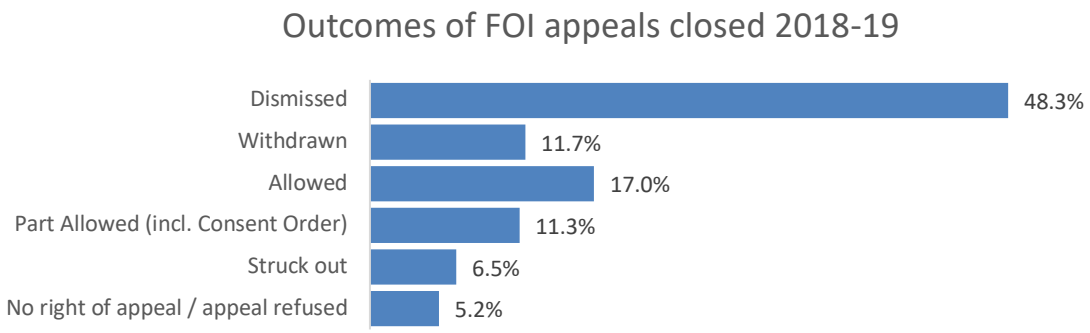
Local government has continued to be the sector which is the subject of most FOIA complaints, at 42%. This is a very high proportion of complaints even though local government authorities represent a relatively low proportion of all public authorities, which reflects the level of interest in local decision making.



At the same time as receiving increased volumes and handling historic levels of FOIA complaints, resulting in a record number of section 50 FOIA decision notices, we have seen a reduction in the number of decision notices being appealed. This has reduced from 281 in 2016-17 to 246 in 2018-19. This represents a reduction from 21% of decision notices being appealed in 2016-17 to 17% in 2018-19.



Over 70% of First Tier tribunal appeals against our decision notices have been successfully defended during 2018-19.



This year has seen a number of technical issues being explored in the Tribunal. In Kirkham v IC [2018] UKUT 126 (AAC) the scope of the section 12 FOIA "appropriate costs" limit was being examined by the Upper Tribunal in the context of increasingly sophisticated electronic records management systems. This is an area which will doubtless come before the Commissioner and Tribunal again.

In August 2018, the Commissioner issued a decision notice which considered the correct application of the Environmental Information Regulations, finding that Poplar Housing & Regeneration Community Association was a public authority for the purposes of those Regulations. That decision was overturned by the First Tier Tribunal and is currently subject of an ongoing appeal to the Upper Tribunal.

In March 2019, the Commissioner prepared the first set of proceedings for certification for contempt of court by a public authority issued under Section 54 FOIA and Rule 81 of the Civil of Procedure Rules and issued them in April. In that case, Information Commissioner v The University Council of the University of Southampton (CO/1635/2019) the Commissioner alleges that the public authority has failed to comply with an information notice issued under section 51 FOIA.

Section 4: Collaboration

Delivering our International Strategy

Goal 3: influence the global information rights community

We have a responsibility to protect UK citizens and residents, which means that we have to engage with our counterparts internationally on enforcement co-operation. In addition, the UK economy's digital trade means that data has to flow internationally with minimal cost or delay. Both of these matters require a data protection authority which has an international reach. GDPR enshrines this into law. This means that we have needed to commit significant resources during 2018-19 to build successful international relations, which allow us to protect the privacy of UK citizens and residents, promote and protect the UK and its role in the wider global digital economy, and influence the development of privacy regulation.

To deliver this responsibility, we have an International Strategy, published in 2017, which commits us to maintaining the strong links we have in the EU and beyond. It also sets out a clear vision of where we need to develop our capacity to co-operate on enforcement and to share best practice from international exemplars.

We have engaged with our EU partners to effectively deliver GDPR, which we have achieved through participation in the EU Data Protection Board and its various expert sub-groups (on subjects including technology, social media, regulatory co-operation, regulatory enforcement, borders, travel and law enforcement). We continue to grow and strengthen our links with the EU supervisory authorities to support ongoing data protection work, protecting the information rights of UK citizens and residents.

Preparations for the UK's withdrawal from the EU have made this international work even more important. This has been supplemented by regular bilateral meetings with key EU partners. We are confident that, in addition to providing guidance to UK businesses in the event of a no-deal exit, this will enable strong regulatory co-operation throughout Europe following the UK's EU exit.

Addressing the reality that the digital economy is a global phenomenon, that data has no borders and in anticipation of the UK's EU exit, we have also devoted significant resources to building our relationships and influence outside the EU. The ICO has taken a prominent role in a number of international networks. This includes:

- The International Conference of Data Protection and Privacy Commissioners (ICDPPC), which brings together around 120 data protection offices across the world. In October 2018, the Information Commissioner was elected as chair of ICDPPC, giving the UK an ability to not just share policy and enforcement experience, but to take on a leadership role within the global privacy and information rights community.
- The International Conference of Freedom of Information Commissioners. In March 2019, the Information Commissioner chaired the conference, which ended with the adoption of the Johannesburg Charter. This will formalise governance and the ability of this forum to be a coherent voice on freedom of information issues globally, co-ordinating sharing of good practice, and enhancing the ICO's ability to learn from the rest of the world.
- The Asia Pacific Privacy Authorities (APPA), where we attended forum meetings in December 2018 and May 2019 (in New Zealand and Japan respectively). The Information Commissioner spoke at the forum meeting in New Zealand, on regulatory convergence and international collaboration. Following attendance at the APPA event in Japan in May 2019, the Information Commissioner delivered the closing keynote speech at a G20 side event on the topic of "International seminar on personal data". This topic is directly relevant to Japanese Prime Minister Abe's call for the G20 summit to be the start of a new focus on worldwide data governance. The Commissioner's speech, on the subject of interoperability of international data standards, was in line with Prime Minister Abe's call.

- The Common Thread Network (CTN), which we co-chair, brings together data protection and privacy regulators across commonwealth countries. We hosted an event on privacy, trust and the digital economy in the Commonwealth in April 2018 and will be representing CTN at the first African Regional Data Protection Privacy Conference in late June 2019 in Accra. This will give us the opportunity to promote data protection and privacy laws in Africa.
- The Global Privacy Enforcement Network (GPEN), which aims to increase co-operation in the enforcement of privacy laws across borders.

As well as developing working relationships with international colleagues, our work with these groups helps to ensure that UK data protection law and practice is a benchmark for high global standards.

We have also worked closely with the USA's Federal Trade Commission (FTC), giving evidence on international cooperation, competition, privacy and GDPR. We have also been working with the FTC to share our expertise to assist in the expansion of their data protection capacity and capability. This will continue to be a key relationship for us in years to come, particularly if the USA creates a new federal privacy law, which would clearly have a significant impact on the information rights of UK citizens and residents. We also worked with the Foreign and Commonwealth Office to inform the introduction of Brazil's proposed data protection law, which is expected to be closely related to GDPR. This included speaking at events in Brazil in April 2019.

In addition, we have developed international memoranda of understanding for information sharing for enforcement purposes, tactical exchanges of information and intelligence sharing. We have supported myriad investigations by other data protection authorities and received information in turn from other authorities to assist our regulatory work.

The scope of our international work is clear. This year we have reached key international partners to deliver our crucial goal of influencing the information rights agenda throughout a connected world and digital economy, for the economic and social benefits of UK citizens, residents and organisations. This will continue to be a key area of work during 2019-20 and beyond, particularly as data protection is likely to be an important factor in international trade deals after the UK's EU exit. Maintaining digital trust is key to both productive trade and data sharing.

Working with Parliament

Goal 2: improve standards of information rights practice

Closer to home, our work with Parliament and Government has increased year-on-year, enabling us to advise from as early a stage as possible in the development of policy and legislation. The Information Commissioner and members of her Executive Team appeared before Select Committees six times during 2018-19, to give evidence on a range of issues, including the use of personal data in Artificial Intelligence (AI), the spread of disinformation and "fake news", electoral campaigning and data transfers with Europe post-Brexit. These appearances were also supplemented by written evidence in relation to inquiries. We have also attended two All-

Party Parliamentary Groups (APPGs), where we have advised on personal data usage in AI, data analytics, electoral campaigning and fake news. We have also responded to a number of consultations from the devolved administrations, notably participating in oral evidence sessions of the Scottish Parliament's Justice Sub-Committee on Policing. In addition to this, we have regularly met with parliamentarians and government departments to discuss information rights matters.

We have been working with parliament to take steps to address the pressing issue of online harms. The Information Commissioner appeared before the DCMS Select Committee to discuss this issue in April and we will respond to the Government's white paper on the subject. As the regulator for the delivery of content online, when that involves personal data, we will continue to play a significant role in this space, maintaining our current remit and working alongside our fellow regulators to support them in their roles. However, despite this, we do not believe that we are the correct regulator to take responsibility for content moderation.

In addition to our discussions with Parliament, earlier in this report we discussed some of the areas where we are already working to tackle online harms. For example, the Age Appropriate Design Code, collaboration with other regulators, and working with organisations to develop compliant innovative technological solutions. Our Democracy Disrupted? work on electoral interference is also relevant to this area. We will continue to seek out other ways within our statutory remit to protect UK citizens and residents from online harms. We are committed to continuing to support the Government and fellow regulators in developing solutions to the issue of online harms and we look forward to engaging further on a number of the issues which we have highlighted.

We continue to work with a range of parliamentarians on a cross-party basis to raise the profile of information rights. We also provided expert advice to Government in relation to Brexit planning, including no-deal planning. We worked particularly closely with DCMS to provide expert advice on the draft Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019, the statutory instrument which will ensure that the legal framework for data protection within the EU continues to function correctly after the UK's exit from the EU. This legislation is now ready to be taken forward when appropriate. There has also been strong engagement throughout the year with the digital data and open data initiatives within the devolved administrations, to ensure that information rights are protected.

A key part of our work with Parliament has been around data analytics in political campaigning, including our Democracy Disrupted? report, which is discussed earlier in this report.

Goal 1: increase the public's trust and confidence

Working with domestic regulators and stakeholders

Goal 2: improve standards of information rights practice

On a national level we have continued to build strong relationships with other regulators, particularly with Ofcom, the FCA and the CMA. In 2019-20, we will further boost this by joining the UK Regulator's Network. These relationships not only support our enforcement and operational work, but also enable us to ensure that data protection and information rights are a key topic for all regulators. One part of our work in this area has been to convene the Regulators and AI forum, which will let regulators share best practice on regulating AI.

We have also worked with the Centre for Data Ethics and Innovation (CDEI), the Alan Turing Institute and TechUK as we build up our technology and innovation work. We have also advised the British Board of Film Classification (BBFC) on data protection implications of age verification solutions, as they develop their work on age verification in relation to access to online pornography. This is an important piece of work, given the potential privacy implications if high data protection standards are not applied in this area.

Section 5: Facilitating Innovation

Regulatory Sandbox

Goal 2: improve standards of information rights practice

Privacy and innovation are not mutually exclusive. Far from limiting or preventing these developments, we want to ensure that privacy is built into new products and services by design, enabling data protection good practice to become an essential aid to effective innovation. That is why in March 2019 we opened the regulatory sandbox for applications.

The sandbox, a first amongst data protection authorities, is an innovative new service to support organisations using personal data to develop products and services that are innovative and have demonstrable public benefit. This both supports innovation in the UK, and helps us better understand how organisations are finding new ways to utilise personal data. This new service will help us address emerging data protection risks to individuals, as they arise.

Goal 4: relevant; excellent service; abreast of evolving technology

The sandbox is a place where organisations are supported to develop innovative products and services using personal data in different ways. Participants will be able to work through how they use personal data in innovative projects with our specialist staff, to help ensure they comply with data protection rules. We expect that many of the products that will come into the Sandbox will be at the cutting edge of innovation and may be operating in particularly challenging areas of data protection where there is genuine uncertainty about what compliance looks like.

The application process closed in May 2019 with 64 applications received.

Regulators' Business and Privacy Innovation Hub

Goal 2: improve standards of information rights practice

In October 2018, we were awarded £537,000 of grant funding from the Department of Business, Energy and Industrial Strategy (BEIS) to provide data privacy expertise to other UK regulators, to ensure rules and regulations can keep pace with technologies of the future. This was as part of BEIS's £10m Regulators' Pioneer Fund.

This allowed us to create a Regulators' Business and Privacy Innovation Hub within the ICO, which will work in partnership with other regulators to provide expert support to businesses in information privacy and data protection, helping them to embed data protection by design and have the confidence to create innovative products and services.

This Hub works alongside the Sandbox to ensure that the ICO is able to embed strong data protection principles in to the development of innovative products and services throughout the economy.

Research Grants Programme

Goal 2: improve standards of information rights practice

We have previously reported on our Research Grants Programme, which includes £1m of funding to promote good practice and support innovative research on privacy and data protection issues. The first phase of grants were awarded in 2017-18 and have been progressing during 2018-19. In the first phase, we awarded grants to four organisations:

- Open Rights Group: Development of a website to help individuals protect and enforce their information rights, particularly in relation to privacy policies in the insurance and banking sectors.
- Teeside University: Development of a prototype software tool to capture patient privacy preferences to allow secure sharing of medical information to support research (as part of the Great North Care Record).
- London School of Economics: A project looking at children's information rights and privacy, particularly with regard to children's capacity to consent and the production of an accessible online toolkit for children, parents and teachers.
- Imperial College London: Development of an online tool for the public and organisations to evaluate the risk of re-identification of pseudonymised data.

In 2018-19, we selected four innovative research projects to receive a total of over £275,000 in funding for Phase 2. These initiatives were:

- Connection at St Martin's in the Field: A project to engage with homeless people in London to better understand their knowledge and awareness about how their personal information is used.
- Oxford University: A study of six smart homes to study current privacy preferences and to prototype new tools, interfaces, and approaches to smart home privacy.

- PHG Foundation: A project researching the nature of pseudonymised genomic data, its function as personal data under the GDPR and DPA 2018, uses in medical research and how any potential associated risks may be mitigated.
- Cardiff University: A project to develop a training programme for researchers working with a wide range of routine public sector data.

We look forward to reporting on the work of the second phase of grants projects in our 2019-20 annual report.

Explainability of artificial intelligence (AI)

Goal 4: relevant; excellent service; abreast of evolving technology

One of our key workstreams during the second half of 2018-19 has been to develop guidance on the explainability of AI, as requested by the government in the AI Sector Deal. This project has been brought forward in collaboration with the Alan Turing Institute under the banner of Project ExplAIn. The goal of this project is to create practical guidance to assist organisations with explaining decisions made by AI to the individuals affected.

This work included citizens' juries, conducted in conjunction with the Greater Manchester Patient Safety Translational Research Centre (GM PSTRC), who were conducting their own research into public perceptions of the use of AI in healthcare. We also held structured roundtable discussions with industry groups, with the co-operation of the Alan Turing Institute and techUK. This work provided an excellent opportunity for mutual collaboration to build strong results for all organisations involved.

We published an interim report on Project ExplAIn in June 2019 and we expect to publish a draft of the guidance for consultation during summer 2019. This project is just one part of our work to strengthen our knowledge of AI and machine learning, which has been led by our new Technology Policy and Innovation Executive Directorate. Further information on the work of this Directorate is provided later in the report.

Section 6: Resourcing

Growth of the ICO to meet demand

As the profile, responsibilities, powers and size of the organisation have increased, our funding has been reviewed to ensure we are well resourced to deliver its vital role. To ensure that we were able to meet the demands from DPA 2018, changes were made to the Data Protection Fee, which came into force with the DPA 2018. Details of this are set out within the financial summary later in this report.

In 2018-19, the number of organisations paying the Data Protection Fee increased by 16%, compared to a historical average yearly increase of 6%. However, due to the funding model change, this meant that our fee income increased by 84% in 2018-19 compared to 2017-18.

This has enabled us to invest in the capacity and capability of our workforce. During 2018-19 we increased our workforce from 505 to more than 700, an increase of 40%. We expect demand for, and interest in, our work to continue to increase into 2019-20. Therefore, we plan to further increase our workforce throughout 2019-20 and 2020-21, eventually taking us to an anticipated 825 full time equivalent staff in early 2020-21. This growth has had to be delivered at the same time at meeting the growth of our services outlined earlier in the report. In particular, we doubled the size of the Data Protection Complaints Directorate, which was already our largest department, and we more than doubled the size of our Customer Contact department.

As part of our overall expansion we appointed a new Senior Leadership Team, sitting below the Executive Team. This Team is made up of 13 Directors across the ICO, who are responsible for overseeing the delivery of the strategic direction set by the Information Commissioner, Management Board and Executive Team.

Increasing our capability in technology and cyber security

Goal 4: relevant; excellent service; abreast of evolving technology

Goal 6: be a knowledgeable regulator for cyber-related privacy

It is fundamentally important to our work that we keep pace with developments in technology and cyber security. The challenges are as real for us, as a regulator, as they are for those we regulate. As well as expanding our capacity to deal with the increased work, we have needed to increase our capability to deal with more complex areas.

Some of the most significant data protection risks to individuals, including cyber attacks, AI, cross-device tracking and machine learning, are now driven by the use of new technologies.

Last year we produced our Technology Strategy, which set out our plans in this area. During 2018-19, we took some significant steps to deliver that strategy. We established a new Executive Directorate for Technology Policy and Innovation and appointed Simon McDougall as the Executive Director, reporting directly to the Information Commissioner. Simon joined in October 2019, and has become a valuable member of the Executive Team and Management Board.

Simon has appointed skilled staff to a wide range of technology roles within the Technology Policy and Innovation Directorate. This included the appointment of Dr Reuben Binns (from Oxford University's Department of Computer Science) as our first postdoctoral research fellow for Artificial Intelligence, for a two-year term. During this term Dr Binns will research and investigate a framework for auditing algorithms (which we will publish in 2019-20) and conduct further in-depth research activities in AI and machine learning. Our work on AI is also informed by our "Project ExplAIn" programme, mentioned earlier in the report. In 2019-20 we will also establish a Technology Hub, bringing together technological expertise from across the ICO into one location.

This increased capability in technology has already been hugely beneficial, contributing heavily to our Age Appropriate Design Code, to protect children from harm online. As mentioned earlier in the report, this has also allowed

us to establish a Regulators and AI forum, to let regulators share best practice on regulating AI. This builds on the speech made by the Information Commissioner at the Politics of AI conference on data protection.

We have consulted extensively with industry to increase our understanding of advertising technology (particularly the use of personal data in real-time bidding) under GDPR and DPA 2018. This included a full-day fact-finding forum with participants from across the advertising technology industry. We have refined our understanding of this area and published an update report regarding real-time bidding during June 2019. We prioritised this work due to the risks this form of data processing presents to data subjects.

Goal 2: improve standards of information rights practice

High quality staff

To meet the challenges of the GDPR and DPA 2018 it was vital to recruit and retain staff with the right mix of skills and experience. We have different ways of attracting the right people, including developing secondments, apprenticeships and research fellowships. In addition, a review of our pay arrangements helped to mitigate the risks posed by uncompetitive pay.

Goal 4: relevant; excellent service; abreast of evolving technology

Flexibility in the way we pay our staff, which was agreed by DCMS and Treasury in 2017-18, is vital in allowing us to achieve recruitment and retention of high quality staff. This flexibility allows us, for a three-year period (from April 2018 to the end of March 2021), to determine the pay necessary to maintain the necessary expertise needed to deliver our regulatory priorities.

Our first step was to bring our pay levels more into line with the public sector average. This led to a 7% pay rise for all roles in April 2018.

The next step was to introduce a career progression framework to allow us to retain high quality staff and ensure they have the opportunity to progress within their role. This framework allows staff to progress in their existing roles, based on increased personal competence, contribution and impact within the role, and is aligned to the organisation's vision and values. The framework was implemented in April 2019 and we expect it to have significant benefits to staff development, satisfaction and retention.

As might be expected, training and development of our staff has been a key feature of 2018-19. This has been important for new staff, to ensure that they are fully aware of the legislation that we regulate, but also for existing staff, many of whom are in new roles and responsible for regulation of new legislation.

In 2018-19 we reviewed our People Strategy and established new corporate values, which we are embedding into everything we do. This will ensure that we maximise the benefits of our high quality staff. The values we established through this strategy are:

- Ambitious – Working boldly, ready to test boundaries and take advantage of new opportunities; working with a sense of genuine urgency, continuously improving when striving to be the very best we can be.

- Collaborative – Working towards achieving our goals, supporting one another whilst seeking and sharing information and expertise and working effectively with a range of partners to achieve our collective objectives.
- Service focused – Working impartially and ethically to provide excellent services – continuously innovating to remain relevant to the environment we regulate.

To embed the 'service focused' value, Professor Mark Colgate (Professor of Service Excellence at the University of Victoria) joined us for a week in February 2019. During that week, Professor Colgate hosted 20 workshops for all staff, to discuss what great service means and how we can go about providing this to all of our customers. Professor Colgate also recorded a session to ensure that all staff joining the ICO quickly understand our focus on service excellence.

At present, we are considering ways in which we can best align our staffing structures to embed service excellence into everything which we do.

Ensuring adequate resources

Goal 4: relevant; excellent service; abreast of evolving technology

In the short term, it is vital that we continue to be adequately resourced to deliver against our responsibilities under the DPA 2018. We will continue to grow the numbers of organisations paying the fee and push for every single organisation required to pay the fee to do so.

Goal 5: Enforce the laws we oversee

The DPA 2018 increased our ability to pursue non-payment of the data protection fee. Under DPA 1998 we could pursue this as a criminal offence, but under DPA 2018 we are now able to issue penalty notices for non-payment of the fee, up to a maximum fine of £4,350. Using this new power, we issued 3,335 notices of intent to fine (NOIs) for this during 2018-19, which led to 2,491 responses, with total payments of £585,490 in data protection fees. We have also issued 227 penalty notices following on from these NOIs. In 2018-19, 67 of those led to payment, leading to a further £99,170 in total fees and penalties.

Goal 2: improve standards of information rights practice

This process will continue in 2019-20, focusing on larger organisations. It is important to stress that an increase in the number of organisations paying the fee is not so that we have unlimited funding. We will continue to resource ourselves according to our goals. If the income from fees consistently outstrips our needs, it will bring the potential to reduce the fee for all organisations, reducing the burden for every organisation, but ensuring that burden is shared equally.

A risk to ensuring the ICO has adequate resources is the increased risk of contentious, complex and lengthy legal proceedings which has already started with the Facebook appeal as mentioned earlier in the report and is likely to continue to with the size of the fines that can be assessed under GDPR and DPA 2018.

Our existing funding arrangements are such that surpluses is remitted to the Treasury Consolidated Fund. However, it is very difficult to budget accurately for litigation costs, as the costs within any given financial year are dependent on a number of external factors which are increasingly difficult to predict.

We are currently exploring options to mitigate this risk. These options include ring-fencing fine income (as mentioned earlier in the report, this is currently returned directly to the Consolidated Fund) specifically to fund litigation costs, additional grant in aid, deficit budgeting, use of reserves, or seeking awards of costs through court proceedings. A key piece of work for 2019-20 will be to identify the way forward in this area.

Annex: Operational performance

This annex to our major achievements and work this year provides full statistical information of our operational performance during 2018-19. Last year we reported that our operational teams had done well to meet unprecedented demand and complexity. That has redoubled in 2018-19.

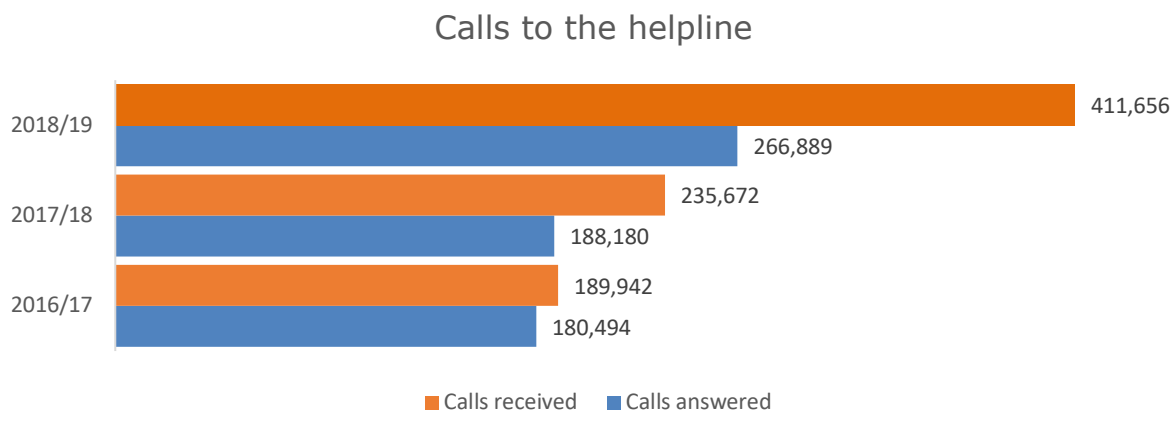
The following operational figures reflect the significant increases in output of our operational teams across the organisation: output from self-reported breaches is up by 290%; output from data protection complaints is up by 62%; and output from freedom of information complaints is up by 9%. This has been supported by the work of our customer contact service, which has had an increase of 66% in total contacts (and 75% in phone calls specifically).

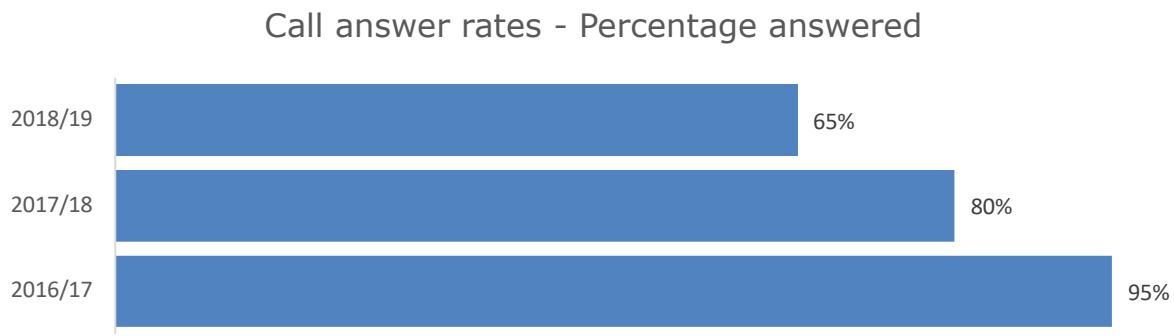
As set out earlier in the report, in most cases we have been able to keep pace with increased workload and caseloads have remained manageable. This was assisted by a temporary redeployment of some staff from September 2018 to January 2019 to meet the challenge of the increased number of data protection complaints and breach reports which we received. As our organisation has grown and our operational teams have gained experience we believe that we are now well-placed to meet this new, much higher demand for our service.

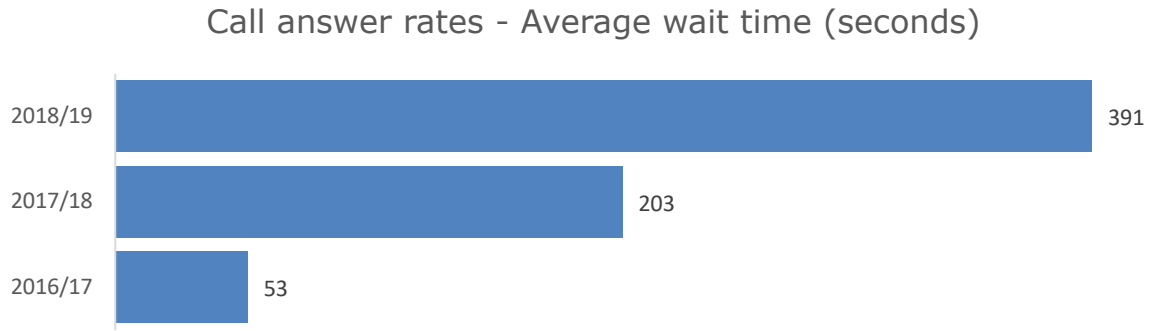
Further narrative on many of the individual statistics has been provided earlier in the report.

Advice services

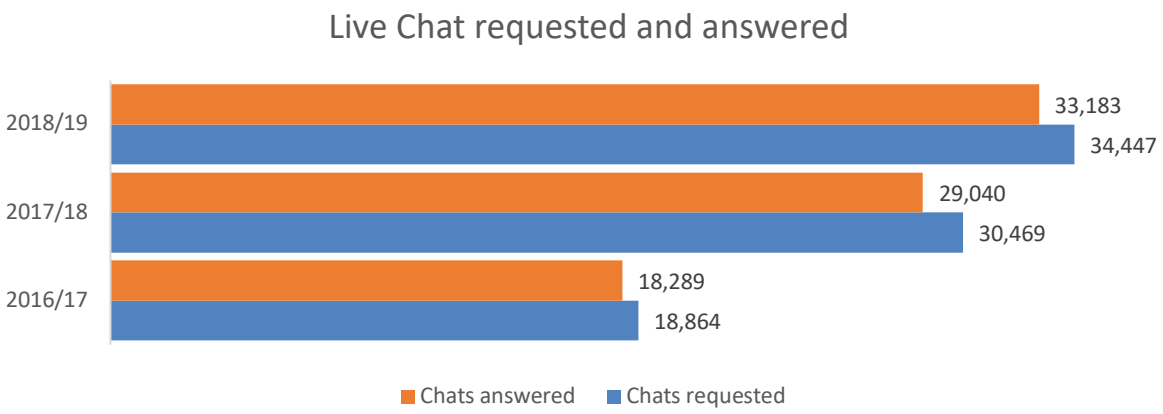
Calls to helpline

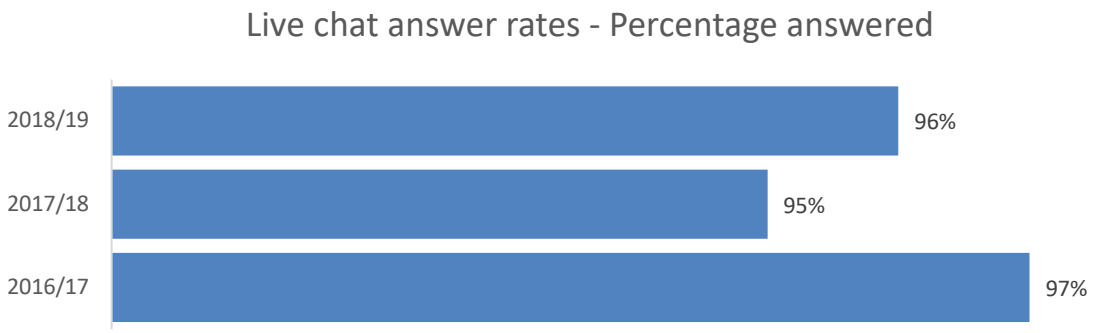


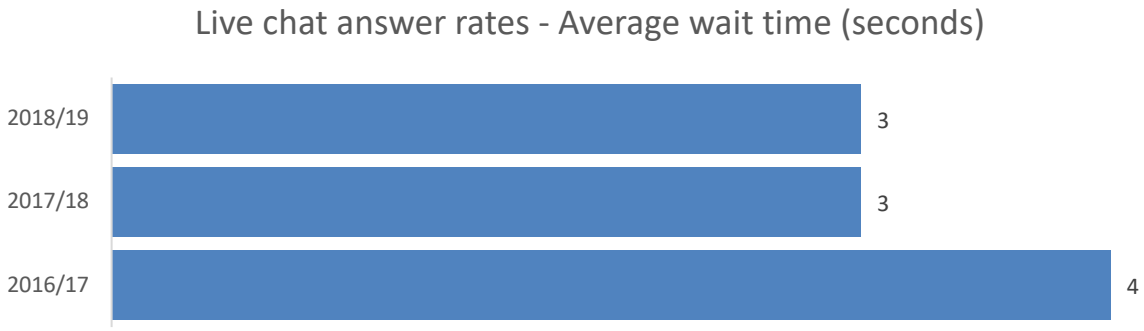




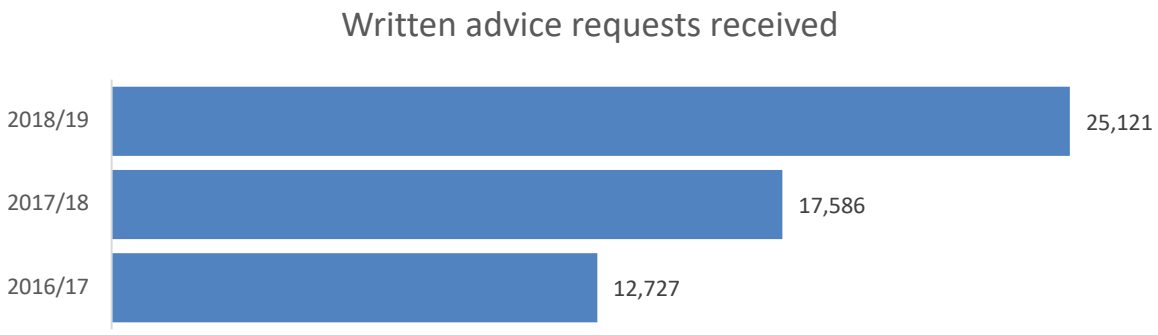
Live Chat

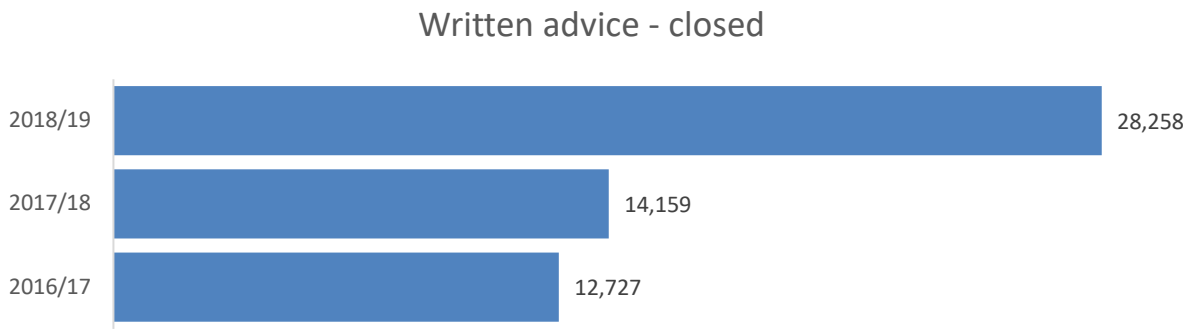


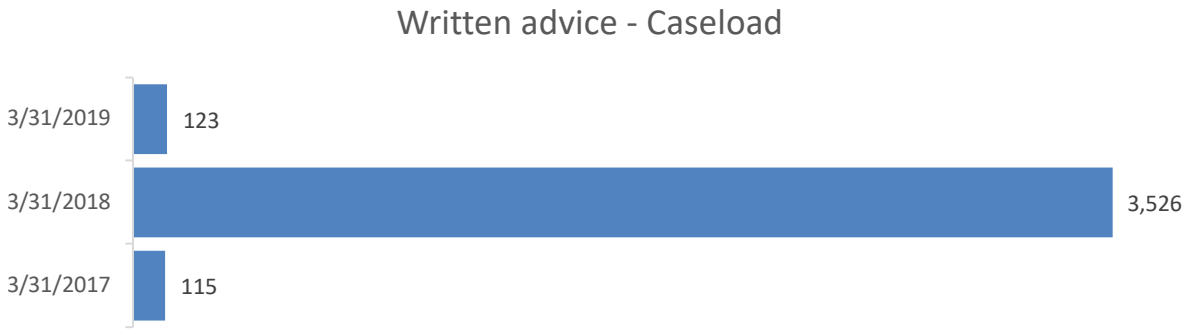


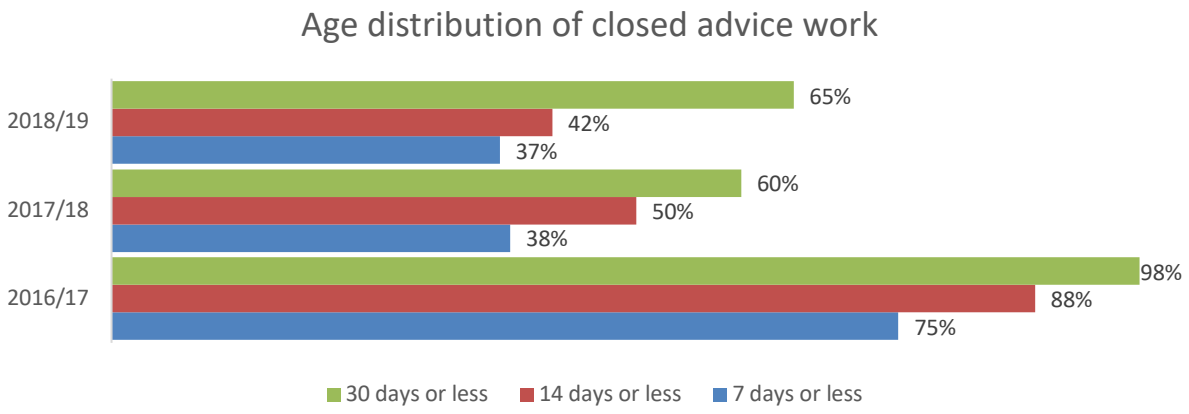


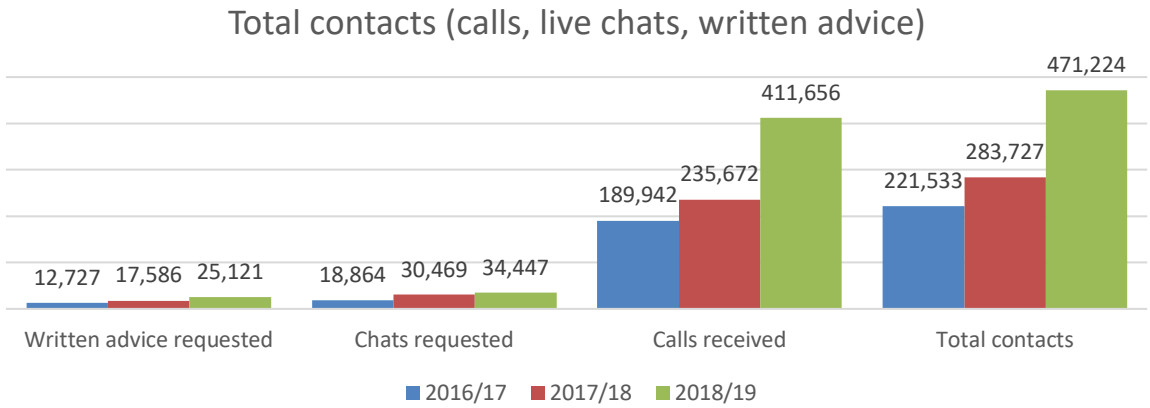
Written Advice



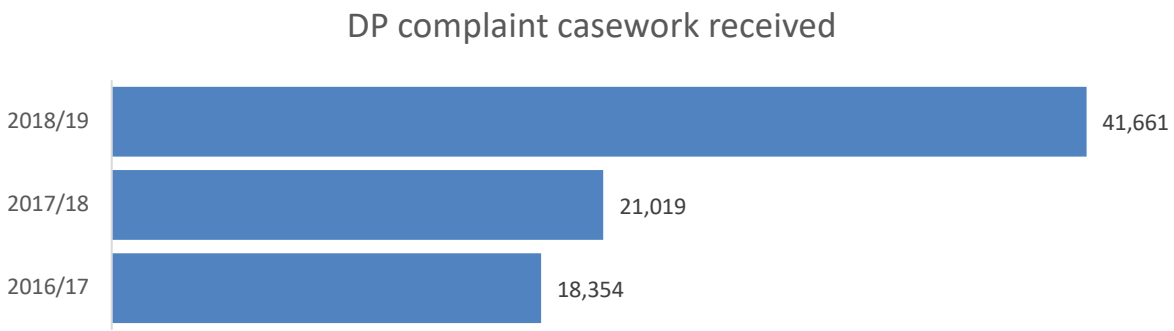

Written advice - closed
2018/19
28,258
2017/18
14,159
2016/17
12,727

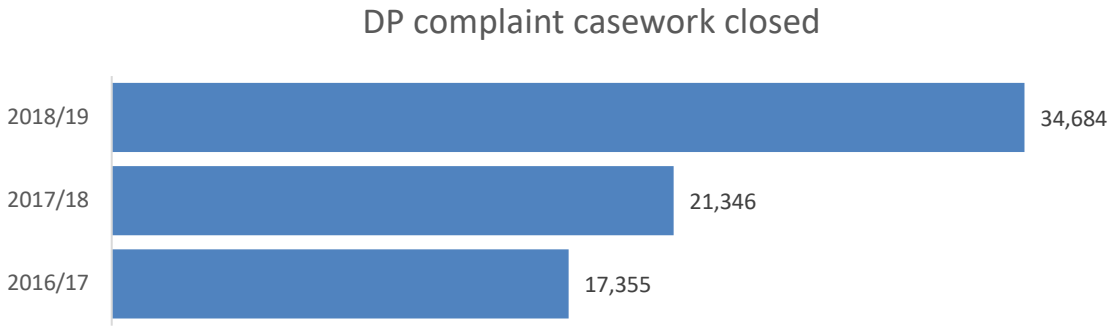

Written advice - Caseload
3/31/2019
123
3/31/2018
3,526
3/31/2017
115

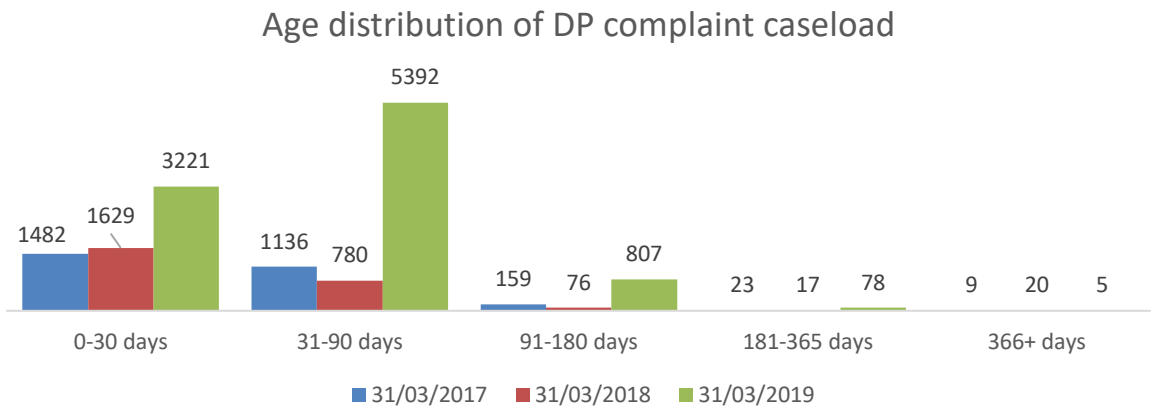

Age distribution of closed advice work
2018/19
65%
42%
37%
2017/18
60%
50%
38%
2016/17
98%
88%
75%
30 days or less
14 days or less
7 days or less

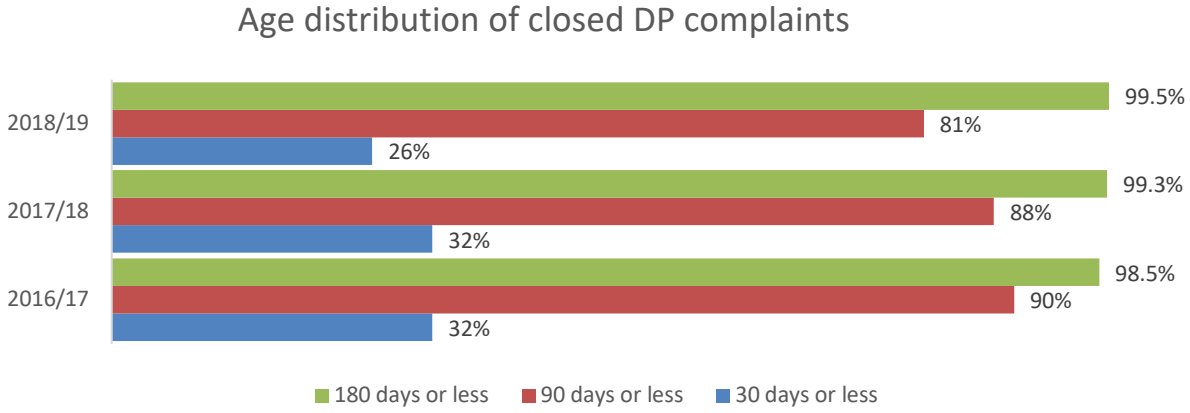

Total contacts (calls, live chats, written advice)
12,727
17,586
25,121
18,864
30,469
34,447
189,942
235,672
411,656
221,533
283,727
471,224
Written advice requested
Chats requested
Calls received
Total contacts
2016/17
2017/18
2018/19

Data protection concerns

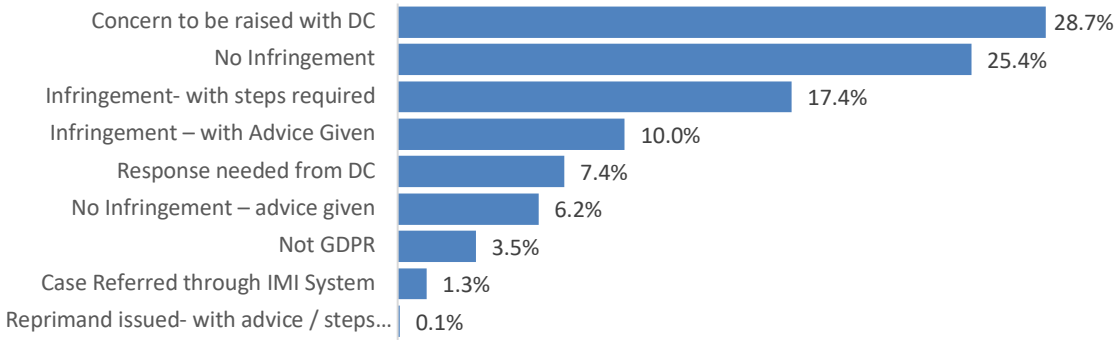




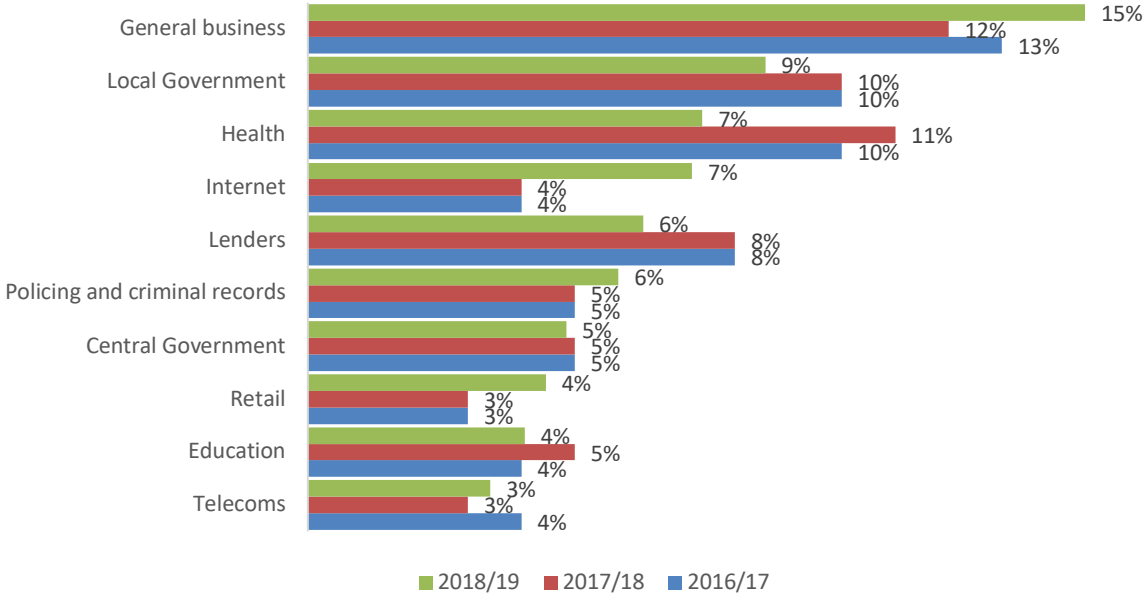




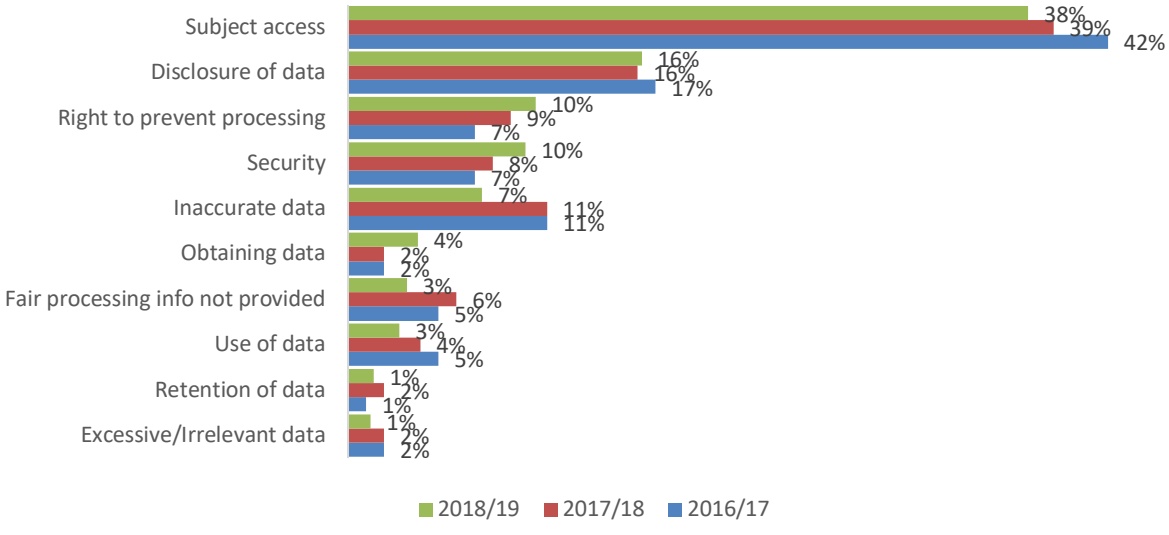
Outcomes 2018/19



Sectors generating most DP complaints

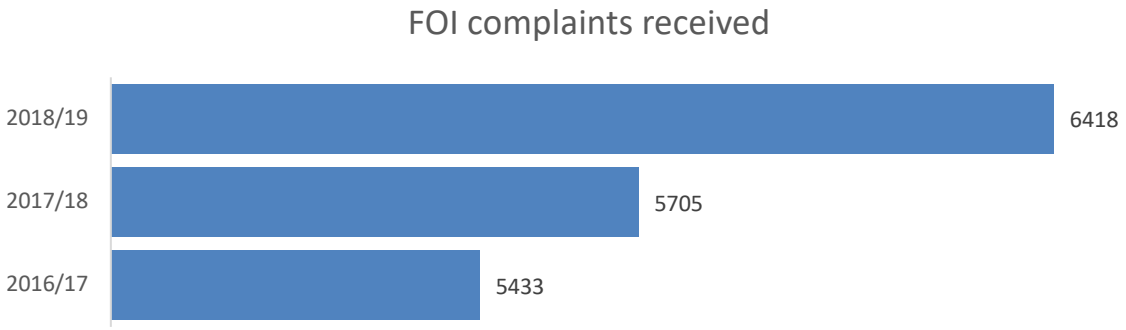


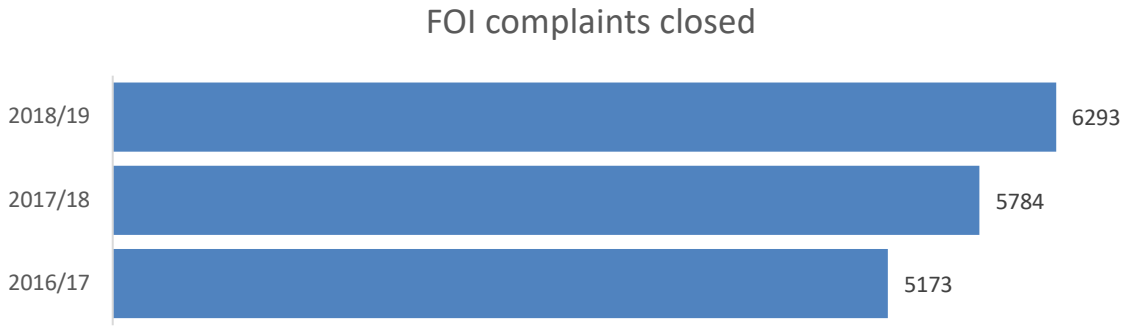
Reasons generating most complaints

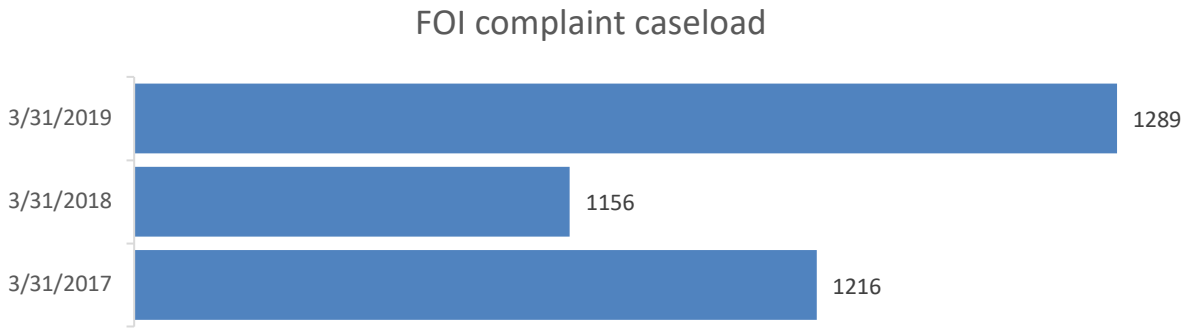


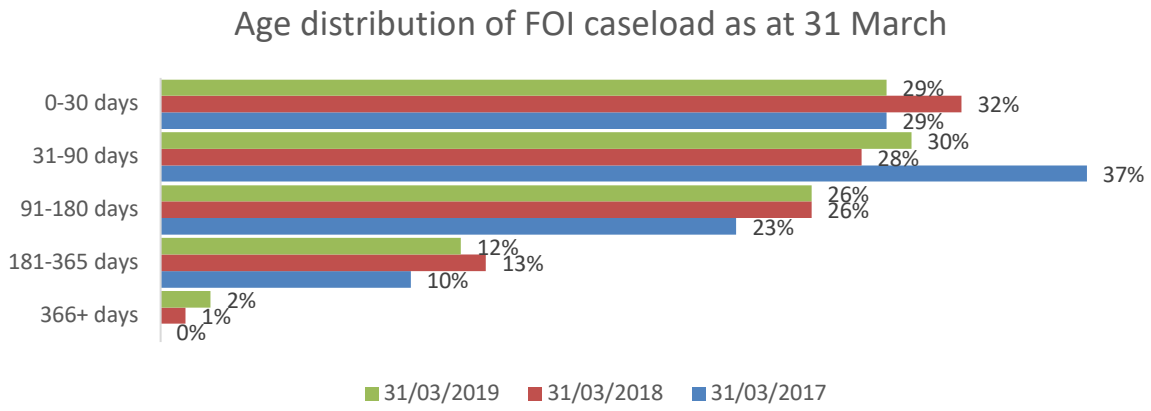
Freedom of information

FOI complaint casework

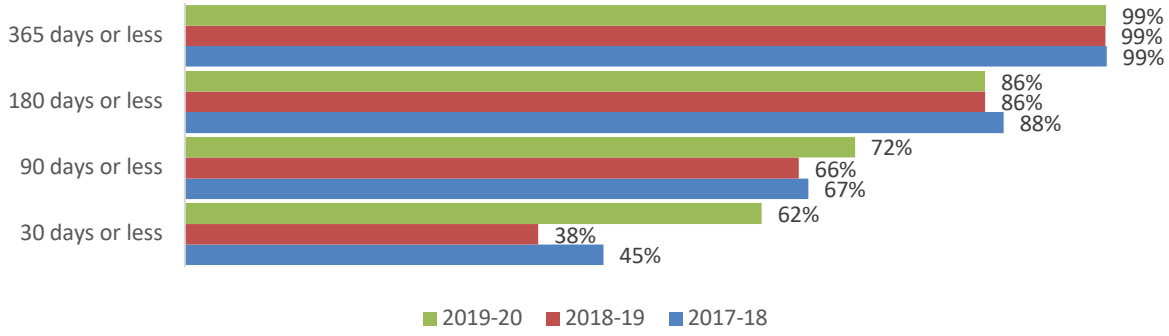




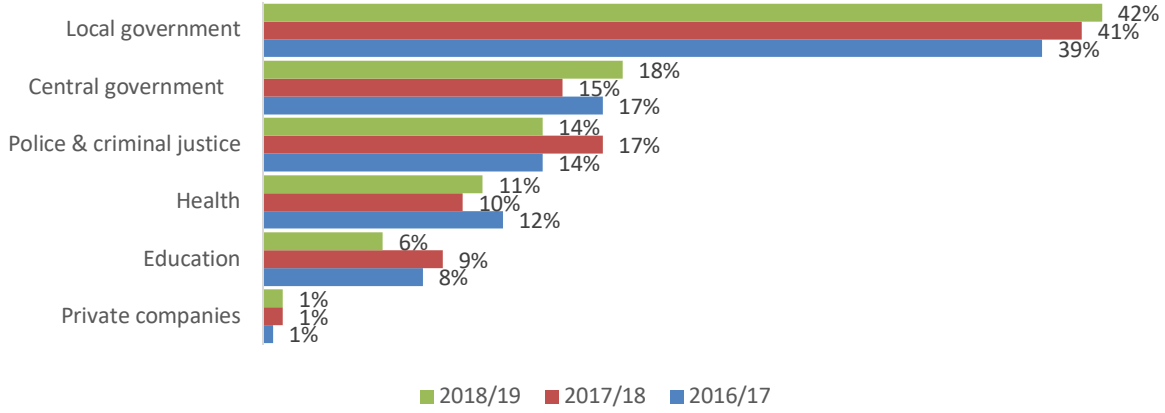




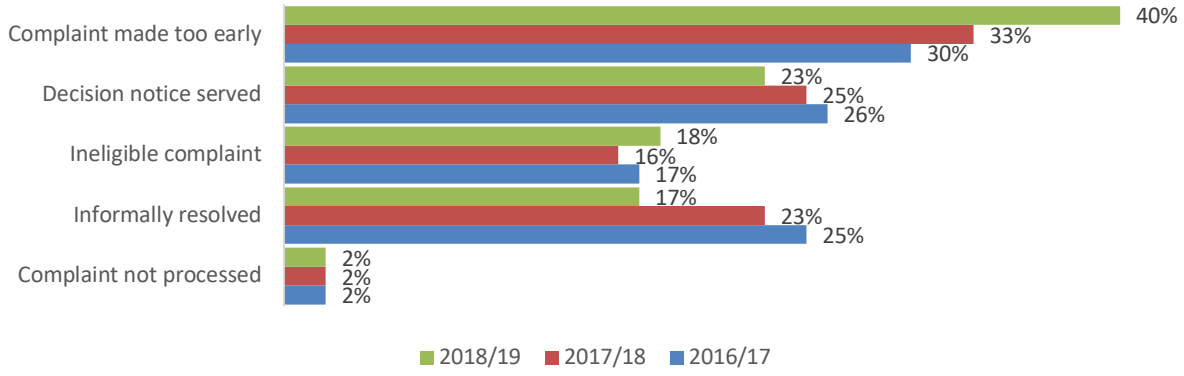
Age distribution of finished casework %

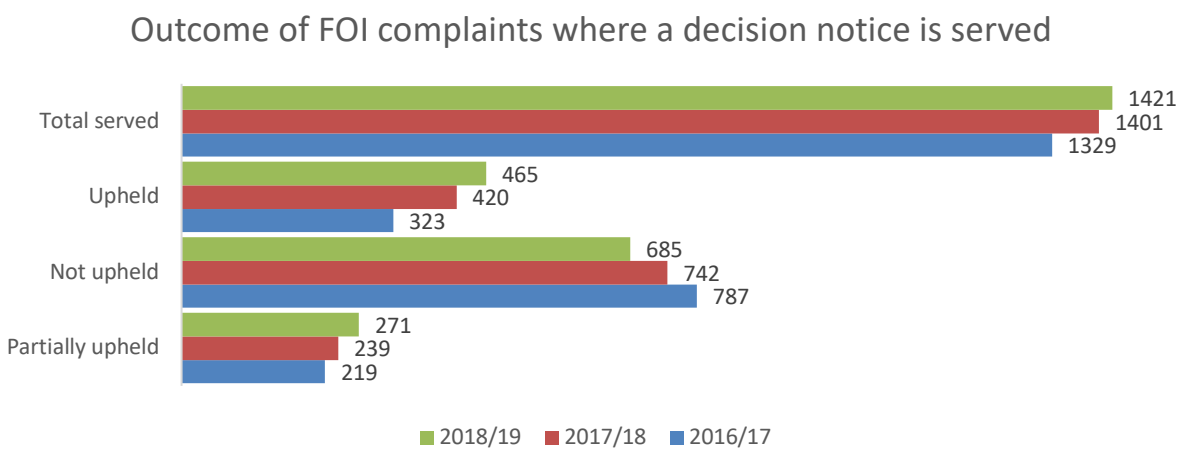


Sectors and reasons generating most FOI complaints

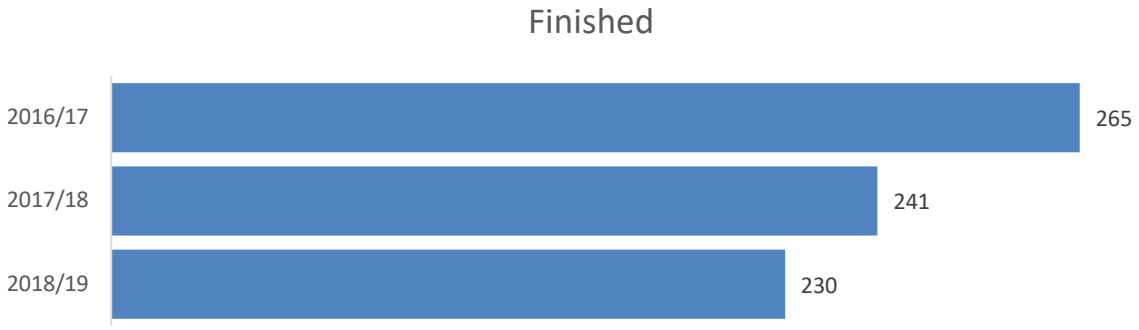


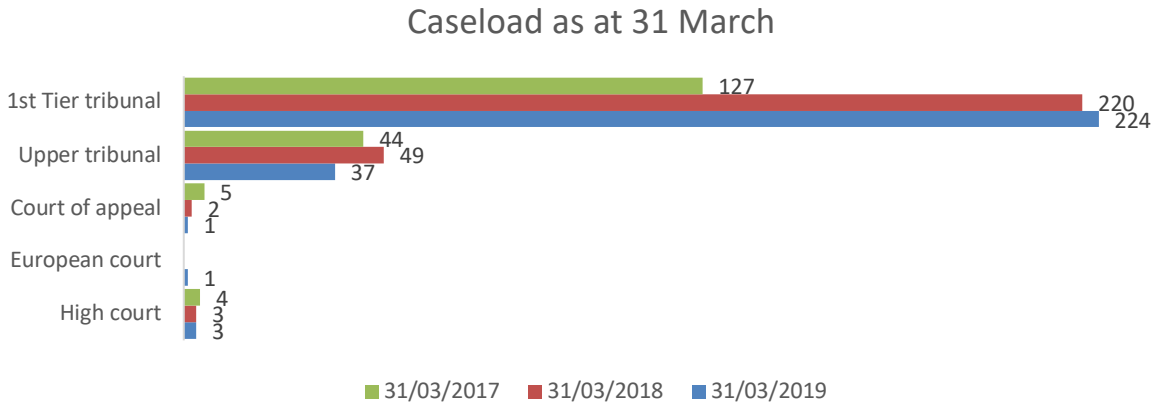
Outcomes of FOI complaints

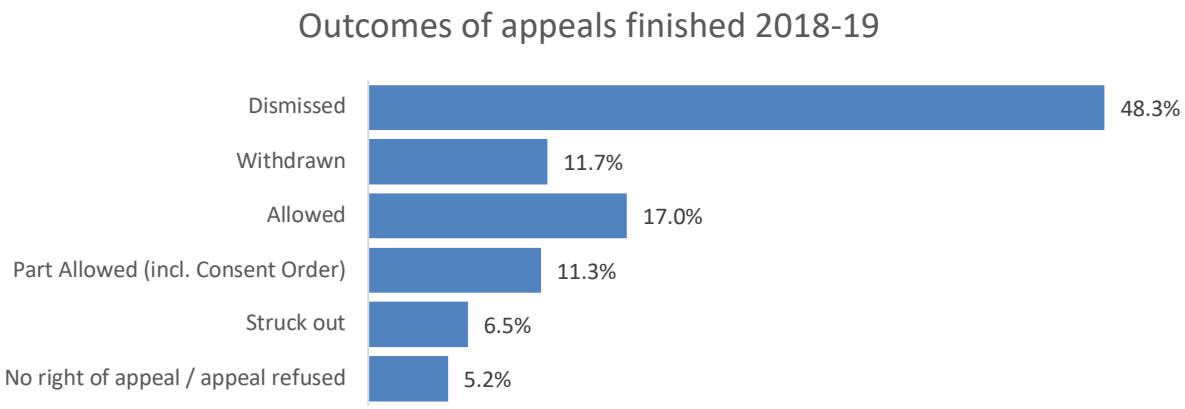




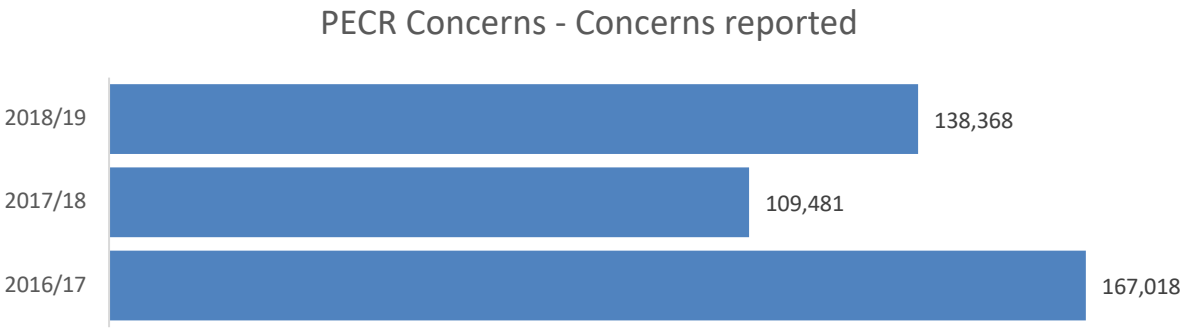
Appeals to the Information Rights Tribunal

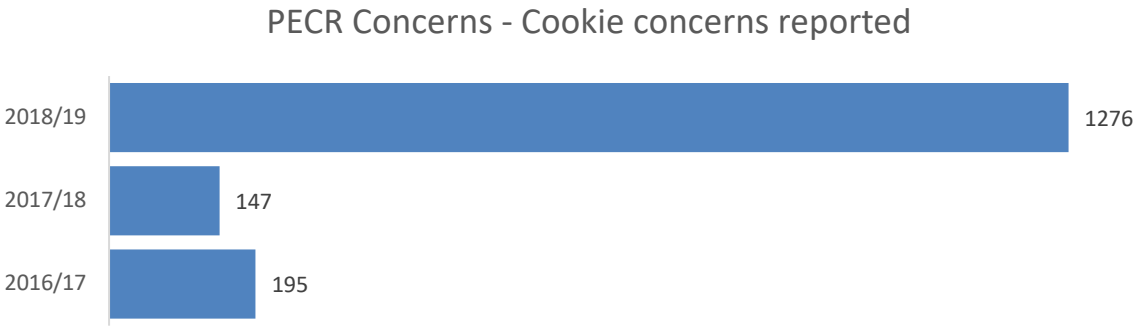


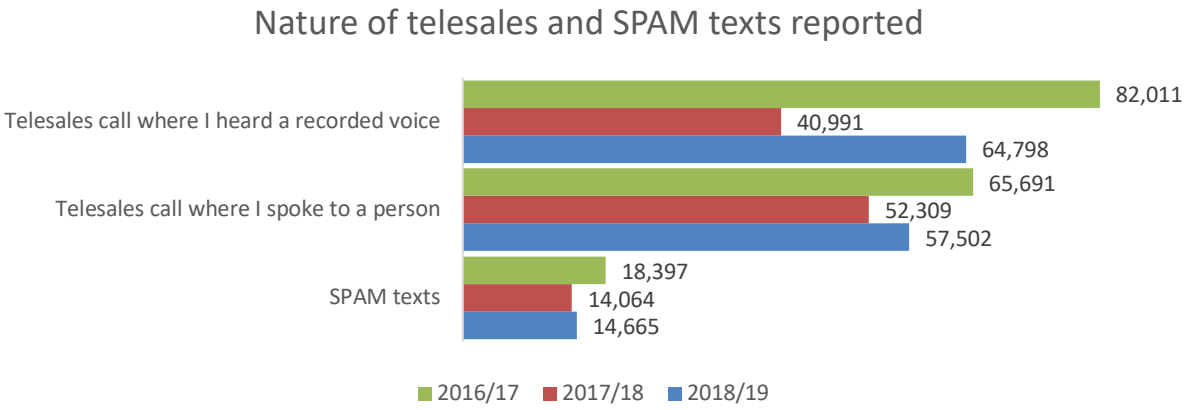




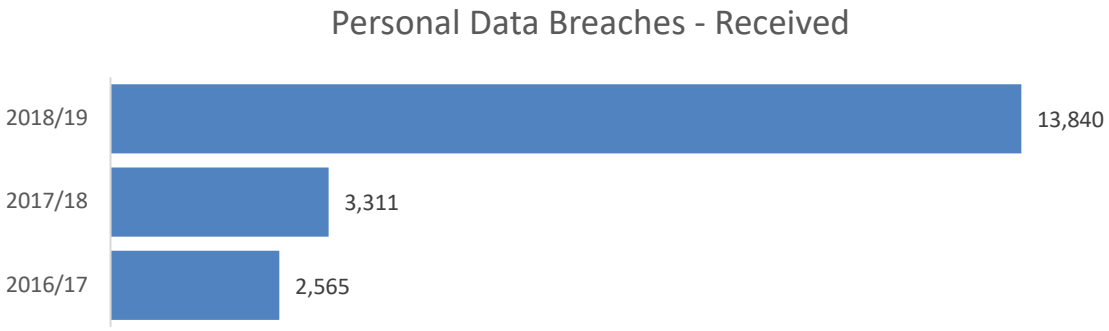
PECR concerns

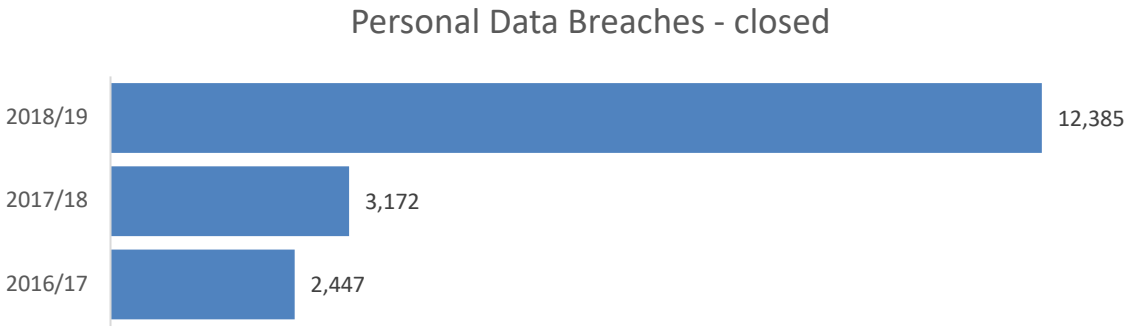


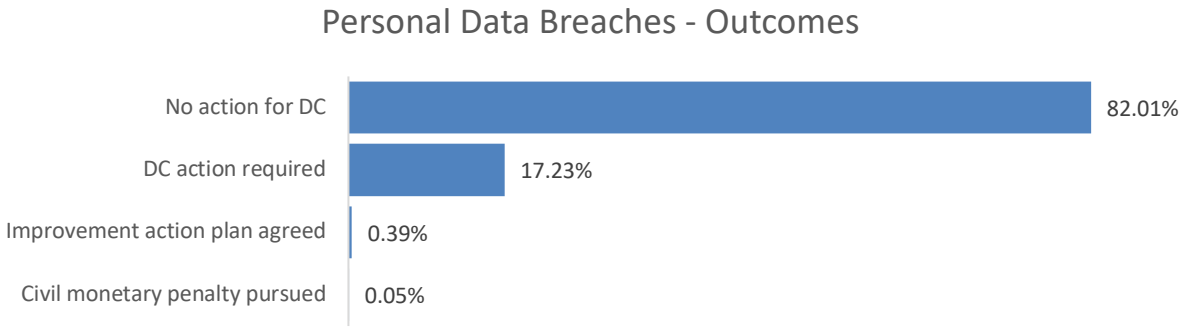




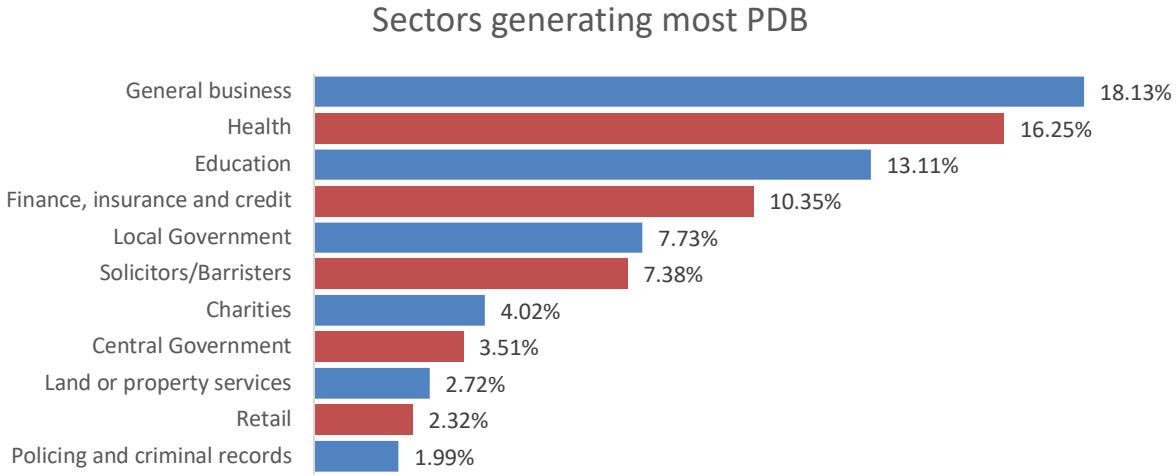
Self-reported data breaches



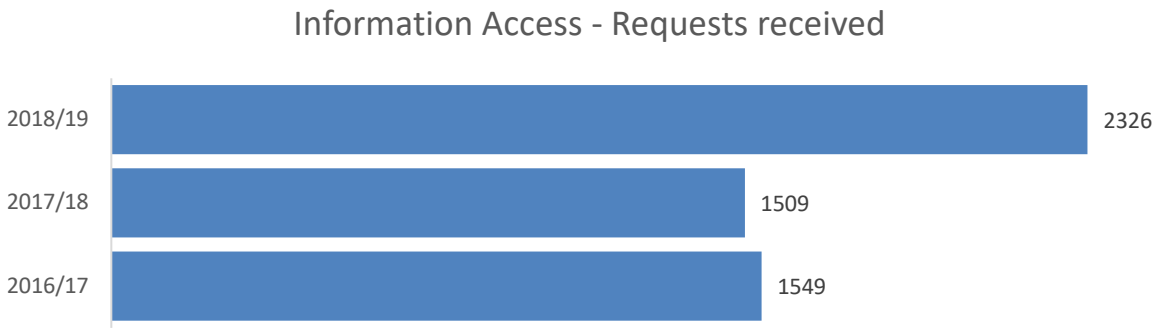


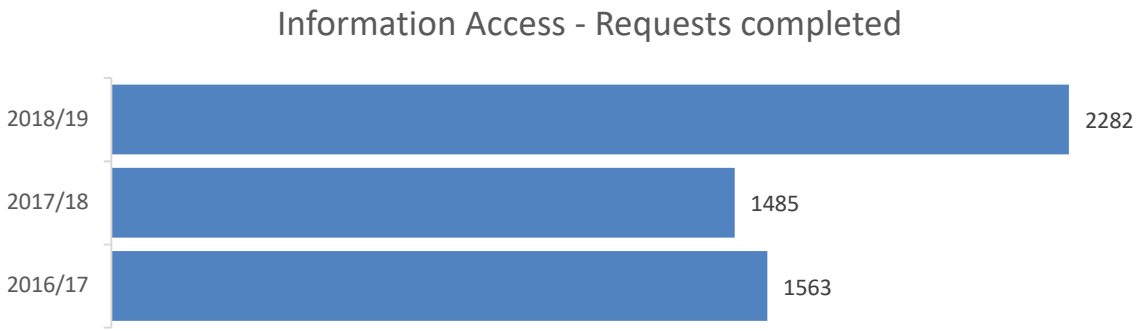


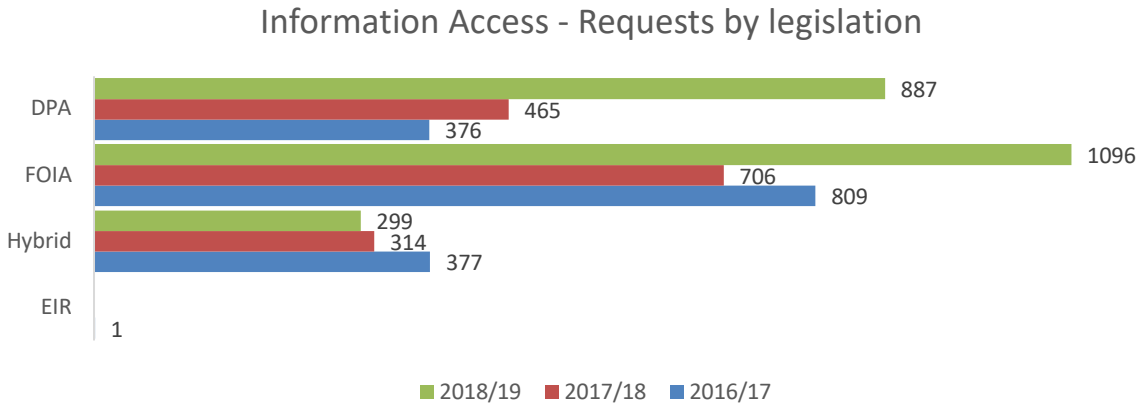
*Note: an additional 0.3% of PDBs closed with the following outcomes: investigation pursued, audit visit recommended, DPA 1998/2018 not applicable, or data controller outside the UK.

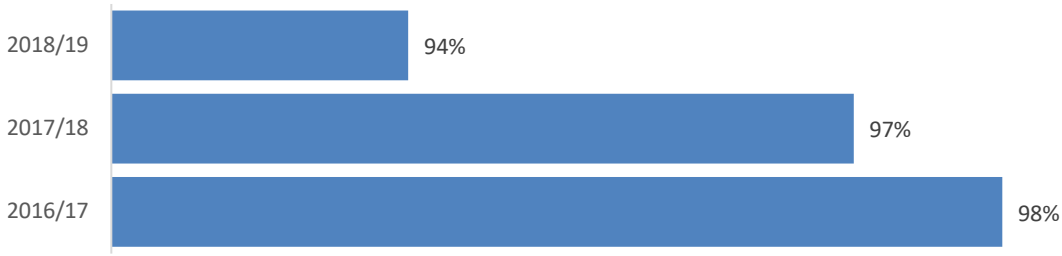


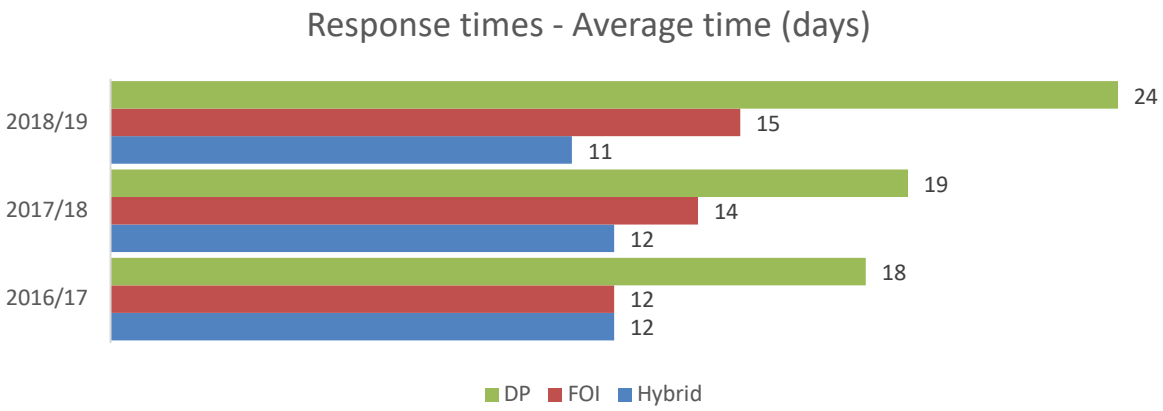
Information access

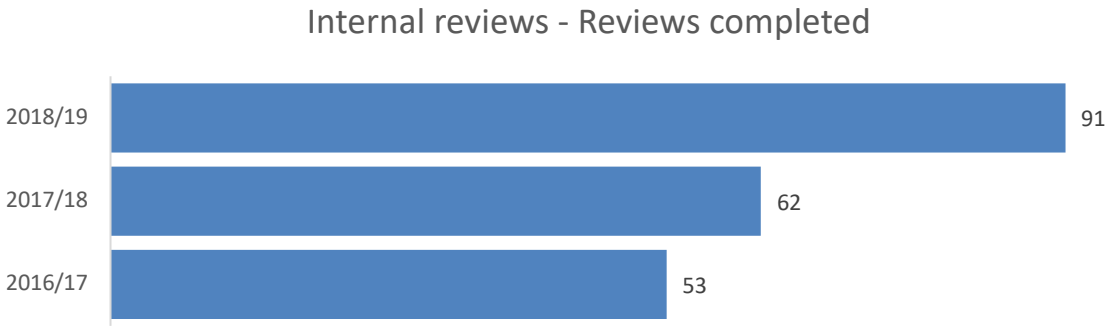


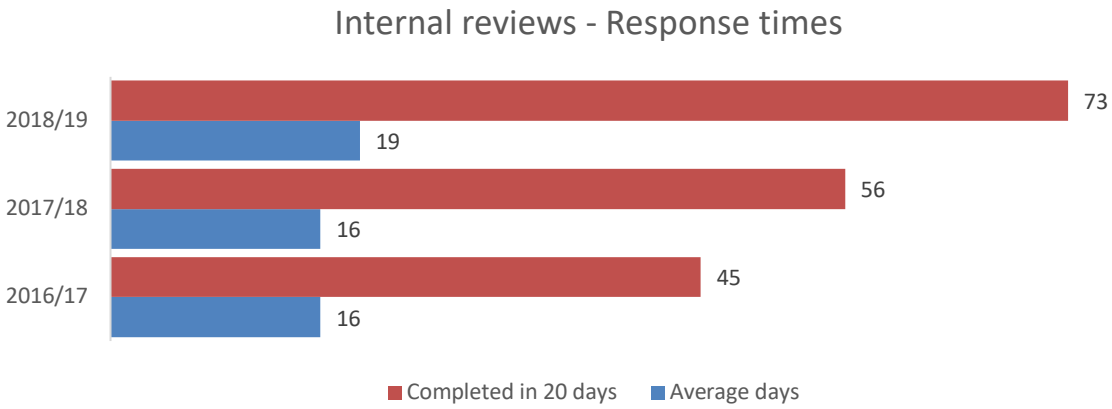


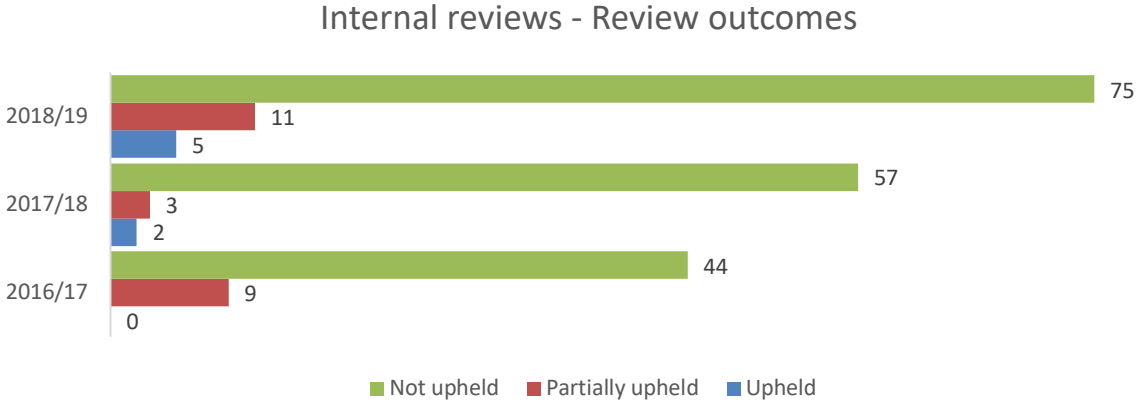





Response times - Average time (days)
2018/19
2017/18
2016/17
24
15
11
19
14
12
18
12
12
DP
FOI
Hybrid


Internal reviews - Reviews completed
2018/19
2017/18
2016/17
91
62
53


Internal reviews - Response times
2018/19
2017/18
2016/17
73
19
56
16
45
16
Completed in 20 days
Average days


Internal reviews - Review outcomes
2018/19
2017/18
2016/17
75
11
5
57
3
2
44
9
0
Not upheld
Partially upheld
Upheld

Financial performance summary

Grant in aid

Freedom of information expenditure continued to be funded by grant in aid. In addition, our work on Network and Information Systems (NIS) was funded by grant in aid. The total grant in aid available for 2018-19 was £4.3m (2017-18: £5.2m). However, during 2017-18 a £1.4m advance on grant in aid was received to assist with additional costs resulting from the implementation for GDPR. Therefore, the grant available for 2018-19 was adjusted downwards by £1.4m, resulting in grant in aid of £2.9m being received during the year.

No grant in aid was carried forward in 2018-19 (2017-18: nil).

Fees

Until the implementation of DPA 2018, data protection related work was financed by fees collected from data controllers who had to notify their processing of personal data under the DPA 1998. The annual fee was £35 which applied to charities and small organisations with fewer than 250 employees. A higher fee of £500 was applicable for larger data controllers defined as those with an annual turnover of £25.9 million or more and employing more than 250 people. For public authorities employing more than 250 people the fee was also £500.

Following the implementation of DPA 2018, data protection related work continued to be financed by fees collected from data controllers, but with a new fee structure. The annual fee structure is:

- £40 for charities or organisations with no more than 10 members of staff or a maximum turnover of £632,000.
- £60 for organisations with no more than 250 members of staff or a maximum turnover of £36m.
- £2,900 for all other organisations.

A £5 discount was given to all fees which were paid by direct debit.

Fees collected in the year totalled £39.256m (2017-18: £21.300m), an 84% increase on the previous year.

Annual expenditure

The total comprehensive expenditure for the year was £3.336m (2017-18: £5.941m).

Financial instruments

Details of our approach and exposure to financial risk are set out in note 8 to the financial statements.

Sustainability

Overall strategy

Our carbon footprint is generated primarily from heating and lighting ICO accommodation, powering our IT infrastructure and from business travel. We make as full a use of technology as possible to reduce electricity and gas consumption; for example by purchasing low energy use IT, fitting new more efficient boilers and installing motion detecting lights.

We also aim to ensure appropriate and proportionate communications tools are in place so that we can engage with stakeholders through relevant channels. As a growing organisation there are increasing business travel demands, but, where appropriate, we seek to communicate electronically rather than have to travel for face to face meetings.

Performance

Throughout 2018-19, preparations for the UK's exit for the European Union ramped up. This has required our staff to travel with increased frequency to Brussels for EU meetings. We have also increased our travel beyond the EU, to develop strong bilateral relationships throughout the world. In addition to promoting excellent personal data practices, these relationships will be of vital assistance to the UK in creating new trade deals in the post-EU exit period, as data has no borders. Data protection will be a key consideration to those trade deals.

In addition, due to the implementation of the GDPR in May 2018 and preparation for the enactment of the DPA 2018 at the same time, we were very heavily involved in stakeholder engagement at the start of 2018-19. This led to high levels of business travel. Overall, in 2018-19 we had higher levels of travel than previously, which is reflected in the increase in travel emissions.

Our use of gas increased significantly during 2018-19. This was due to upgrades being completed to the heating systems in our main offices. These upgrades had been ongoing for a number of years and now ensure that heating is provided to our facilities more efficiently

2018-19 was also a year of expansion for the ICO. As set out earlier in the report, our staffing levels increased by almost 200 staff during the year and we expanded the footprint of our main Wilmslow accommodation by 79% to keep pace with the increasing size of our workforce. Despite this, our total utility usage stayed relatively static. As such, our total emissions from utilities per full-time staffing equivalent reduced when compared to 2017-18.

Biodiversity action planning

The ICO is not responsible for any outside space and therefore does not have a biodiversity plan.

Sustainable procurement

We ask those tendering for contracts to provide their sustainability statements and policies as standard in most procurement exercises.

Green house gas emissions

Total tonnes CO_2

	2015-16	2016-17	2017-18	2018-19
Scope 1 (gas)	18	7	6	36
Scope 2 (electricity)	160	123	172	160
Scope 3 (travel)	94	86	127	202
Total emissions	273*	217*	306*	398

Tonnes CO2 per full time equivalent staffing

	2015-16	2016-17	2017-18	2018-19
Scope 1 (gas)	0.04	0.02	0.01	0.06
Scope 2 (electricity)	0.39	0.30	0.33	0.26
Scope 3 (travel)	0.23	0.21	0.25	0.33
Total	0.67*	0.53	0.59	0.66*

*Not a direct sum due to rounding.

Waste minimisation and management and finite resource consumption

Total waste, water and paper consumption

	2015-16	2016-17	2017-18	2018-19
Waste / tonnes	16	16	37	35
Water consumption / m^3	2,100	2,382	5,963	3,983
A4 paper / reams	3,700	4,000	4,300	4,280

Waste, water and paper consumption per full time equivalent staffing

	2015-16	2016-17	2017-18	2018-19
Waste / tonnes	0.04	0.04	0.07	0.06
Water consumption / m^3	5.14	5.82	11.61	6.57
A4 paper / reams	9.06	9.78	8.37	7.06

Details of ICO performance:

Total Travel

	2015-16	2016-17	2017-18	2018-19
Cars				
Kms	31,662	37,264	40,216	57,336
Cost £	8,484	8,195	11,023	14,699
Tonnes CO_2	6	7	8	11
Rail				
Kms	637,460	615,052	820,202	1,120,361
Cost £	178,755	184,443	259,483	404,552
Tonnes CO_2	29	28	37	51
Flights				
Number	496	254	515	1,060
Kms	377,845	327,356	523,413	889,325
Cost £	49,770	56,614	103,127	202,847
Tonnes CO_2	60	52	82	140
Travel summary				
Cost £	237,009	249,252	373,633	622,098
Tonnes CO_2	94	86	127	202

Travel per full time equivalent staffing

	2015-16	2016-17	2017-18	2018-19
Cars				
Kms	77.49	91.11	78.27	94.61
Cost £	20.76	20.04	21.45	24.26
Tonnes CO_2	0.01	0.02	0.01	0.02
Rail				
Kms	1,560	1,504	1,596	1,848
Cost £	437.48	450.96	505.03	667.58
Tonnes CO_2	0.07	0.07	0.07	0.08
Flights				
Number	1.21	0.62	1.00	1.75
Kms	924.73	800.38	1,018.71	1,467.53
Cost £	121.81	138.42	200.71	334.73
Tonnes CO_2	0.15	0.13	0.16	0.23
Travel summary				
Cost £	580.05	609.42	727.20	1,026.56
Tonnes CO_2	0.23	0.21	0.25	0.33

Total utilities

	2015-16	2016-17	2017-18	2018-19
Gas				
Kwh	99,146	37,336	34,514	195,575
Cost £	3,703	1,606	1,549	6,281
Tonnes CO_2	18	7	6	36
Electricity				
Kwh	319,493	246,219	343,910	319,151
Cost £	64,957	50,238	65,122	51,995
Tonnes CO_2	160	123	172	160
Utility summary				
Cost £	68,660	51,844	66,671	58,276
Tonnes CO_2	178	130	178	196

Utilities per full time equivalent staffing

	2015-16	2016-17	2017-18	2018-19
Gas				
Kwh	242.65	91.29	67.17	322.73
Cost £	9.06	3.93	3.01	10.36
Tonnes CO_2	0.04	0.02	0.01	0.06
Electricity				
Kwh	782	602	669	527
Cost £	158.97	122.83	126.75	85.80
Tonnes CO_2	0.39	0.30	0.33	0.26
Utility summary				
Cost £	168.04	126.76	129.76	96.17
Tonnes CO_2	0.44	0.32	0.35	0.32

Notes:

- Information on waste is provided by relevant contractors.
- Travel costs and mileage are collated from central records and from staff directly.
- Figures may not add due to rounding. This is marked with an asterisk where applicable.

Whistleblowing disclosures

The ICO is a 'prescribed person' under the Public Interest Disclosure Act 1998, meaning that whistleblowers are provided with protection when disclosing certain information to us.

The Prescribed Persons (Reports on Disclosures of Information) Regulations 2017 require prescribed persons to report annually on whistleblowing disclosures made to them.

The number of whistleblowing disclosures made to us during the period 1 April 2018 to 31 March 2019 was 319. All information provided was recorded and used to develop our overall intelligence picture, in line with our Information Rights Strategic Plan 2017-2021.

Further action was taken on 135 of the above disclosures. Further action may result in referral to appropriate departments for further consideration, referral to external organisations (including other regulators and law enforcement) or consideration for use of our enforcement powers. After review and assessment 184 of the 319 disclosures resulted in no further action taken at that time.

During the period 1 April 2018 to 31 March 2019 further action on the aforementioned 135 disclosures resulted in 146 referrals to various departments (11 disclosures resulted in multiple referrals). The outcomes of these referrals were:

- 55 disclosures being taken into consideration for ongoing investigations;
- 28 disclosures being considered as data protection complaints;
- 27 disclosures being considered in relation to non-payment of the data protection fee;
- 12 disclosures being referred to strategic policy for consideration;
- 11 disclosures being referred to advice services for advice for the whistleblower; and
- 13 disclosures being referred to other departments for various actions.

After receipt of a concern we will decide how to respond in line with our Regulatory Action Policy. In all cases, we will look at the information provided by whistleblowers alongside other relevant information we hold. For example, if an organisation reports a breach to us we may use information provided by a whistleblower to focus our follow-up enquiries. More broadly, we may use information from whistleblowers to focus our liaison and policy development within a sector, using the information to identify a particular risk or concern.

Going concern

The accounts are prepared on a going concern basis as a non-trading entity continuing to provide statutory public sector services.

Grant in aid has already been included in the DCMS's estimate for 2019-20 and the DPA 2018 and GDPR allows the ICO to fund data protection related work through fees paid by data controllers. Although GDPR is EU legislation, the DPA 2018 is UK law and will continue to be in force following the UK's exit from the EU.

There is no reason to believe that future sponsorship and parliamentary approval will not be forthcoming.

Elizabeth Denham
1 July 2019

B

Accountability report

Directors' report

Directorships and other significant interests held by Board members that may conflict with their management responsibilities

Membership of the ICO's Management Board, along with further information, is detailed in the Governance Statement.

A register of interests is maintained for the Information Commissioner and her Management Board. It is published on the Commissioner's website at www.ico.org.uk. Declarations of interest in any of the items considered at a particular meeting are also asked for at Management Board and Audit Committee meetings.

Employee involvement and well being

The ICO is a growing organisation, committed to being the best employer we can be. As part of our People Strategy, we are aiming to build on our positive culture as a smaller organisation, where caring and supporting others is valued and the ICO is a good corporate citizen. The ICO is being developed in collaboration with staff.

The ICO has a policy of co-operation and consultation with recognised trade unions over matters affecting staff. Senior managers meet regularly with trade unions to discuss issues of interest, and staff involvement in the work of the office is actively encouraged as part of the day-to-day process of line management. In 2018-19 we revised the ICO people strategy to capture three new values: ambitious; service-focused; collaborative.

As part of the new People Strategy, in January 2019 we consulted with all staff on our new wellbeing policy. Over 380 staff responded to this consultation. The new policy will be launched during 2019-20.

Equal opportunities and diversity

We put equality and diversity at the heart of everything we do as a growing, tech-savvy regulator. As part of this, we have reviewed our equality and diversity objectives and defined them as follows:

Spreading knowledge and taking action

We will raise awareness of information rights across the community and take action to ensure that organisations fulfil their obligations. We will have particular focus on groups and sectors where knowledge gaps may cause information rights inequalities or vulnerabilities. We will consider equality and diversity issues when prioritising our action as a regulator.

Accessible Services

Our services and information will be accessible for users and potential users of our services, and we will provide our staff with the skills and knowledge they need to provide high quality services for all. We will try to anticipate customer needs and we will take action to remove barriers to our services when possible.

Encouraging others

We will use our status as a regulator, advisory body and purchaser of services to influence improvements in equality by other organisations and across society.

Employer

Our workplaces and practices will be accessible, flexible, fair and inclusive. We will value the diversity, skills, backgrounds and experience of our people, enabling them to perform to their best in a welcoming and supportive environment.

These objectives aim to ensure that the ICO is inclusive, accessible and diverse as a regulator, service provider and employer. This will help to ensure that all members of society have awareness of, and access to, their information rights and receive appropriate protection if their rights are infringed.

Our Equality and Diversity Committee oversees our efforts to provide an increasingly accessible service. We have reviewed the role of this Committee, to ensure that, with the increased size of the organisation, it continues to ensure that we embed equality and diversity into everything we do, as a regulator, a service provider and employer. This has included the creation of staff forums focusing on various equality and diversity issues.

We provide our staff with a work environment and IT systems which help meet a range of needs; including accessible offices and IT systems, flexible and part-time working (to help work-life balance) and the provision of occupational health services.

We aim to recruit from a range of backgrounds and take the applicant anonymous approach when assessing candidates for employment.

The community

For the last two years, ICO staff have supported Dementia UK as our corporate charity. We are currently taking nominations from staff for our corporate charity for 2019-20.

Personal data incidents

There have been no substantive security incidents during 2018-19.

Public sector information holders

The ICO has complied with the cost allocation and charging requirements set out in HM Treasury guidance.

Pension liabilities

Details on the treatment of pension liabilities are set out in note 3 to the financial statements.

Annual accounts and audit

The annual accounts have been prepared in a form directed by the Secretary of State with the consent of the Treasury in accordance with paragraph 11(4) of Schedule 12 to the DPA 2018.

Under paragraph 11(3) of Schedule 12 to the DPA 2018 the Comptroller and Auditor General was appointed auditor to the Information Commissioner for the financial year 2018-19. The cost of audit services for this year was £30k (2017-18: £30k). No other assurance or advisory services were provided.

So far as the Accounting Officer is aware, the Comptroller and Auditor General is aware of all relevant audit information, and the Accounting Officer has taken all the steps that she ought to have taken to make herself aware of relevant audit information and to establish that the Comptroller and Auditor General is aware of that information.

Directors' statement

The ICO's leadership team consists of the Commissioner, Executive Directors and Non-executive Directors. Each of these persons at the time this report is approved:

(a) so far as they are aware there is no relevant audit information of which the auditor is unaware; and

(b) they have taken all the steps they ought to have taken in their role in order to make themselves aware of any relevant audit information and to establish that the auditor is aware of that information.

Statement of the Information Commissioner's responsibilities

Under paragraph 11(4) of Schedule 12 to the DPA 2018 the Secretary of State directed the Information Commissioner to prepare for each financial year a statement of accounts in the form and on the basis set out in the Accounts Direction. The accounts are prepared on an accruals basis and must give a true and fair view of the state of affairs of the Information Commissioner at the year end and of her income and expenditure, recognised gains and losses and cash flows for the financial year.

In preparing the accounts the Information Commissioner is required to comply with the requirements of the Government Financial reporting Manual (FReM) and in particular 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 as set out in the FReM have been followed, and disclose and explain any material departures in the financial statements; and
- 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.

The Accounting Officer of the DCMS has designated the Information Commissioner as Accounting Officer for her Office. The responsibilities of an Accounting Officer, including responsibility for the propriety and regularity of the public finances and for keeping of proper records and for safeguarding the Information Commissioner's assets, are set out in the Non-Departmental Public Bodies' Accounting Officer Memorandum, issued by the Treasury and published in Managing Public Money.

The Accounting Officer confirms that, as far as she is aware, the entity's auditors are aware of all relevant audit information, and the Accounting Officer has taken all the steps that she ought to have taken to make herself aware of any relevant audit information and to establish that the entity's auditors are aware of that information.

The Accounting Officer confirms that the annual report and accounts as a whole is fair, balanced and understandable and that she takes personal responsibility for the annual report and accounts and the judgments required for determining that it is fair, balanced and understandable.

Governance statement

Introduction

The Information Commissioner is a corporation sole as established under the DPA 1998 and as confirmed under the DPA 2018. Under the terms of the EU Data Protection Directive and the GDPR, the Information Commissioner and her office must be completely independent of Government. The Information Commissioner is accountable to Parliament for the exercise of statutory functions and the independence of the ICO is enshrined in legislation.

Relationship with the DCMS

The DCMS is the sponsoring department for the ICO. The relationship with the department is governed by a Management Agreement. The Management Agreement for 2018-2021 was agreed in July 2018. This agreement sets out our responsibility to support the work of both organisations and to ensure the independence of the Information Commissioner and the ICO. The agreement also ensures that appropriate reporting arrangements are in place to enable the DCMS to monitor the expenditure of public money allocated to the ICO.

The agreement also confirms that the ICO has been granted pay flexibility up to 2020-21. This ensures that we have the flexibility to determine the levels of pay necessary for the ICO to maintain the expertise the office needs to fulfil its functions. Following this period, the ICO will revert to being subject to standard public sector pay policy guidelines.

The DCMS has policy responsibility for DPA 2018 and its associated legislation. The Cabinet Office has policy responsibility for the Freedom of Information Act.

Management Board

The Information Commissioner has a Management Board for support in the role of Accounting Officer. The Board is responsible for developing strategy, monitoring progress in implementing strategy, providing corporate governance and assurance and for managing corporate risks. The Board comprises the Information Commissioner, two Deputy Commissioners, a Deputy Chief Executive Officer, an Executive Director and four non-executive members.

The Board meets quarterly and considers risk management and operational, financial, organisational and corporate issues. It also receives reports from the Audit Committee and Executive Team.

In the course of 2018-19 the following changes were made to Board membership:

- Simon McDougall, Executive Director – Technology Policy and Innovation, was appointed on 1 October 2018 on a two-year contract.

- Emma Bate served as General Legal Counsel until 31 December 2018. On 1 January 2019, Emma's role formally changed to Director of Legal Services – Policy and Commercial. We continue to carry a vacancy for a General Legal Counsel as part of the Management Board (and Executive Team) and will consider recruiting to this role if appropriate.

In addition to the changes set out above, Peter Hustinx has been appointed to join the Management Board as a Non-executive Director from 1 April 2019.

The table below details attendance at the Management Board meetings during the year.

Dates	11 May 2018	6 August 2018	5 November 2018	4 February 2019
Elizabeth Denham	Yes	Yes	Yes	Yes
Paul Arnold	Yes	Yes	Yes	Yes
Emma Bate	No	No	No	
Ailsa Beaton	Yes	Yes	Yes	Yes
David Cooke	Yes	Yes	Yes	Yes
James Dipple-Johnstone	Yes	No	Yes	Yes
Jane McCall	Yes	Yes	Yes	Yes
Simon McDougall			Yes	No
Steve Wood	Yes	Yes	No	Yes
Nicola Wood	Yes	Yes	Yes	Yes

Audit Committee

The Audit Committee meets quarterly and provides a structured, systematic oversight of the ICO's governance, risk management, and internal control practices. The committee assists the board and management team by providing independent advice and guidance on the adequacy and effectiveness of the organisation's management practices detailed below, including any potential improvements to these practices:-

- governance structure
- risk management
- internal control framework
- oversight of the internal audit activity, external auditors, and other providers of assurance
- finance statements and public accountability reporting.

The Committee is chaired by Ailsa Beaton as a Non-executive Director. Jane McCall is the other Non-executive Director and Roger Barlow is the independent member.

The table below shows attendance of Audit Committee members at the meetings during the year.

Dates	15 June 2018	15 October 2018	17 January 2019	29 April 2019
Ailsa Beaton	Yes	Yes	Yes	Yes
Roger Barlow	Yes	Yes	Yes	Yes
Jane McCall	Yes	Yes	Yes	Yes

The Information Commissioner has attended all meetings of the Audit Committee during this period. Both external and internal auditors attend the Audit Committee and have pre-meetings with Committee members before each meeting.

The Audit Committee publishes its own Annual Report. Each annual report, including the 2018-19 report, is available on the ICO website (www.ico.org.uk). The report states that the Committee is satisfied with the quality of internal and external audit and believes that it is able to take a measured and diligent view of the quality of the systems of reporting and control within the ICO.

The Chair of the Audit Committee attends regular meetings of the Chairs of the Audit and Risk Committees of DCMS arms length bodies. These meetings include discussions with senior DCMS staff and the Comptroller and Auditor General, and provide opportunities to share issues of interest.

The Audit Committee receives a quarterly report on incidents of fraud, security breaches and whistleblowing incidents as assurance that the reporting mechanisms are in place and are effective.

Executive Team

The Executive Team provides day-to-day leadership for the ICO and as such is responsible for developing and delivering against the Information Rights Strategic Plan. The team consists of the Information Commissioner, two Deputy Commissioners, Deputy Chief Executive Officer and Executive Director – Technology Policy and Innovation.

The Executive Team is supported in its role by the Senior Leadership Team. This is a new team for 2018-19, consisting of 13 new directors across the organisation. These directors have provided significant new capacity in 2018-19 to help the ICO to deliver the vision set out by the Information Commissioner, the Management Board and the Executive Team.

Board effectiveness

The Management Board has considered its compliance with the Corporate governance in central government departments: Code of good practice 2018. The ICO does not adopt all aspects of the Code, but the Board considers that there are good reasons for this given the nature of the organisation as a corporation sole. In particular:

- the Board does not have the powers and duties of a Board in which is vested the ultimate authority of the organisation. This is because the Information Commissioner is a corporation sole;
- the Board does not have a lead non-executive director, but given the role of the Information Commissioner as a corporation sole, this is not felt to be necessary;
- Non-executive Directors do not have a specific section in the ICO's Annual Report, but this is not currently considered necessary;
- composition of the Board reflects the nature, responsibilities and size of the ICO;
- at the beginning of 2018-19, the ICO did not have a Nominations and Governance Committee. The Board considers governance matters and had taken on overview of remuneration policies. However, in November 2019 we established the Remuneration Advisory Panel to advise the Information Commissioner on remuneration policies related to Executive Team pay. As a corporation sole, the Information Commissioner retains ultimate authority in this area; and
- in respect of an operating framework the Board operates within the overall system of corporate governance at the ICO.

The Board has reviewed the information it receives and is satisfied with its quality. The Board is also satisfied that it is, itself, operating effectively.

Issues and highlights

The ICO's corporate governance structure has considered various issues of substance during the course of the year. These include:

- progress towards achieving the ICO's Information Rights Strategic Plan 2017-2021 and the strategies which directly support this, including the Technology Strategy, International Strategy, Innovation Plan, Resource and Infrastructure Strategic Plan and Freedom of Information Strategy.
- preparation for and the impact of the GDPR and DPA 2018, including the new funding model to support data protection work after May 2018.
- preparation for the UK's exit from the EU.
- updates on the ICO's priority investigations.
- organisational planning matters, including accommodation, recruitment, retention and staff pay, during a period of expansion.

Risk assessment

Risks and opportunities are regularly reviewed by senior managers. All risks and opportunities are reviewed at least quarterly by Executive Directorate Steering Groups and more strategic risks and opportunities are discussed on a monthly basis by Executive Team and Senior Leadership Team. The Management Board and Audit Committee also consider the strategic risks and opportunities at each meeting.

In October 2018 the Audit Committee conducted a full review of all of the ICO's risks and opportunities. The Committee does this on an annual basis. All activities within Directorate business plans are directly linked to risks or opportunities, which has ensured even more regular consideration of risks and opportunities, along with clear identification of actions to mitigate risks or exploit opportunities.

The main risks and opportunities identified during 2018-19 were:

- the opportunity to develop the ICO's culture as the organisation expands and introduces new senior leaders;
- the UK's upcoming exit from the EU having a significant impact on international data transfers;
- ensuring the ICO had sufficient capacity to respond to increased demand for ICO services;
- dealing with the issues arising from major investigations during the year;
- delivering the guidance to the public and businesses, including the statutory codes required under DPA 2018.

The main area of uncertainty for the future relates to the UK's exit from the European Union and establishing its new international position. This is vital for the ICO, as data has no borders. In the run-up to the EU exit, the ICO has devoted significant resources to developing our bilateral relationships with other data protection authorities, both in the EU and beyond.

Sources of assurance

As Accounting Officer the Information Commissioner has responsibility for reviewing the effectiveness of the system of internal control, including the risk management framework. This review is informed by the work of the internal auditors and senior managers who have responsibility for the development and maintenance of the internal control framework, and comments made by the external auditors in their management letter and other reports.

2018-19 was the first year of our contract for internal audit with Mazars, who will provide our internal audit services until June 2021. In their annual report, they gave an opinion that the framework of governance, risk management, and control is moderate in its overall adequacy and effectiveness ("moderate" is defined by Mazars as "some improvements are required to enhance the adequacy and effectiveness of the framework of governance, risk management and control."). This is broadly equivalent

to the opinion given last year by our previous auditors, Grant Thornton. Mazars stated that certain weaknesses and exceptions were highlighted by their audit work, however none were considered fundamental. These matters have been discussed with management, to whom they made a number of recommendations. All of these have been, or are in the process of being addressed.

The Information Commissioner is satisfied that a plan to address weaknesses in the system of internal control and to ensure continuous improvement of the system is in place. The Information Commissioner is also satisfied that all material risks have been identified and that those risks are being properly managed.

Remuneration policy

Schedule 4 to the DPA 2018 states that the salary of the Information Commissioner be specified by a Resolution of the House of Commons. In March 2018 the House resolved that the salary would be £160k per annum from 1 April 2018. The salary is paid directly from the Consolidated Fund. In addition to this salary, the Information Commissioner also receives a non-consolidated, non-pensionable annual allowance of £20,000.

In January 2018 the ICO was granted pay flexibility from 1 April 2018 to 31 March 2021 to enable it to review its pay and grading structure. During this period the ICO has the flexibility to determine the levels of pay necessary for it to maintain the expertise it needs to fulfil its functions as a supervisory authority. In exercising this flexibility, the assumption is that matching market averages will be the upper limit of the ICO's pay levels, since a public sector organisation's pay should be slightly below averages in the wider market. This flexibility is also subject to standard public spending principles and the Information Commissioner will keep HM Treasury and DCMS updated with how this flexibility is being exercised.

In making decisions on remuneration the Information Commissioner has regard to the following considerations:

- the need to recruit, retain and motivate suitably able and qualified people;
- government policies for improving the public services;
- the funds available to the Information Commissioner; and
- Treasury pay guidance.

In matters relating to Executive Team pay, the Information Commissioner also has regard to the recommendations of the Remuneration Advisory Panel (established from February 2019).

To implement pay flexibility during 2018-19, staff pay levels were benchmarked against market rates. New pay scales were established in line with this and a career progression framework was agreed. This framework creates a means by which the ICO can recognise and reward staff, based on increased personal competence, contribution and impact within the role, aligned to the organisation's vision and values. The framework has allowed us to attract and retain higher quality staff.

Once this period of pay flexibility finishes after 2020-21, the ICO's remuneration policy will return to being in line with Section 108 of the Protection of Freedoms Act 2013. As such, the remuneration of staff and other officers will be determined by the Information Commissioner in consultation with the Secretary of State and Treasury.

Staff appointments are made on merit on the basis of fair and open competition and, unless otherwise stated, are open-ended until normal retiring age. Individuals who are made redundant are entitled to receive compensation as set out in the Civil Service Compensation Scheme.

Non-executive Directors are paid an annual salary of £13,824 and are appointed for an initial term of three years, renewable by mutual agreement for one further term of a maximum of three years.

Remuneration and staff report

Salary and pension entitlements (audited)

Details of the remuneration and pension interests of the Information Commissioner and her most senior officials are provided below.

Remuneration (salary, bonuses, benefits in kind and pensions)

Officials	Salary (£'000)		Benefits in kind (-nearest £100)		Compensation schemes (£'000)		Pension benefits (£'000) (-nearest £1,000)		Total (£'000)	
	2018-19	2017-18	2018-19	2017-18	2018-19	2017-18	2018-19	2017-18	2018-19	2017-18
Elizabeth Denham Information Commissioner	180-185[1]	140-145	–	–	–	–	61	55	240-245[1]	190-195
Simon Entwisle Deputy CEO[2]	–	75-80 (full year 90-95)	–	100	–	–	–	(9)	–	65-70
Paul Arnold Deputy CEO	95-100	85-90	100	100	–	–	72	162	165-170	250-255
Rob Luke Deputy Commissioner (Policy)[3]	–	45-50 (full year 80-85)	–	100	–	–	–	97	–	145-150
Steve Wood Deputy Commissioner (Policy)[4]	95-100	80-85	100	100	–	–	75	61	170-175	140-145
James Dipple-Johnstone Deputy Commissioner (Operations)[5]	100-105	70-75 (full year 85-90)	100	100	–	–	17.5[6]	12	115-120	80-85
Simon McDougall Executive Director (Technology Policy and Innovation)[7]	50-55 (full year 105-110	–	–	–	–	–	21	–	75-80	–
Emma Bate General Legal Counsel[8]	75-80[9] (full year 100-105)	45-50 (full year 85-90)	100	100	–	–	38[10]	20	110-115	65-70

Officials	Salary (£'000)		Benefits in kind (-nearest £100)		Compensation schemes (£'000)		Pension benefits (£'000) (-nearest £1,000)		Total (£'000)	
	2018-19	2017-18	2018-19	2017-18	2018-19	2017-18	2018-19	2017-18	2018-19	2017-18
Ailsa Beaton Non-Executive Board Member	15-20	10-15	–	–	–	–	–	–	15-20	10-15
Nicola Wood, Non-Executive Board Member	20-25	10-15	–	–	–	–	–	–	20-25	10-15
David Cooke Non-Executive Board Member	25-30	10-15	–	–	–	–	–	–	25-30	10-15
Jane McCall Non-Executive Board Member	15-20	10-15	–	–	–	–	–	–	15-20	10-15

Notes:

1. This includes a non-consolidated, non-pensionable annual allowance of £20,000
2. Retired January 2018.
3. Left ICO employment October 2017.
4. Appointed June 2017.
5. Appointed June 2017.
6. James Dipple-Johnstone is a member of a Partnership pension scheme. We are required to disclose Employer contributions to pensions to the nearest £100.
7. Appointed October 2018.
8. Served as General Legal Counsel until 31 December 2018.
9. This is the remuneration received in the role of General Legal Counsel.
10. The data provided by MyCSP is an aggregate for the full year. Therefore, this figure includes pension contributions for the full year, both as General Legal Counsel and in new role as Director of Legal Services (Policy and Commercial).

The value of pension benefits accrued during the year is calculated as the real increase in pension multiplied by 20 plus the real increase in any lump sum, less the contributions made by the individual. The real increases exclude increases due to inflation or any increase or decrease due to a transfer of pension rights.

Salary comprises gross salary and any other allowance to the extent that it is subject to UK taxation. There were no bonus payments to Board Members in 2017-18.

All benefits in kind relate to the ICO's contribution to the ICO's health care plan provided by BHSF.

Pension Benefits (audited)

	Accrued pension at pension age as at 31 March 2019 and related lump sum	Real increase in pension and related lump sum at pension age	CETV at 31 March 2019	CETV at 31 March 2018	Real increase in CETV
	£000	£000	£000	£000	£000
Elizabeth Denham Information Commissioner	5-10	2.5-5	149	83	46
Paul Arnold Deputy CEO	25-30 plus a lump sum of 55-60	2.5-5 plus a lump sum of 2.5-5	410	314	42
Steve Wood Deputy Commissioner (Policy)	15-20	2.5-5	278	195	47
James Dipple-Johnstone Deputy Commissioner (Operations)[1]	–	–	–	–	–
Simon McDougall Executive Director (Technology Policy and Innovation)	0-5	0-2.5	14	0	9
Emma Bate General Legal Counsel[2]	0-5	0-2.5	38	11	18

Notes:

1. Member of partnership pension scheme.
2. Served in this role until 31 December 2018.

The Cash Equivalent Transfer Value (CETV) figures are provided by MyCSP, the ICO's Approved Pensions Administration Centre, who have assured the ICO that they have been correctly calculated following guidance provided by the Government Actuary's Department.

Partnership pensions

There is one member of staff included in the list of the Commissioner's most senior staff who has a partnership pension. Please see note 6 to the table on page 86.

Civil Service pensions

Further details about the Civil Service pension arrangements are available at www.civilservice.gov.uk/pensions.

Cash Equivalent Transfer Values

A CETV is the actuarially assessed capitalised value of the pension scheme benefits accrued by a member at a particular point in time. The benefits valued are the member's accrued benefits and any contingent spouse's pension payable from the scheme. It represents the amount paid made by a pension scheme or arrangement to secure pension benefits in another pension scheme or arrangement when the member leaves a scheme and chooses to transfer the benefits accrued in their former scheme.

The pension figures shown relate to the benefits that the individual has accrued as a consequence of their total membership of the pension scheme, not just their service in a capacity to which disclosure applies.

The figures include the value of any pension benefit in another scheme or arrangement that the individual has transferred to the Civil Service pension arrangements. They also include any additional pension benefit accrued to the member as a result of their purchasing additional pension benefits at their own cost. CETV's are worked out in accordance with The Occupational Pensions Schemes (Transfer Values) (Amendment) Regulations 2008 and do not take account of any actual or potential reduction to benefits resulting from Lifetime Allowance Tax which may be due when pension benefits are taken.

Real increase in CETV

This reflects the increase in CETV that is funded by the employer. It does not include the increase in accrued pension due to inflation, contributions paid by the employee (including the value of any benefits transferred from another pension scheme or arrangement) and uses common market valuation factors for the start and end of the period.

Pay multiples (audited)

Reporting bodies are required to disclose the relationship between the remuneration of the highest paid director in their organisation and the median remuneration of the organisation's workforce. The Information Commissioner is deemed to be the highest paid director and no member of staff receives remuneration higher than the highest paid director.

The banded remuneration of the highest paid director of the ICO in the financial year 2018-19 was £180k to £185k (2017-18: £140k to £145k). This was 6.6 times (2017-18: 5.6 times) the median remuneration of the workforce, which was £27,096 (2017-18 £25,703). The median total remuneration is calculated by ranking the annual full time equivalent salary as at 31 March 2019 for each member of staff.

Staff remuneration ranged from £19,299 to £180,000 (2017-18: £16,718 to £140,000).

Total remuneration includes salary, non-consolidated performance-related pay and benefits-in-kind. It does not include severance payments, employer pension contributions or the CETV of pensions.

During 2018-19, as stated above, the ICO was granted pay flexibility, although it still adheres to the principle of government pay restraint policies.

Number of senior civil service staff (or equivalent) by band

The Information Commissioner, the two Deputy Commissioners, the Deputy Chief Executive Officer, the Executive Director – Technology Policy and Innovation and the four Non-executive Directors are the only staff categorised as being at a grade equivalent to the senior civil service.

Staff composition

As of the end of this financial year there were nine members of the Management Board, of whom five were male and four female. Across the ICO as a whole 37% of staff were male and 63% female.

Sickness absence

The average number of sick days taken per person during the year was 5.5 days (2017-18: 3.9 days).

Staff policies relating to the employment of disabled persons

The ICO's recruitment processes ensure that shortlisting managers only assess the applicant's skills, knowledge and experience for the job. All personal information is removed from applications before shortlisting.

The ICO applies the Disability Confident standard for job applicants who are disabled. It has also assisted in the continued employment of disabled people by providing a work environment that is accessible and equipment that allows people to perform effectively. Our disabled staff are given equal access to training and promotion opportunities and adjustments are made to work arrangements, work patterns and procedures to ensure that people who are, or become, disabled, are treated fairly and can continue to contribute to the ICO's aims.

Staff numbers and costs

As at 31 March 2019 the ICO had 722 permanent staff (679.7 full time equivalents).

Average number of full time equivalents during 2018-19

	Permanently employed staff	Temporarily employed staff	2018-19 Total	2017-18 Total
Directly employed	601	5	606	466
Agency staff	0	32	32	14
Total employed	601	37	638	480

Staff costs

	Permanently employed staff	Others	2018-19 Total	2017-18 Total
	£000	£000	£000	£000
Wages and salaries	20,972	1,868	22,840	14,517
Social security costs	2,154	–	2,154	1,331
Other pension costs	4,050	–	4,050	2,732
Sub-total	27,176	1,868	29,044	18,580
Less recoveries in respect of outward secondments	(1)	–	(1)	–
Total net costs	27,175	1,868	29,043	18,580

Included in staff costs above are notional costs of £220k (2017-18: £190k) in respect of salary and pension entitlements of the Information Commissioner and the associated employers national insurance contributions (which are credited directly to the General Reserve), temporary agency staff costs of £1.415m (2017-18: £508k) and inward staff secondments of £453k (2017-18: £109k), as well as the amounts disclosed in the Remuneration section above.

Expenditure on consultancy

During 2018-19 there was expenditure totalling £329k on consultancy as defined in Cabinet Office spending controls guidance (2017-18: £39k). This expenditure mainly relates to external support in establishing the ICO's pay flexibility policies, following completion of the business case last year. It also includes support which has been necessary in other areas during our growth in the last year, such as review of our regulatory sandbox, preparation for the UK's EU exit, strategic communications, and research.

Off-payroll engagements

There were no off payroll engagements during 2018-19.

Exit packages (audited)

Redundancy and other departure costs are paid in accordance with the provisions of the Civil Service Compensation Scheme, a statutory scheme made under the Superannuation Act 1972. Exit costs are accounted for in full in the year of departure. Where the Information Commissioner has agreed early retirements the additional costs are met by the Information Commissioner and not by the Principle Civil Service Pension Scheme (PCSPS). Ill health retirement costs are met by the pension scheme and are not included in the table above.

There were no compulsory redundancies in 2018-19 (2017-18: none) and no other exit packages.

Ex-gratia payments made outside of the provisions of the Civil Service Compensation Scheme are agreed directly with the Treasury.

Trade union facility time

Relevant union officials	
Number of employees who were relevant union officials during the relevant period	17
Full time equivalent employee number	1.50

Percentage of time spent on facility time	
0%	0
1-50%	15
51%-99%	2
100%	0

Percentage of pay bill spent on facility time	
Total cost of facility time	£46,063.20
Total pay bill	£27,176,000
Percentage	0.22%

Paid trade union activities	
Time spent on trade union activities as a percentage of total paid facility time hours	100%

Regularity of expenditure (audited)

There are no regularity of expenditure issues.

Fees and charges (audited)

Information on fees collected from data controllers who notify their processing of personal data under the DPA is provided in the Financial Performance Summary, as part of the performance report earlier in this document. Further information on data protection fees is also set out in notes 1.5 and 2 to the financial statements.

Remote contingent liabilities

Please see note 16 to the accounts.

Long-term expenditure trends

The ICO is currently embedding new processes to face the challenge of regulating new data protection legislation, the GDPR and DPA 2018. This new legislation was a major change in data protection legislation, which has had a large impact, not only on the duties and responsibilities of data controllers and the rights of individual citizens, but also on how the ICO works as a regulator.

From 25 May 2018, a new data protection fee structure was introduced, which allows the ICO to better match fee income to the cost of regulation. Fee income is expected to increase to over £46m this financial year, and to approximately £49m by 2020-21.

Grant in aid for our freedom of information work is expected to remain at £3.75m per annum.

Elizabeth Denham
1 July 2019

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

Opinion on financial statements

I certify that I have audited the financial statements of the Information Commissioner's Office for the year ended 31 March 2019 under the Data Protection Act 2018. The financial statements comprise: the Statements of Comprehensive Net Expenditure, Financial Position, Cash Flows, Changes in Taxpayers' Equity; and the related notes, including the significant accounting policies. These financial statements have been prepared under the accounting policies set out within them. I have also audited the information in the Accountability Report that is described in that report as having been audited.

In my opinion:

- the financial statements give a true and fair view of the state of the Information Commissioner's Office's affairs as at 31 March 2019 and of the net expenditure for the year then ended; and
- the financial statements have been properly prepared in accordance with the Data Protection Act 2018 and Secretary of State directions issued thereunder.

Opinion on regularity

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

Basis of opinions

I conducted my audit in accordance with International Standards on Auditing (ISAs) (UK) and Practice Note 10 'Audit of Financial Statements of Public Sector Entities in the United Kingdom'. My responsibilities under those standards are further described in the Auditor's responsibilities for the audit of the financial statements section of my certificate. Those standards require me and my staff to comply with the Financial Reporting Council's Revised Ethical Standard 2016. I am independent of the Information Commissioner's Office in accordance with the ethical requirements that are relevant to my audit and the financial statements in the UK. My staff and I have fulfilled our other ethical responsibilities in accordance with these requirements. I believe that the audit evidence I have obtained is sufficient and appropriate to provide a basis for my opinion.

Conclusions relating to going concern

I am required to conclude on the appropriateness of management's use of the going concern basis of accounting and, based on the audit evidence obtained, whether a material uncertainty exists related to events or conditions that may cast significant doubt on the Information Commissioner's Office's ability to continue as a going concern for a period of at least twelve months from the date of approval of the financial statements. If I conclude that a material uncertainty exists, I am required to draw attention in my auditor's report to the related disclosures in the financial statements or, if such disclosures are inadequate, to modify my opinion. My conclusions are based on the audit evidence obtained up to the date of my auditor's report. However, future events or conditions may cause the entity to cease to continue as a going concern. I have nothing to report in these respects.

Responsibilities of the Accounting Officer for the financial statements

As explained more fully in the Statement of Information Commissioner's Responsibilities, the Accounting Officer is responsible for the preparation of the financial statements and for being satisfied that they give a true and fair view.

Auditor's responsibilities for the audit of the financial statements

My responsibility is to audit, certify and report on the financial statements in accordance with the Data Protection Act 2018.

An audit involves obtaining evidence about the amounts and disclosures in the financial statements sufficient to give reasonable assurance that the financial statements are free from material misstatement, whether caused by fraud or error. Reasonable assurance is a high level of assurance, but is not a guarantee that an audit conducted in accordance with ISAs (UK) will always detect a material misstatement when it exists. Misstatements can arise from fraud or error and are considered material if, individually or in the aggregate, they could reasonably be expected to influence the economic decisions of users taken on the basis of these financial statements.

As part of an audit in accordance with ISAs (UK), I exercise professional judgment and maintain professional scepticism throughout the audit. I also:

- identify and assess the risks of material misstatement of the financial statements, whether due to fraud or error, design and perform audit procedures responsive to those risks, and obtain audit evidence that is sufficient and appropriate to provide a basis for my opinion. The risk of not detecting a material misstatement resulting from fraud is higher than for one resulting from error, as fraud may involve collusion, forgery, intentional omissions, misrepresentations, or the override of internal control.
- obtain an understanding of internal control relevant to the audit in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the Information Commissioner's Office's internal control.
- evaluate the appropriateness of accounting policies used and the reasonableness of accounting estimates and related disclosures made by management.

- evaluate the overall presentation, structure and content of the financial statements, including the disclosures, and whether the consolidated financial statements represent the underlying transactions and events in a manner that achieves fair presentation.

I communicate with those charged with governance regarding, among other matters, the planned scope and timing of the audit and significant audit findings, including any significant deficiencies in internal control that I identify during my audit.

In addition, I am required to obtain evidence sufficient to give reasonable assurance that the income and expenditure reported in the financial statements have been applied to the purposes intended by Parliament and the financial transactions conform to the authorities which govern them.

Other Information

The Accounting Officer is responsible for the other information. The other information comprises information included in the annual report, other than the parts of the Accountability Report described in that report as having been audited, the financial statements and my auditor's report thereon. My opinion on the financial statements does not cover the other information and I do not express any form of assurance conclusion thereon. In connection with my audit of the financial statements, my responsibility is to read the other information and, in doing so, consider whether the other information is materially inconsistent with the financial statements or my knowledge obtained in the audit or otherwise appears to be materially misstated. If, based on the work I have performed, I conclude that there is a material misstatement of this other information, I am required to report that fact. I have nothing to report in this regard.

Opinion on other matters

In my opinion:

- the parts of the Accountability Report to be audited have been properly prepared in accordance with Secretary of State directions made under the Data Protection Act 2018;
- in the light of the knowledge and understanding of the Information Commissioner's Office and its environment obtained in the course of the audit, I have not identified any material misstatements in the Performance Report or the Accountability Report; and
- the information given in the Performance Report and Accountability Report for the financial year for which the financial statements are prepared is consistent with the financial statements.

Matters on which I report by exception

I have nothing to report in respect of the following matters which I report to you if, in my opinion:

- adequate accounting records have not been kept or returns adequate for my audit have not been received from branches not visited by my staff; or
- the financial statements and the parts of the Accountability Report to be audited are not in agreement with the accounting records and returns; or
- I have not received all of the information and explanations I require for my audit; or
- the Governance Statement does not reflect compliance with HM Treasury's guidance.

Report

I have no observations to make on these financial statements.

Gareth Davies
Comptroller and Auditor General **4 July 2019**

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

C

Financial statements

Statement of comprehensive net expenditure for the year ended 31 March 2019

	Note	2018-19 £'000	2018-19 £'000	2017-18 £'000	2017-18 £'000
Expenditure					
Staff costs	3		29,043		18,580
Other expenditure	4	13,689		8,431	
Depreciation and other non-cash costs	4	584	14,273	445	8,876
Total expenditure			43,316		27,456
Income					
Income from activities	5a		(39,980)		(21,838)
Net expenditure			3,336		5,618
Other comprehensive expenditure					
Net (gain)/loss on revaluation of property, plant and equipment			0		323
Total comprehensive expenditure for the year ended 31 March			3,336		5,941

Note:
All income and expenditure relates to continuing operations.

The notes on pages 102 to 115 form part of these financial statements.

Statement of financial position as at 31 March 2019

	Note	31 March 2019 £'000	31 March 2019 £'000	31 March 2018 £'000	31 March 2018 £'000
Non-current assets					
Property, plant and equipment	6	1,839		1,658	
Intangible assets	7	36		148	
Total non-current assets			1,875		1,806
Current assets					
Trade and other receivables	9	6,420		3,466	
Cash and cash equivalents	10	3,101		2,923	
Total current assets			9,521		6,389
Total assets			11,396		8,195
Current liabilities					
Trade and other payables	11		(8,647)		(5,120)
Provisions	12		(35)		(9)
Non-current assets plus net current assets			2,714		3,066
Non-current liabilities					
Provisions	12		(510)		(641)
Assets less liabilities			2,204		2,425
Taxpayers' equity					
Revaluation reserve		—		—	
General reserve		2,204		2,425	
			2,204		2,425

The notes on pages 102 to 115 form part of these financial statements.

Elizabeth Denham
1 July 2019

Statement of cash flows for the year ended 31 March 2019

	Note	2018-19 £'000	2017-18 £'000
Cash flows from operating activities			
Net expenditure		(3,336)	(5,618)
Adjustment for non-cash items	3,4,12	708	890
Decrease/(increase) in trade and other receivables	9	(1,000)	(640)
Increase/(decrease) in trade payables	11	1,923	381
Use of provisions	12	(10)	(9)
Net cash outflow from operating activities		(1,715)	(4,996)
Cash flows from investing activities			
Purchase of property, plant and equipment	6	(623)	(981)
Purchase of intangible assets	7	(30)	(23)
Net cash outflow from investing activities		(653)	(1,004)
Cash flows from financing activities			
Grant in aid received from the DCMS	1.3	2,896	5,195
Net cash inflow from financing activities		2,896	5,195
Net increase/(decrease) in cash and cash equivalents during the year before adjustment for receipts and payments to the Consolidated Fund		528	(805)
Receipts due to the Consolidated Fund which are outside the scope of the Information Commissioner's activities		2,990	2,132
Payments of amounts due to the Consolidated Fund		(3,340)	(2,033)
Net increase/(decrease) in cash and cash equivalents in the year after adjustment for receipts and payments to the consolidated fund		178	(706)
Cash and cash equivalents at the start of the year		2,923	3,629
Cash and cash equivalents at the end of the year	10	3,101	2,923

The notes on pages 102 to 115 form part of these financial statements.

Statement of changes in taxpayers' equity for the year ended 31 March 2019

	Note	Revaluation reserve £'000	General reserve £'000	Total reserves £'000
Balance at 31 March 2017		323	2,659	2,982
Changes in tax payers' equity 2017-18				
Grant in aid from the DCMS	1.3	—	5,195	5,195
Transfers between reserves		—	—	—
Comprehensive expenditure for the year		(323)	(5,618)	(5,941)
Non-cash charges – Information Commissioner's salary costs	3	—	189	189
Balance at 31 March 2018		—	2,425	2,425
Changes in tax payers' equity 2018-19				
Grant in aid from the DCMS		—	2,896	2,896
Transfers between reserves		—	—	—
Comprehensive expenditure for the year		—	(3,336)	(3,336)
Non-cash charges – Information Commissioner's salary costs		—	219	219
Balance at 31 March 2019		—	2,204	2,204

The notes on pages 102 to 115 form part of these financial statements.

Notes to the accounts

1. Statement of accounting policies

These financial statements have been prepared in accordance with the 2018-19 Government Financial Reporting Manual (FReM) issued by HM Treasury. The accounting policies contained in the FReM apply International Financial Reporting Standards (IFRS) as adapted or interpreted for the public sector context. Where the FReM permits a choice of accounting policy, the accounting policy which is judged most appropriate to the particular circumstances of the Information Commissioner for the purpose of giving a true and fair view has been selected. The particular policies adopted by the Information Commissioner are described below. They have been applied consistently in dealing with items that are considered material to the accounts.

1.1 Accounting convention

These accounts have been prepared under the historical cost convention modified to account for the revaluation of property, plant and equipment and intangible assets at their value to the business by reference to current costs.

1.2 Disclosure of IFRSs in issue but not yet effective

The Information Commissioner has reviewed the IFRSs in issue but not yet effective (as below), and has determined that there is a new standard that is likely to have a significant impact.

Standard	Impact
IFRS 16 – Leases	Implemented in January 2019. This standard will impact on the accounting treatment of any current leases and will have a material effect on the accounts of the ICO. All leases will be required to be presented on the Statement of Financial Position except those considered out of scope. The estimated impact of IFRS 16 has been calculated to show a use of asset to be brought onto the balance sheet as £4.3m. There is a corresponding £4.3m increase in liabilities.

1.3 Grant in aid

Grant-in-aid is received from the DCMS to fund expenditure on freedom of information work, and is credited to the General Reserve on receipt. In 2017/18, the ICO received additional Grant-in-Aid to cover expansion plans in relation to General Data Protection Regulation legislation. This was paid back over the 12 month period to 31 March 2019.

1.4 Cash and cash equivalents

Cash and cash equivalents recorded in the Statement of Financial Position (SoFP) and Statement of Cash Flows include cash in hand, deposits held at call with banks, other short-term highly liquid investments and bank overdrafts.

1.5 Income from activities and Consolidated Fund income

Income collected under the Data Protection Act 1998 and subsequent Data Protection Act 2018 is surrendered to the DCMS as Consolidated Fund income, unless the DCMS (with the consent of the Treasury) has directed otherwise, in which case it is treated as Income from activities. There are three main types of income collected:

Data protection notification fees

Fees are collected from annual notification fees paid by data controllers required to notify their processing of personal data under the Data Protection Act 1998 until 25 May 2018 and subsequently the Data Protection Act 2018. The Information Commissioner has been directed to retain the fee income collected to fund data protection work and this is recognised in the Statement of Comprehensive Net Expenditure as income. At the end of each year, the Information Commissioner may carry forward to the following year sufficient fee income to pay year end creditors. Any fees in excess of the limits prescribed within the Management Agreement with DCMS are paid over to the Consolidated Fund. Under IFRS 15, if an entity does not satisfy a performance obligation over time, the performance obligation is satisfied at a point in time. As fees are recognised and used in the year in which they are received, then under IFRS 15 the performance obligations are considered to have been satisfied at a point in time. The introduction of IFRS 15 has not impacted on the timing of recognition for notification fees.

Civil monetary penalties

The Information Commissioner can impose civil monetary penalties for serious breaches of the DPA or PECR of up to £500k up to 25 May 2018 and up to 4% of global turnover thereafter. A penalty can be reduced by 20% if paid within 30 days of being issued.

The Information Commissioner can impose fines for not paying the data protection fee up to a maximum of £4,350 under the Data Protection Act 2018.

The Information Commissioner does not take action to enforce a civil monetary penalty unless and until the period specified in the notice as to when the penalty must be paid has expired and the penalty has not been paid, all relevant appeals against the monetary penalty notice and any variation of it have either been decided or withdrawn, and the period for the data controller to appeal against the monetary penalty and any variation of it has expired.

Civil monetary penalties collected by the Information Commissioner are recognised on an accruals basis when issued. They are paid over to the Consolidated Fund, net of any early payment reduction when received. Civil monetary penalties are not recognised in the Statement of Comprehensive Net Expenditure, but are treated as a receivable and payable in the Statement of Financial Position.

The amounts recognised are regularly reviewed and subsequently adjusted in the event that a civil monetary penalty is varied, cancelled, impaired or written off as irrecoverable. Amounts are written off as irrecoverable on the receipt of legal advice. Legal fees incurred in recovering debts are borne by the ICO.

Sundry receipts
The Information Commissioner has been directed to retain certain sundry receipts such as other legislative funding, grants, management charges, reimbursed travel expenses and recovered legal costs. This is recognised in the Statement of Comprehensive Net Expenditure as income.

The Information Commissioner has interpreted the Financial Reporting Manual (FReM) to mean that she is acting as a joint agent with the DCMS, and that income not directed to be retained as Income from Activities falls outside of normal operating activities and are not reported through the Statement of Comprehensive Net Expenditure, but disclosed separately within the notes to the accounts. This included receipts such as bank interest, which is paid to the Consolidated Fund.

1.6 Notional costs

The salary and pension entitlement of the Information Commissioner are paid directly from the Consolidated Fund and are included within staff costs and reversed with a corresponding credit to the General Reserve.

1.7 Pensions

Past and present employees are covered by the provisions of the Principal Civil Service Pensions Scheme.

1.8 Property, plant and equipment

Assets are classified as property, plant and equipment if they are intended for use on a continuing basis, and their original purchase cost, on an individual basis, is £2,000 or more, except for laptop and desktop computers, which are capitalised even when their individual cost is below £2,000.

Property, plant and equipment (excluding assets under construction) is valued under a depreciated historical cost basis as a proxy for current value in existing use or fair value for assets that have short useful lives or low values.

At each balance sheet date the carrying amounts of property, plant and equipment and intangible assets are reviewed to determine whether there is any indication that those assets have suffered an impairment loss. If any such indication exists the fair value of the asset is estimated in order to determine the impairment loss. Any impairment charge is recognised in the Statement of Comprehensive Net Expenditure account in the year in which it occurs.

1.9 Depreciation

Depreciation is provided on property, plant and equipment on a straight-line basis to write off the cost or valuation evenly over the asset's anticipated life. A full year's depreciation is charged in the year in which an asset is brought into service. No depreciation is charged in the year of disposal. The principal lives adopted are:

Information technology	Between 5 and 10 years
Plant and machinery	Between 5 and 10 years
Leasehold improvements	Over the remainder of the property lease

1.10 Intangible assets and amortisation

Intangible assets are stated at the lower of replacement cost and recoverable amount. Computer software licences and their associated costs are capitalised as intangible assets where expenditure of £2,000 or more is incurred. Software licences are amortised over their useful economic life which is estimated as four years or the length of the contract, whichever is the shorter term.

1.11 Operating leases

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

1.12 Provisions

Provisions are recognised when there is a present obligation as a result of a past event where it is probable that an outflow of resources will be required to settle the obligation and a reliable estimate of the amount of the obligation can be made.

1.13 Value added tax

The Information Commissioner is not registered for VAT as most activities of the Information Commissioner's Office are outside of the scope of VAT. VAT is charged to the relevant expenditure category, or included in the capitalised purchase cost of non-current assets.

1.14 Segmental reporting

The policy for segmental reporting is set out in note two to the Financial statements.

2. Analysis of net expenditure by segment

	Data protection	Freedom of information	Other grant in aid	2018-19 Total
	£'000	£'000	£'000	£'000
Gross expenditure	40,920	3,750	(1,354)	43,316
Income	(39,980)	–	–	(39,980)
Net expenditure	940	3,750	(1,354)	3,336

	Data protection	Freedom of information	Other grant in aid	2017-18 Total
	£'000	£'000	£'000	£'000
Gross expenditure	22,261	3,750	1,445	27,456
Income	(21,838)	–	–	(21,838)
Net expenditure	423	3,750	1,445	5,618

Expenditure is classed as administrative expenditure except those costs associated with readiness for legislative changes which have been classified as programme.

The analysis above is provided for fees and charges purposes and for the purpose of IFRS 8: Operating Segments.

The factors used to identify the reportable segments of data protection and freedom of information are that the Commissioner's main responsibilities were contained within the DPA 98 (until 25 May 2018 and DPA 2018 thereafter) and FOIA, and funding during 2018-19 and in prior years was provided for data protection work by collecting an annual registration fee from data controllers under the DPA, whilst funding for freedom of information is provided by a grant in aid from the DCMS. Other Grant in Aid related to £500k for network infrastructure and systems regulation, £46k for electronic identification and trust services regulation and less £1.4m by way of a reduction in Grant in Aid following an increased Grant in Aid of £1.4m in the prior year plus £45k for electronic identification and trust services regulation.

The data protection notification fee was set by the Secretary of State, and in making any fee regulations under section 26 of the DPA 1998 and subsequently section 134 of the DPA 2018, as amended by paragraph 17 of Schedule 2 to the FOIA, the Secretary of State had to have regard to the desirability of securing that the fees payable to the Commissioner were sufficient to offset the expenses incurred by the Commissioner, the Information Tribunal and any expenses of the Secretary of State in respect of the Commissioner of the Tribunal, and any prior deficits incurred, so far as attributable to the functions under the DPA 2018.

These accounts do not include the expenses incurred by the Information Tribunal or the Secretary of State in respect of the Commissioner, and therefore cannot be used to demonstrate that the data protection fees offset expenditure on data protection functions, as set out in the DPA 2018.

Expenditure is apportioned between the data protection and freedom of information work on the basis of costs recorded in the ICO's accounting system. This allocates expenditure to various cost centres across the organisation. A financial model is then applied to apportion expenditure between data protection and freedom of information on an actual basis, where possible, or by way of reasoned estimates where expenditure is shared.

3. Staff numbers and related costs

Staff costs comprise:

	Permanently employed staff	Others	2018-19 Total	2017-18 Total
	£'000	£'000	£'000	£'000
Wages and salaries	20,972	1,868	22,840	14,517
Social security costs	2,154	–	2,154	1,331
Other pension costs	4,050	–	4,050	2,732
Sub-total	27,176	1,868	29,044	18,580
Less recoveries in respect of outward secondments	(1)	–	(1)	–
Total net costs	27,175	1,868	29,043	18,580

Included in staff costs above are notional costs of £220k (2017-18: £190k) in respect of salary and pension entitlements of the Information Commissioner and the associated employers national insurance contributions which are credited directly to the General Reserve, temporary agency staff costs of £1.415m (2017-18: £508k) and inward staff secondments of £453k (2017-18: £109k) as well as the amounts disclosed in the Remuneration Report.

Average number of persons employed
The average number of whole time equivalent persons employed during the year was:

	Permanently employed staff	Temporarily employed staff	2018-19 Total	2017-18 Total
Directly employed	601	5	606	466
Agency staff	–	32	32	14
Total employed	601	37	638	480

Pension arrangements
The Principal Civil Service Pension Scheme (PCSPS) is an unfunded multi-employer defined benefit scheme. The Information Commissioner is unable to identify its share of the underlying assets and liabilities. The Scheme Actuary valued the scheme at 31 March 2015. Details can be found in the resource accounts of the Cabinet Office Civil Superannuation (www.civilservice.gov.uk/pensions).

For 2018-19 employers contributions of £3.866m (2017-18: £2.643m) were payable to the PCSPS at one of four rates in the range 20% to 24.5% of pensionable pay, based on salary bands. The Scheme's Actuary reviews employer contributions usually every four years following a full Scheme valuation. The contribution rates are set to meet the cost of benefits accruing during 2018-19 to be paid when the member retires and not the benefits paid during the period to existing pensioners.

Employees can opt to open a 'Partnership' account, a stakeholder pension with an employer contribution. Employers' contributions of £142k (2017-18: £88k), were paid to one or more of a panel of three appointed stakeholder pension providers for the period from April to

September 2018. In October 2018 Partnership pension arrangements were changed and contributions are now paid to a single provider. Employers' contributions are age related and range from 8% to 14.75% of pensionable pay. If an employee choses to contribute to the pension, the employer will also match those contributions up to a maximum of an additional 3% of salary. In addition, employer contributions of £4.9k (2017-18: £2.9k), 0.5% of pensionable pay, were payable to the Principal Civil Service Pension Scheme to cover the cost of future provision of lump sum benefits on death in service and ill health retirement of these employees.

Contributions due to partnership pension providers at the Statement of Financial Position date were £6.6k (2017-18 £8.7k). Contributions prepaid at this date were £nil (2017-18 £nil).

Other pension costs include notional employers' contributions of £39k (2017-18: £34k) in respect of notional costs in respect of the Information Commissioner.

No individuals retired early on health grounds during the year.

4. Other expenditure

	2018-19		2017-18	
	£'000	£'000	£'000	£'000
Accommodation (business rates and services)	698		582	
Rentals under operating leases	1,060		571	
Office supplies and stationery	168		426	
Carriage and telecommunications	58		55	
Travel and subsistence	1,022		621	
Staff recruitment	579		288	
Specialist assistance and policy research	2,880		658	
Communications and external relations	834		403	
Legal costs	974		666	
Learning and development, health and safety	520		348	
IT Service delivery costs	3,302		2,720	
IT development costs	1,291		997	
Audit fees	30		30	
Grants Fund	273		66	
		13,689		8,431
Non-cash items				
Depreciation	439		323	
Amortisation	141		119	
Loss on disposal of assets	4		3	
		584		445
Total expenditure		14,273		8,876

5. Income

5a. Income from activities

	2018-19		2017-18
	£'000	£'000	£'000
Fees	39,256	21,300	
Sundry receipts	724	538	
		39,980	21,838

5b. Consolidated Fund income

	2018-19		2017-18
	£'000	£'000	£'000
Fees			
Collected under the DPA	39,256	21,300	
Retained under direction as Income from Activities	(39,256)	(21,300)	
		–	–
Civil Monetary Penalties - Investigations			
Penalties issued	5,436	4,810	
Early payment reductions	(663)	(501)	
Repaid following a successful appeal	–	–	
Cancelled after successful appeals	–	–	
Re-issued after appeal	–	–	
Impairments	–	(429)	
		4,773	3,880
Civil Monetary Penalties - Non payment of fees			
Penalties Issued	171		
Impairments	–	–	
		171	–
Sundry receipts			
Receipts under the Proceeds of Crime Act	–	–	
Grant income (repaid)	–	–	
Bank interest received	–	–	
Recovered legal fees	11	101	
Reimbursed travel expenses	36	23	
Conference fees	52	41	
Management Fee from Telephone Preference Service	12	–	
Income received from The Regulatory Pioneers Fund	279	–	
Income receipts under the Data Retention and Investigatory Powers Act	330	330	
Marketing income	4	43	
	724	538	
Sundry receipts retained under direction as Income from Activities	(724)	(538)	
		–	–
Income payable to Consolidated Fund		4,944	3,880
Balances held at the start of the year		2,939	1,092
Income payable to the Consolidated Fund		4,944	3,880
Payments to the Consolidated Fund		(3,340)	(2,033)
Balances held at the end of the year (note 11)		4,543	2,939

As set out in note 1.5 income payable to the Consolidated Fund does not form part of the Statement of Comprehensive Net Expenditure. Amounts retained under direction from the DCMS with the consent of the Treasury are treated as income from activities within the Statement of Comprehensive Net Expenditure. The amounts receivable at 31 March 2019 were £4.149m (2017-18: £2.343m) and the amounts payable were £4.389m (2017-18: £2.939m).

6. Property, plant and equipment

	Information technology	Plant and machinery	Leasehold improvements	Assets under construction	2019 Total	2018 Total
	£'000	£'000	£'000	£'000	£'000	£'000
Cost or valuation						
At 01 April 2018	7,488	257	2,375	621	10,741	11,102
Additions	436	31	7	149	623	981
Transfers	–	–	–	–	–	–
Disposals	(148)	–	–	–	(148)	(313)
Revaluations	–	–	–	–	–	(773)
Impairment	·	–	–	–	–	(256)
At 31 March 2019	7,776	288	2,382	770	11,216	10,741
Depreciation						
At 01 April 2018	6,653	100	2,330	–	9,083	9,520
Charged in year	378	48	13	–	439	323
Disposals	(145)	–	–	–	(145)	(311)
Revaluations	·	–	–	–	–	(449)
At 31 March 2019	6,886	148	2,343	–	9,377	9,083
Net book value at 31 March 2019	890	140	39	770	1,839	1,658
Owned	890	140	39	770	1,839	1,658
Net book value at 31 March 2019	890	140	39	770	1,839	1,658

Property, plant and equipment (excluding assets under construction) is valued under a depreciated historical cost basis as a proxy for current value in existing use or fair value for assets that have short useful lives or low values. This is considered an appropriate model for all classes of assets as the majority have useful lives of 5 years or are considered an immaterial value.

7. Intangible assets

	Software licences	Assets under construction	2019 Total	2018 Total
	£'000	£'000	£'000	£'000
Cost or valuation				
At 1 April 2018	3,403	–	3,403	3,380
Additions	30	–	30	23
Disposals	(54)	–	(54)	–
Transfers		–		–
Reclassifications	–	–	–	–
At 31 March 2019	3,379	–	3,379	3,403
Amortisation				
At 1 April 2018	3,255	–	3,255	3,136
Charged in year	141	–	141	119
Disposals	(53)	–	(53)	–
At 31 March 2019	3,343	–	3,343	3,255
Net book value at 31 March 2019	36		36	148
Asset financing				
Owned	36	–	36	148
Net book value at 31 March 2019	36	–	36	148

8. Financial instruments

As the cash requirements of the Information Commissioner are met through fees collected under the Data Protection Act 1998, subsequently Data Protection Act 2018 and grant-in-aid provided by the DCMS, financial instruments play a more limited role in creating and managing risk than would apply to a non-public sector body.

The majority of financial instruments relate to contracts to buy non-financial items in line with the Information Commissioner's expected purchase and usage requirements and the Information Commissioner is therefore exposed to little credit, liquidity or market risk.

As a result, the impact of adopting IFRS 9 has not had a material impact.

9. Trade receivables and other current assets

		31 March 2019		31 March 2018
		£'000		£'000
Amounts falling due within one year				
Trade debtors		405		142
Deposits and advances		–		–
Prepayments and accrued income		1,734		981
Sub-total		2,139		1,123
Consolidated Fund receipts due	4,297		2,772	
less amounts impaired (note 5b)	–		(429)	
Other	(16)		–	
		4,281		2,343
		6,420		3,466
Split:				
Other central government bodies		354		225
Local authorities		–		75
NHS Bodies		12		–
Bodies external to government		6,054		3,166
		6,420		3,466

10. Cash and cash equivalents

	31 March 2019	31 March 2018
	£'000	£'000
Balance at 1 April	2,923	3,629
Net change in cash and cash equivalent balances	178	(706)
Balance at 31 March	3,101	2,923
Split:		
Commercial banks and cash in hand	2,146	2,563
Government Banking Service	955	360
	3,101	2,923

11. Trade payables and other current liabilities

	31 March 2019	31 March 2018
	£'000	£'000
Amounts falling due within one year		
Taxation and social security	621	665
Trade payables	568	358
Other payables	1,155	576
Accruals and deferred income	1,760	582
Sub-total	4,104	2,181
Amount payable to government (note 5b)	4,543	2,939
	8,647	5,120

Split:		
Sponsor department - DCMS	4,543	2,939
Other central government bodies	621	665
Bodies external to government	3,483	1,516
	8,647	5,120

The amount payable to the sponsor department represents the amount which will be due to the Consolidated Fund when all of the income due is collected.

12. Provision for liabilities and charges

	Dilapidations		Early departure costs	
	2018-19	2017-18	2018-19	2017-18
	£'000	£'000	£'000	£'000
Balance at 1 April	605	605	45	54
Provided in year	(95)[ᵏ]	–	–	–
Provision utilised in year	–	–	(10)	(9)
Balance at 31 March	510	605	35	45

[ᵏ]This represents a reassessment of the provision

Analysis of expected timing of discounted flow:

	Dilapidations		Early departure costs	
	2018-19	2017-18	2018-19	2017-18
	£'000	£'000	£'000	£'000
Not later than one year	–	–	35	9
Later than one year and not later than five years	510	605	–	36
Later than five years	–	–	–	–
	510	605	35	45

Dilapidations provision
The lease on the ICO main premises at Wycliffe House, Wilmslow expired on 1 January 2017 and a new lease was signed with a break clause in 5 years. Further leases were entered into during the period (see note 14) with no dilapidations deemed applicable as at 31 March 2019. A provision has been made based upon the assessment by GVA, commercial property advisers, dated January 2013. A full dilapidation report will be completed across the full Wilmslow estate during 2019/20.

The ICO also occupies government properties in Edinburgh and Cardiff under Memorandum of Terms of Occupation agreements ending 2016 and 2024 respectively. Under these agreements, the ICO may have dilapidations liabilities at the end of the term of occupation but these are considered immaterial to recognise further.

Early departure costs
The additional cost of benefits, beyond the normal PCSPS benefits in respect of employees who retire early, are provided for in full when the early departure decision is approved by establishing a provision for the estimated payments discounted by the Treasury discount rate of 0.10% (2017-18: 0.10%). The estimated payments are provided by MyCSP.

13. Capital commitments

There were no capital commitments in the year ending 31 March 2019 (2017-18 £nil).

14. Commitments under operating leases

The ICO leases properties in Wilmslow, Belfast, London and Cardiff under non-cancellable operating lease agreements. The lease in Wycliffe House allows for a break clause on 1 January 2022. The King's Court lease allows for a break clause on 9 August 2022. The Sandfield House lease allows for a break clause on 31 January 2024. All leases have no option to purchase and no specific renewal terms. Renewals are negotiated with the lessor in accordance with the provisions of the individual lease agreements.

Total future minimum lease payments under operating leases are:	31 March 2019 £'000	31 March 2018 £'000
Buildings		
Not later than one year	1,320	702
Later than one year and not later than five years	3,296	2,970
Later than five years	–	–
	4,616	3,672

The minimum lease payments are determined from the relevant lease agreements and do not reflect possible increases as a result of market based reviews. The lease expenditure charged to the Statement of Comprehensive Net Expenditure during the year is disclosed in note 4.

15. Related party transactions

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

During the financial year 2018-19 the DCMS was a related party to the Information Commissioner.

During the year no related party transactions were entered into, with the exception of providing the Information Commissioner with grant-in-aid, other funding and the appropriation-in-aid of Civil Monetary Penalty and sundry receipts to the Ministry of Justice for surrender to the Consolidated Fund.

In addition the Information Commissioner has had various material transactions with other central government bodies, most of these transactions have been with the Principal Civil Service Pension Scheme (PCSPS)

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

16. Contingent Liabilities

There are no contingent liabilities at 31 March 2019 (31 March 2018: none).

17. Events after the reporting period

There were no events between the Statement of Financial Position date and the date the accounts were authorised for issue, which is interpreted as the date of the Certificate and Report of the Comptroller and Auditor General.

The Accounting Officer authorised these financial statements for issue on 4 July 2019.

Notes