Information Governance Annual Report

2018/19

Contents

Executive Summary

This Information Governance Annual Report sets out how the Council has performed throughout 2018/19 against the Councils five pillars of Information Governance (IG):

- **Records Management** including email - to ensure the Council effectively manages and uses its paper and digital records
- **Publication and Transparency** - the Council should adopt a strategic and shared approach to developing a publication scheme that is up to date, relevant and easy to navigate, which will involve a Council-wide approach, centrally co-ordinated, to manage and publish relevant information
- **Information Sharing and Processing** - to enable Services to meet statutory duties and support integrated services and joint commissioning
- **Legislation compliance** with regards to Data Protection, Environmental Information and Freedom of Information
- **Organisational Culture Change** - Services develop their Information culture and effectively allocate responsibilities for Information Assets within their Service.

There have been significant achievements throughout the year including:

- The strategic leadership and management of IG for the Council has been prioritised and implemented, with mandates to the IG Board from Executive Team being raised and successfully actioned.
- The Kirklees Information Management Strategy was signed off by Executive Team and IG Board, with some key objectives being progressed within 2018/19
- The Service Directors, who are also known as Information Asset Owners, have had training updates to help them improve the management and use of the information within their areas of responsibility to ensure information is collected and stored and used appropriately.
- Information Asset Owners will ensure that the Information Asset Register is maintained for their areas of responsibility. The Information Asset Register is completed by each team as they identify information assets they are due to collect and retain as part of their work.
- Activities to ensure the complexities of the General Data Protection Regulation (GDPR) have been implemented with regular self-assessment checks being carried out by all services, demonstrating improved compliance.
- The Council has developed online systems to ensure Information Asset Register and Data Protection Impact Assessments are completed for every information asset in a way which reduces paperwork and complexity for officers.
- The Central Archive holds over 14,500 boxes of Council records, processing 20 boxes per week, and has supported Services to create 21 retention schedules.
- The Council now has an approved Cyber Security Strategy which will help drive the Councils focus on ensuring all electronic data remains secure.
- The mandatory GDPR training programme has resulted in a 100% success rate for training around the new legislation.

These achievements required the combined work from the Council's Information Governance Team and the collaboration of Officers from all Directorates and partners from across the region. These examples of strong and joined-up working practices provide confidence for the future development of the Information Governance culture within the Council.

An overview of the work carried out in 2018/19 can be found in the following pages. An outline for the work programme for 2019/20 is provided towards the end of this report, to enable understanding of how IG is being further developed and embedded within the Council in the coming year.

Recommendations

The Information Governance Board would be grateful for any comments from Members on the content of this report and ideas of what items Members would find useful to have included in future Information Governance Annual Reports.

It has been noted previously that this annual report is becoming larger each year. The Committee are asked if having a half yearly update would continue to be useful.

Introduction

Information Governance (IG) brings together all of the requirements, standards and best practice that apply to the handling of information on all media. It allows the Council to manage information in an appropriate, efficient and secure manner that balances the importance of maintaining confidentiality and individual privacy at the same time as promoting openness and transparency.

Having effective Information Governance practices:
- assists with the effective use of our information assets
- enables effective information sharing, generating useful intelligence streams
- creates an effective and dynamic organisation
- instils confidence in the citizens of Kirklees
- contributes to the management of risk
- helps officers protect the Council's reputation
- helps avoid statutory penalties

In order to achieve effective Information Governance practices the Council uses the tools within its Information Governance Framework. This framework ensures that the organisation and individuals have information that is accurate, meets legal requirements, is dealt with effectively and is secure. These are important foundations for the service delivery requirements of the Council.

The Information Governance Framework has five fundamental aims:
- To support and promote the effective and appropriate use of information
- To encourage responsible staff to work together, preventing duplication of effort and enabling more efficient use of resources
- To develop support arrangements and provide staff with appropriate tools and support to enable them to discharge their responsibilities to consistently high standards
- To enable the Council to understand performance relating to information use and manage improvement in a systematic and effective way
- To enable the effective sharing of information across Council Services and with partners

The Framework currently encompasses:
- Data Protection Act 2018 including General Data Protection Regulation (GDPR)
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Local Government Transparency Code 2014
- Kirklees Information Governance Policies including:
  - Information Governance Policy
  - Information Sharing and Processing Policy and Guidance
  - Records Management Policy and Guidance
  - Information Security Policy and Guidance
- Information Management Strategy

- Cyber Security Strategy

Background

Information Governance is a dynamic area in terms of regulation with a range of new and amended requirements each year.

Prior to 2012 the Council's focus on Information had essentially been driven by legislation compliance, including the Data Protection Act 1998, Freedom of Information Act 2000 and Environmental Information Regulations 2004. The Information Governance Team had been established for a number of years to co-ordinate and manage the requests for information from the public and their responses from Services.

In 2012 the Council appointed the position of Information Governance and Senior Support Manager. Part of this role was to take stock of the Council's Information Governance landscape and help the Council develop an Information Governance framework.

In 2013 it was identified that in order to have a consistent and Council-wide approach to Information Governance a Director-led Board was required. This Information Governance (IG) Board was established and is chaired by the Council's Senior Information Risk Officer (SIRO).

Overview of 2018/19

In May 2018, the General Data Protection Regulation (GDPR) was introduced which required the Council to refresh its approach to Data Protection in line with the new legislation. GDPR required a new role of Data Protection Officer (DPO) to be appointed by the Council, which was completed on April 2018. Whilst GDPR came into force in 2018/19, the work to prepare for this legislation was carried out for most of 2017/18.

The key headlines to note are:
- Subject Access Request requests have increased by 35.4% from 2017/18 with a reduced response rate of 73%
- Police Disclosures have reduced by 3.2% from 2017/18 with a reduced response rate of 79%
- Freedom of Information requests have increased by 9.7% from 2017/18 with an increased response rate of 89%
- There has been an increase of internal reviews, 33 up by 4 from 2017/18
- There was a reduction in complaints to the ICO with only 1 received in 2018/19

The key achievements made within 2018/19 are:

- The strategic leadership and management of IG for the Council has been prioritised and implemented, with mandates to the IG Board from Executive Team being raised and successfully actioned.
- The Kirklees Information Management Strategy was signed off by Executive Team and IG Board, with some key objectives being progressed within 2018/19
- The Service Directors, who are also known as Information Asset Owners, have had training updates to help them improve the management and use of the information within their areas of responsibility to ensure information is collected and stored and used appropriately.
- Information Asset Owners will ensure that the Information Asset Register is maintained for their areas of responsibility. The Information Asset Register is completed by each team as they identify information assets they are due to collect and retain as part of their work.
- Activities to ensure the complexities of the General Data Protection Regulation (GDPR) have been implemented with regular self-assessment checks being carried out by all services, demonstrating improved compliance.
- The Council has developed online systems to ensure Information Asset Register and Data Protection Impact Assessments are completed for every information asset in a way which reduces paperwork and complexity for officers.
- The Central Archive holds over 14,500 boxes of Council records, processing 20 boxes per week, and has supported Services to create 21 retention schedules.
- The Council now has an approved Cyber Security Strategy which will help drive the Councils focus on ensuring all electronic data remains secure.
- The mandatory GDPR training programme has resulted in a 100% success rate for training around the new legislation.

Governance

The IG Board has an established approach to policy review which means that all of the IG related policies are reviewed and updated annually at the IG Board. These Policies form part of the Information Governance Framework which provides the foundation for the Council's Information Governance work.

The IG Board performs a council-wide, strategic role for Information Governance, supported by more operational task groups. The IG Board is made up of representatives from each directorate, who take back tasks and key strategic messages/actions from the Board to their Directorate areas. The Terms of Reference for the IG Board can be found in Appendix A.

In 2018/19 the task groups were adjusted to focus solely on GDPR implementation and the wider strategic records management work which was identified as a priority in 2017/18.

The GDPR Implementation Task Group meets every month to be updated on developments and provide peer support for GDPR implementation activities. This group is continuing to meet monthly and ensure that GDPR implementation becomes business as usual.

The Electronic Records Management Task Group has been investigating the breadth of the records management concerns within the council. The group's investigations have prompted a focus on the storage of staff records and work will continue on this into 2019/20.

Activities completed through 2018/19

More detail of the IG work carried out through the financial year is outlined below. Further reports to support these summaries can be found in the appendices.

Kirklees Information Management Strategy

The Information Management Strategy provides the bedrock for the activities relating to information between 2018 and 2021. The strategy was developed following extensive consultation with Council officers and Partners. These conversations were analysed to identify coordinating themes. These themes have become the overarching objectives of the strategy. The strategy objectives are:
- To ensure we are embedding the requirements of the General Data Protection Regulation (GDPR)
- Using information to create a resource for decision making
- To unlock the value of data, where it sits and how it travels, allowing the Council to have a strategic overview of its information
- Support culture change – to improve awareness of the importance of information management and embed excellent IM practices throughout the organisation
- To improve citizen experience through 'tell us once'
- Train staff understand the value of information – in order to maximise access to high quality information in order for all staff to be able to unlock the value within
- Encourage collaborative working – by breaking down communication and technological barriers that prevent information from being shared appropriately
- Implement a more proactive information management function – focussing on communications, training and prevention rather than remediation
- Embed a collaborative culture - where knowledge is actively shared without compromising confidentiality
- Services work closely with IG and IT - to ensure appropriate infrastructure is available to support excellent information management

The following specific tasks are set to be achieved before 2021:
- Develop and maintain the information asset register
- Provide a simple and secure method for sharing confidential information
- Develop a programme of training and support for change

- Develop the intelligence hub – which will focus on data driven decision making for the Council
- Complete a meta data project that will improve the use of meta data and make information easier to use, retrieve and manage
- Build information management as standard into projects, processes and systems
- System rationalisation must be considered when purchasing new data driven systems
- Implement privacy by design and default where information governance considerations are taken into account at the start of new projects
- Proactively publish more information, in order to reduce information access demand and improve transparency for the general public

Many of these activities are outlined as progress updates in this report. There is much work to complete, so the activities relating to these objectives will also be reported in future Annual Reports.

A copy of the full Information Management Strategy can be found in Appendix B

Data Protection

The topic of Data Protection is primarily focussed on the safe keeping of personal data about individuals. This is a very high priority for the Council and its partners, as we serve a diverse range of people and therefore data protection relates to a significant volume of data across the Council.

Legislation Changes – General Data Protection Regulation

The General Data Protection Regulation (GDPR) came into force on **May 25th 2018** and replaced the Data Protection Act (1998). Many of the concepts and principles of the old Data Protection Act (DPA98) are the same within the GDPR however there are some new elements and some significant enhancements, so the Council needed to approach data protection differently as an organisation.

GDPR places greater emphasis on the documentation that the Council must keep to demonstrate our accountability. Compliance requires the Council to revisit our approach to information governance and emphasises how we must manage data protection as a corporate issue.

The legislation expands the potential for breaches and increases the possible fines from £500,000 under the Data Protection Act (1998) to **€20,000,000** under GDPR.

GDPR applies to ALL personal information collected and used. It places greater emphasis on:
- the documentation that the Council must keep to demonstrate accountability
- the speed the Council must respond to requests for personal information (from 40 days to 30 days)
- the ability of the council to delete or stop processing personal data about an individual if collected using specific lawful bases

- reporting all information security incidents over a set threshold to the ICO within 72hours
- having a full, clear and up to date view on what personal information is held by the Council, and which organisations this information is shared with
- updating and communicating information use to the public through privacy notices
- holding a thorough and current information processing log for all appropriate contracts
- appointing a Data Protection Officer, focussing on Data Protection, operating independently and reporting to the Chief Executive
- ensuring Data Protection by Design across all Service areas utilising Privacy Impact Assessments for all projects

To help the Council prepare appropriately for GDPR, the Executive Team granted a mandate to the IG Board which required all heads of service to support the GDPR preparations. In so doing, each service representative was invited to attend fortnightly meetings throughout 2017/18 which focused on GDPR preparation. At these meetings key preparation activities were discussed, appropriate solutions were identified and colleagues from across the Council were able to support one another with their preparations for legislation change.

These meetings have continued throughout 2018/19 but on a monthly basis. The purpose of these meetings has been to provide updates on the new legislation, as the ICO continued to provide further guidance around compliance. They also allowed the service representatives to meet and discuss approaches which were working, which helped provide peer support across the organisation. Throughout the year services have identified information asset coordinators, who are individuals to help services identify their GDPR compliance requirements. These individuals will be supported through the coming financial year, with their data protection responsibilities.

The IG Board and Executive Team have been updated regularly throughout the year on progress towards and maintain GDPR compliance. This is carried out through the GDPR assurance project. This project is run on a 6 monthly basis to identify the status of each service with regards to their legislative compliance. The results of the September 2018 and April 2019 self-assessment can be found in Appendix C

The new legislation is introduced a number of additional ways in which individuals can access the personal data held by an organisation. These rights are outlined here.

GDPR Individual Rights - Data Protection Information Requests

Data Protection Information requests are managed and coordinated centrally from the Democracy Service within the Information Governance Team and also within some specific service areas. The published figures for data protection requests, known as Subject Access Requests (SARs), show a significant increase of **35.4%** on last year from 223 in 2017-18 to 302 in 2018-19.

The response rate by Kirklees Council to these requests has decreased from **83%** compliance in 2017-18 to **73%** compliance in 2018-19. This is well below the ICO's required compliance rate of 90% within the statutory timescale (40 calendar days under the Data Protection Act 1998 and one month under the General Data Protection Regulation). More detail on these figures can be found in Appendix D

Disclosures

In addition to the Subject Access Requests received by individuals, the Council is committed to assisting the law enforcement agencies in their investigations whilst still achieving compliance with the Data Protection Act 1998. These requests are termed Disclosures.

There are no measured response deadlines for Disclosures; however the Council uses the SAR response deadline measurement timescale (40 calendar days under the Data Protection Act 1998 and one month under the General Data Protection Regulation which came into force on 25 May 2018) to assist with monitoring performance around disclosures.

On that basis, in 2018-19 the Council received 422 disclosure requests which is a slight decrease of less than 3.2% on the number received in 2017-18 (436) and achieved a 79% response rate within the timescale outlined above, which is less than the 93% rate in 2017-18.

Freedom of Information Act 2000 & Environmental Information Regulations 2004

This section details how the Council has performed throughout the 2018/19 year in respect of information access requests received and processed under the Freedom of Information Act 2000 (FoI) and Environmental Information Regulations 2004 (EIR).

The Act and the Regulations require public authorities, including the Council, to reply to information requests within 20 working days - either providing the information or saying why it cannot be provided.

The Council received 1660 requests during 2018-19 which is 147 more than the number received in 2017-18, which is a 9.7% increase.

The Council's compliance rate for responding to requests has increased to 89% which is just below the Information Commissioner's Office (ICO) current minimum standard of 90% of responses should be sent out within deadline. It is an improvement on performance in 2017-18, which was 87%.

Compliance rates have fluctuated during 2018-19, ranging from 81.3% in June 2018 up to 96.3% in November 2018; both figures are an improvement on the highest and lowest figures from 2017-18.

The average response time for 2018-19 was 14.2 working days, a slight improvement on 14.5 working days in 2017-18.

The increase in the volume of requests received is a common theme across most of the West Yorkshire Councils, Kirklees has the lowest increase at 9.7%, two other Councils having had increases of between 11.5% and 22.2% from the previous year.

Internal reviews and Complaints

The number of internal reviews carried out of the responses to requests has increased slightly on the previous year, to 33 in 2018-19 from 29 in 2017-18. A quarter were dealt with within the timescale set out in the EIR and suggested by the ICO for FoI; the Council has some work to do to ensure that internal reviews are concluded in a more timely manner.

The number of complaints made to the ICO has decreased by 4, from 5 in 2017-18 to just 1 in 2018-19. The ICO issued a Decision Notice in respect of this one complaint, directing the Council to disclose the information it had withheld. The Council appealed to the First Tier Tribunal (Information Rights) which determined that only some of the information should be disclosed and the remainder withheld as the Council had originally done.

The IG Board reviews FoI response figures at each meeting, which helps raise the profile of any specific difficulties when they arise. In addition to this, discussions at Executive Team have centred on responding to information requests following the increase in focus of GDPR requirements. This has meant that an urgency to respond to FoI requests in a more timely and consistent manner was recognised with new response procedures have been established for 2018/19.

More detail on the FoI and EIR response rates for 2018-19 is included in the Freedom of Information Act 2000 and Environmental Information Regulations 2004 Annual Report in Appendix E

NHS Data Security and Protection Toolkit Accreditation

In 2014/15 it was identified that in order to establish, strengthen and maintain partnership relations with national government and the NHS, the Council would have to annually prove their IG credibility by achieving the IG Toolkit to a level 2 accreditation level.

In 2018/19 NHS Digital replaced the IG Toolkit with the Data Security and Protection Toolkit. Further details about this Toolkit and accreditation process can be found here.

Achieving this standard requires significant resource investment and compliance with rigorous IG standards by the whole organisation. The DSP toolkit does not have a scoring mechanism, the local authority is defined as either passing or failing depending on its response to mandatory questions.

The successful submission for 2018/19 was made to NHS Digital in February 2019 once it had been verified by Internal Audit and signed off by the IG board. It demonstrates the strong and continued positive change across Council departments towards effective and secure information governance.

Data Sharing

To achieve effective, streamlined services, both internally and with partners, it is vital that the information held is shared effectively and in line with the Data Protection Act. There are a range of reasons why data must be shared and there are also legislative reasons why data must not be shared. It is very important that the culture of the Council is focussed on achieving a modern and efficient approach to information sharing whilst maintaining data security and ensuring data sharing uses established legal gateways or the full consent of the individual. It is the role of the Information Governance team within the Council to perform the enabling role required by Council Services to ensure data can be shared with colleagues and Partners.

This is essential for the future, as the organisation will be working more closely with community partners to commission and deliver joined services which require sharing personal information. In order to achieve these requirements, it is important that Information Governance is considered within all arrangements to enable effective and legal data sharing between Council Services and also between the Council and Partners.

Whenever data is shared, there must be an agreement in place which identifies the requirements of the data sharing exercise and also the potential legal gateways which are being utilised, or a full record of consent by the individuals concerned, if Personal Data is being shared.

The council has established information sharing agreements with all of our regular partners. Sharing agreements need to be set up with all other data controllers. Therefore sharing agreements have been set up with all councillors, as councillors are separate data controllers to the council.

On a wider scale the Council is one of the 45 signatories to the West Yorkshire Inter-Agency Information Sharing Protocol. This protocol sets out the requirements for the signatories to utilise when sharing information between each other, which makes the sharing process much more effective and efficient.

Information Security

Historically, whilst information security incidents occurred, they were not generally reported as there was not a wider awareness of what an information security incident was or what an individual should do about it. This can be demonstrated from past incident records, as seen below:

Annual Year	Number of incidents
2014/15	54
2015/16	49
2016/17	56
2017/18	93

The introduction of GDPR in May 2018 brought a mandatory requirement to report high risk information security incidents to the Information Commissioner's Office within 72 hours of a breach occurring.

To enable the Council to respond appropriately, an online information security incident form was rolled out for all officers to utilise in the event of an incident. This was launched and promoted across the Council by the IG Team using the Spotlight system. The intranet pages on information security were also updated to correspond with this awareness raising. This was done alongside and in addition to the GDPR communications messages which were sent out to all teams. With this increased awareness around information security incidents and the improved reporting mechanism the situation around incidents changed dramatically

The online reporting tool has a scoring mechanism built into the software. The score of an incident is applied depending upon which answers the officer reporting selects. Therefore an incident relating to an email containing a single individual's name and address being sent to the wrong recipient would score lower than an email containing the personal and health details of 500 individuals. This scoring approach allows the IG Team to conduct an initial assessment of the priority of the incidents coming in. If, after further investigation, it is considered that the incident meets the requirement to report, the incident details are raised with senior managers for their consideration before being raised with the SIRO with a recommendation to notify the ICO.

In the period 1 April 2018 to 31 March 2019, there were a total of **246** information security incidents reported through the online reporting form.

The graph below gives an indication of the type of incidents received. It's clear from this that both post and emails sent externally continue to be the biggest information security risks for the Council. One of the continuing issues is around the use of the 'auto-complete' function in emails, which many staff rely on, and which they don't realise picks up addresses from any email accounts the staff member regularly uses.

Incidents by type April 2018 - March 2019

Type	Count
Blank	11
Theft of information or equipment	3
Post sent external to the Council	68
Other	81
Insecure electronic transfer of data	4
Information or equipment left in the public domain	7
Email sent internally within the Council	12
Email sent external to the Council	53
Cannot locate information or equipment	7
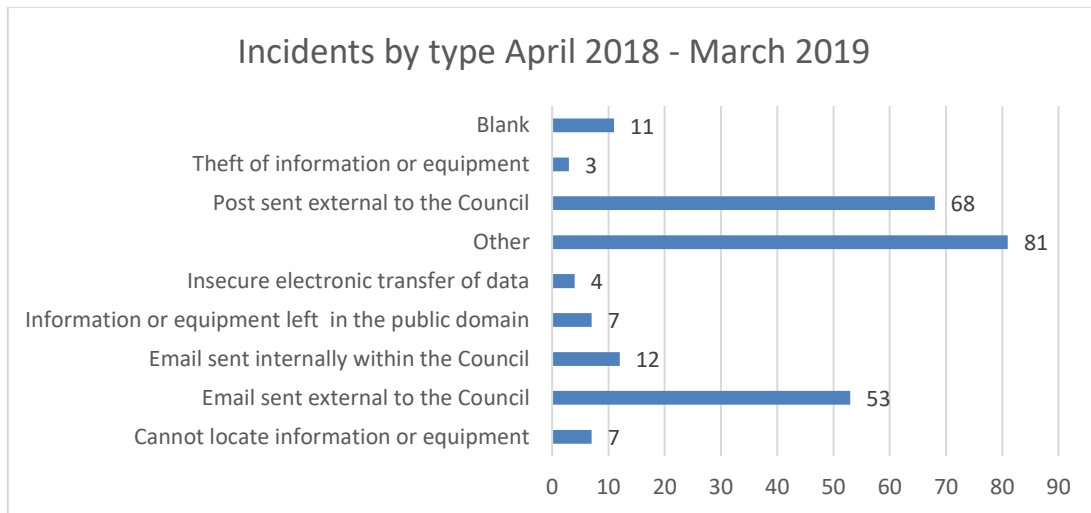
A rough visual analysis of the incidents categorised as 'other' shows that some of the incidents classed this way (around 20) actually do refer to incidents of post or emails going to the wrong recipient. Around another half dozen of the incidents classed as 'other' refer to documents sent to the wrong school or solicitor via AnyComms. However, over half of the reported incidents classed as 'other' refer to planning objectors' details being filtered to the public website without appropriate redaction. Planning have now put in place spot checks to identify these incidents earlier, but it does continue to be an issue.

The table below shows incidents split by service area.

Incidents by service April 2018 - March 2019

Service	Count
Economy & Infrastructure	81
Cllrs	3
Corporate	40
Children & Families	35
Chief Execs Office	18
Adults and Health	69
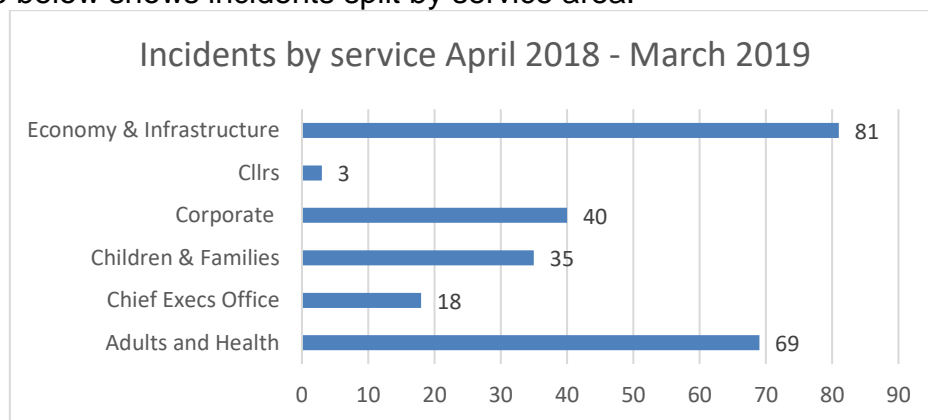
The high number for Economy & Infrastructure in part reflects the planning issue referred to above. It's worth noting that the higher numbers for Economy & Infrastructure and the lower ones for Children & Families do not necessarily accurately reflect rates of actual incidents in these two service areas. Instead, this seems to be reflective of different levels of awareness of information security, and / or a relative level of comfort with reporting versus reluctance to report. However, this conclusion is reached mainly through anecdotal evidence, and is therefore not really possible to quantify.

Whilst the number of incidents has increased by over 2.6 times in 2018/19, the number of breaches which were notifiable to the ICO was only **2**. In each case, the ICO was satisfied with the action taken by and planned to be taken by the Council to

mitigate against any impact on the individual(s) and to improve processes followed by officers to remove risks in the future. The ICO was also comfortable with the Council's approach to staff training and communication and although they provided recommendations for future improvement, no further enforcement action was required by the ICO.

Open Data

The Local Government Transparency Code 2014 was initially published in May 2014 replacing the Code of Recommended Practice for Local Authorities on Data Transparency, first published in September 2011. The Code sets out the minimum data that local authorities must publish and data that the Government recommends local authorities to publish.

The regulations came into force in October 2014. At the same time the Department for Communities and Local Government [DCLG] published a revised version of the Code including some notable changes as well as a further recommendation that local authorities go further than its requirements and provide additional datasets with more detail. The Transparency Code has not been updated since 2015. During 2016, DCLG carried out a consultation on proposed changes to the Code. Since the consultation, there has been no updates made to the Code.

The code has two elements; information which must be published and information that is recommended for publication*.* In 2016, Kirklees Council published data and information, where available, to meet the mandatory requirements of the code. We also started to obtain data & information that would meet the recommended elements at this point.

Since 2017, this local emphasis on requesting data that meets the recommended element of the code has continued and some compliance improvements have been made. The continued focus on the recommended requirements is in preparation for a future anticipated request for all authorities to meet the recommended criteria.

The full detail of the situation up to the end of 2018/2019 can be found in Appendix F.

Collection for 2019/2020 data will begin in February 2020. The published data can be found here:
http://www.kirklees.gov.uk/beta/information-and-data/open-data-sets.aspx

Record Management and the Central Archive

There has been a significant focus on bringing the Councils paper records into one storage facility, rather than paying external organisations to store and release those documents when we need them.

The Central Archive facility at Red Doles Lane currently holds 14,565 boxes of Council records with around 1,600 Childrens records still to return from external storage. The archive processes around 20 boxes per week, receiving recall requests, identifying the boxes within the archive, sending these out to services and logging them back into the archive on return.

Much work has been done with Services to ensure they are responsible for their own records and their record retention. The Council now has 21 retention schedules for services, held on the Council's intranet for all officers to refer to as they need to. In 2018/19 over 780 boxes of records were destroyed in line with these retention schedules.

Asset Mapping and the Information Asset Register

The Information Management Strategy and GDPR have highlighted a number of key areas which require further development relating to the Council's awareness of the information it holds.

Before the Council can achieve its objective of having a strategic overview of information, it needs to identify all the information it holds. This knowledge is also a requirement of GDPR. To help achieve this outcome, the IG Team worked with IT colleagues to create an online Information Asset Register. This tool collects information about the data being created and stored so that the Council has a holistic understanding of the knowledge being generated throughout the organisation.

The Information Asset Register (IAR) is closely linked with the GDPR requirement to create a Data Protection Impact Assessment (DPIA) for each activity requiring the collection of personal data. A DPIA enables all of the legislative and risk based information about a project/area of work to be outlined in one assessment

In the council's online system, if the service identifies they are collecting personal data they are taken to the DPIA platform where they complete this form, then pass through to the IAR. The IAR takes data from the DPIA so the officer only needs to complete the empty fields. If the asset does not contain personal data, the IAR can be completed without a DPIA.

This system was only launched in January 2019 but within the final quarter of the year, 75 IAR and 129 DPIA's were submitted and approved.

Information Protection

This project builds upon the records management plan highlighted throughout 2017/18 financial year that concentrates on the protection of electronic information. This project runs alongside the council's rollout of Office 365 technology to all officers and Councillors.

As part of this project, the team are developing the ways the Council can ensure retention timescales are embedded on all electronic documents, restrictions to share sensitive data are automatically enabled and users are given the ability to ensure their documents are only used for the purposes the creator intended. There will be many other benefits of this project including the potential for collaborative workspaces with external organisations and a reduction in the potential for information security incidents relating to email use.

The project will span a number of financial years but will include work ensuring:
- Emails and documents are given an appropriate label relating to the security they need
- Protective Marking of documents – ensuring documents that contain personal information are always securely processed
- Embedded retention schedules apply to all electronic documents
- The opportunity to utilise collaborative work spaces with other organisations for improved working arrangements

During 2018/19 phase 1 of this project was tested by a specialist group in preparation for roll-out to all users on the Council network. In this phase, the Council would be introducing protective marking for all electronic documents created by the council. This phase was scheduled to go live in May 2019 and phase 2 testing to begin work in September 2019.

Cyber Security

This is a field which in 2017/18 caused some concern within the NHS with the Wannacry hack. Subsequently, the IG Board has been monitoring the national situation and has supported the IT Service Cyber Security Strategy to achieve ET approval in March 2019. This Strategy will be regularly monitored by the IG Board throughout 2019/20.

Training and Awareness

Having a strong culture of Information Governance is vital to the success of many Council activities going forward and IG training has been mandatory for all Kirklees Council employees, volunteers, contractors or other individuals who may have access to council data for a number of years.

The mandatory training has been developed in a number of formats (online and paper based) to ensure that every individual working within the Council can access IG training.

The introduction of GDPR required all officers to complete the mandatory GDPR training as well as all contractors who would be accessing the Council's network. Officers who hadn't completed the training by the deadline were locked out of the system until they had completed the training.

This means the Council has a 100% record of training for GDPR awareness.

Work Programme for 2019/20

In addition to the usual compliance activities and support for Services, the following projects and work programmes are planned for the coming financial year:

Improvements to Freedom of Information (FoI) and Transparency – improving the approach to open data, transparency and FoI responses. This work will be picked up through 2018/19 and progressed in line with other projects within the Council to achieve a consistent approach to these topics.
Information Protection – Phase 1 roll-out and phase 2 testing to encourage collaborative working across the council and with our partners and to embed retention requirements within all digital-born documents
Records Management Digitisation Transformation – Identifying a road-map for digitisation of all paper records to improve the accessibility and availability of information whilst also improving the redaction accuracy and turn-around speed of information requests
Implementation of Cyber Security Strategy – developing and continually testing the IT network in line with the strategy to ensure that the objectives outlined in the strategy are fully delivered

Conclusion

The 2018/19 financial year has been the busiest and most legislatively significant for 15 years.

As an organisation, the Council has progressed from a preparatory phase for GDPR into an implementation phase, with much change being instigated resulting in the establishment of the foundations of a data protection culture across all services.

The GDPR work carried out by all services has been measured throughout the year through the GDPR Self-Assessment process. In September 2018 the trend was towards planning and developing processes and procedures. By March 2019, this had shifted more towards implementing these processes and procedures.

The Information Management Strategy and Cyber Security Strategy were both approved by Executive Team. These create solid foundations upon which to build more robust programmes of work to improve information management and security in the coming years.

The new processes established by the IG Team as well as the tools, such as the Data Protection Impact Assessment, Information Asset Register and Record of Processing Activity, have made the resource intensive processes of GDPR less demanding and have meant the outcome is more effective and understandable.

The work to ensure GDPR compliance will continue through 2019/20 alongside the Digitisation of the Archive, Information Protection phase 1 roll-out and implementation of the Information Management and Cyber Security Strategies.

The IG Board would like to thank the IG Team, GDPR Service representatives, FOI coordinators and SAR coordinators for their hard work throughout this very demanding year. Their work has resulted in some very good outcomes.

Recommendations
The Information Governance Board would be grateful for any comments from Members on the content of this report and ideas of what items Members would find useful to have included in future Information Governance Annual Reports.

It has been noted previously that this annual report is becoming larger each year. The Committee are asked if a half yearly update would be useful.

Appendices

Appendix A - Information Governance Board Terms of Reference

Information Governance Board

Terms of Reference
(Updated August 2018)

Purpose

The Information Governance Board provides a framework and strategic steer to the organisation in relation to Information Governance. The Board ensures that the Council safely uses its information assets to deliver its priorities and objectives legally, securely, effectively and efficiently.

The Board will:

- Develop and promote robust and consistent Information Governance practices across the Council;

- Embed the Kirklees Information Governance Framework throughout the organisation;

- Support and Advise the Council, Contractors and Partners on IG related matters

- Address Information Security risks and establish a risk management framework;

- Establish, monitor and oversee legal compliance with regards to Information Governance;

- Promote and support a transparent information culture;

- Develop and implement Council-wide communications around Information Governance and associated training.

- Support, advise and challenge Services on the implementation of and compliance with associated/relevant legislation and Council policy;

- Ensure the organisation complies with statutory requirements set out by the Information Commissioners Office (ICO).

- Research and advise on relevant new legislation in relation to FOI, EIR, Data Protection, Open Data, Information Security and Records Management;

- Identify and provide organisational development arising from new/amended policies/procedures and assist services in response to changing legislation;

- Support Services to share information with partners effectively and securely and to process information in a legal and safe manner.

- Develop and promote a transparent information culture across the Council, with an aim to having 90% of the Council's non-personal information in the public domain;

- Develop and implement Council wide communications around Information Governance and associated training.

Governance

The **Senior Information and Risk Owner** will chair the Information Governance Board. The SIRO has organisational responsibility for all aspects of Information Governance, including the responsibility for ensuring that Kirklees Council has appropriate systems and policies in place to maintain the security and integrity of Kirklees Council's information. The SIRO will consult with the Board to obtain guidance in relation to Information Governance decisions.

The **Caldicott Guardian** will be a member of the Board acting as the 'conscience' of an organisation. The Guardian actively supports work to enable information sharing where it is appropriate to share, and advises on options for lawful and ethical processing of information. The Caldicott Guardian also has a strategic role, which involves representing and championing confidentiality and information sharing requirements.

The Data Protection Officer (DPO)

The DPO's tasks are defined in GDPR Article 39 as:
- to inform and advise the Council and it's employees about their obligations to comply with the GDPR and other data protection laws;

- to monitor compliance with the GDPR and other data protection laws, and with the Council's data protection polices, including managing internal data protection activities; raising awareness of data protection issues, training staff and conducting internal audits;

- to advise on, and to monitor, data protection impact assessments;

- to cooperate with the supervisory authority; and

- to be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc).

Information Governance Manager (IGM)

The IGM is responsible for providing specialist advice and support on all aspects of Information Governance and is also responsible for reviewing the policy and ensuring it is updated in line with any changes to national guidance or local policy.

Terms of Engagement
- Frequency of meetings – every two months

- Attendance at meetings to be substituted by representatives as required, ensuring all Directorates are represented.

- The Board will provide updates to the Executive Team, Management Board, Corporate Governance and Audit Committee, the Cabinet Member responsible for Information Governance and Cabinet as appropriate.

- The Board will be Chaired by Julie Muscroft, Senior Information Risk Owner and Service Director for Legal, Governance and Commissioning

- The Information Governance Manager will co-ordinate the Board meetings, generate the agenda on consultation with the Chair and distribute papers

- Representatives from all work areas will sit on the board, with non-members being invited to present papers as appropriate

- Communications Strategy – the Communications Plan is updated on a monthly basis in line with developments across the organisation

Review

The Board will review the relevance and value of its work on an annual basis.

Working methods

The Board will have a strategic overview of the Information Governance framework across the organisation. This includes

- Legislative requirements – including FOI, EIR, Data Protection and Transparency

- Information Security

- Incident Reporting

- Records Management

- Information Sharing and Processing

- Organisational Culture, Training and Development

- Open and Transparent Publication

IG Sub-Groups

The Board will oversee a range of sub groups, each with an individual mandate for operation and performance. In 2018/19 these will include:

- GDPR Implementation task group – focussing on the implementation of GDPR practices across all Services and supporting the assurance assessment for the Board

- Records and Transparency Team – Focussing on updating policies and guidance, overseeing and supporting the Information Governance &

Management Strategy and supporting the implementation of the Mobile & Agile work programme.

- Information security team - Focusing on updating policy, approving information sharing agreements, creating a council-wide incident reporting matrix and developing an organisational approach to information security incidents.

-

Board membership

The Board is made up of Council Officers, with all Directorates represented. The 2018/19 membership is outlined in Appendix A

Appendix A
Information Governance Board Membership 2017/18

Chair	Julie Muscroft (SIRO) – Assistant Director, Legal, Governance and Monitoring
Commissioning & Health Partnerships	Saf Bhuta (Caldicott Guardian) – Directorate Lead for Performance, Intelligence and Business Systems
Democracy Service	Carl Whistlecraft – Head of Governance & Democratic Services
	Katy Deacon - Information Governance & Senior Support Manager
	Lindsay Foody – Information Access & Security Officer
IT	Terence Hudson – Head of IT
Audit	Simon Straker – Audit Manager
Customer & Exchequer Services	Steve Bird – Head of Welfare & Exchequer Services
	Julian Hobson – Policy Officer
HR	Maureen Manson – HR Officer
Learning & Organisational Development	Alison Monkhouse – Principal Strategic Liaison Officer
Communications	Niel Stewart – Communications & Marketing Team Manager
Safe & Cohesive Communities	Lee Hamilton – Safer Kirklees Manager Sarah Mitchell – Strategic migration and Refugee Manager
Public Health -	Sean Westerby – Emergency Planning & Business Continuity Manager
Investment & Regeneration	Adrian Wisniewski – Relationship & Performance Manager
	Jane Lockwood – Head of Procurement & Commissioning Support

Appendix B - Kirklees Information Management Strategy

Document Overview			
Kirklees Council considers information to be a vital asset for the successful delivery of services and efficient management of resources. It is important to ensure that information is efficiently managed and that appropriate policies, procedures and management accountability provide a robust governance framework for this information management.			
Intended Audience		All employees and Councillors	
Linked Policy		Information Governance Policy Records Management Policy Data Protection Policy Information Sharing and Processing Policy Information Security Policy	
Revision History			
Version	Author	Reason for issue	Date
1.0	Katy Deacon	New Strategy	February 2019
Date of next revision		April 2021	

Introduction

The purpose of this strategy is to outline the principles, vision and objectives Kirklees Council has for information management until April 2021. It sets out the approach to be taken to provide a robust framework around the use of information.

Accurate, timely and relevant access to information is vital to deliver the highest quality services. It is the responsibility of all staff to ensure information is used appropriately and in accordance with the supporting policies.

In this strategy, the term 'information' covers the breadth of structured and unstructured information such as records, data and documents. It also relates to any format, including electronic, hard copy or handwritten.

Kirklees wants to make better use of the information it has and to ensure teams have access to high quality information to deliver effective services. These provide the foundation for the Council objectives:

- **A Council which connects ideas, people and resources across boundaries of all kinds, supporting communities to harness and build on their strengths**
- **A Council focussed on creating trust and connections between institutions, businesses and citizens in Kirklees**
- **A Council which will be responsible for a consistent level of basic services, but will strive to maximise the impact of all services by collaborating with others; and**
- **A Council which safeguards vulnerable citizens, but wherever possible, seeks to develop a springboard, not simply a safety net, focussed on helping people to control their own lives and to stay safe and well.**

All employees have a role to play in helping the Council to manage information effectively. The quality and outcomes of strategic decisions the Council makes depend on the data we collect as part of our day to day jobs.
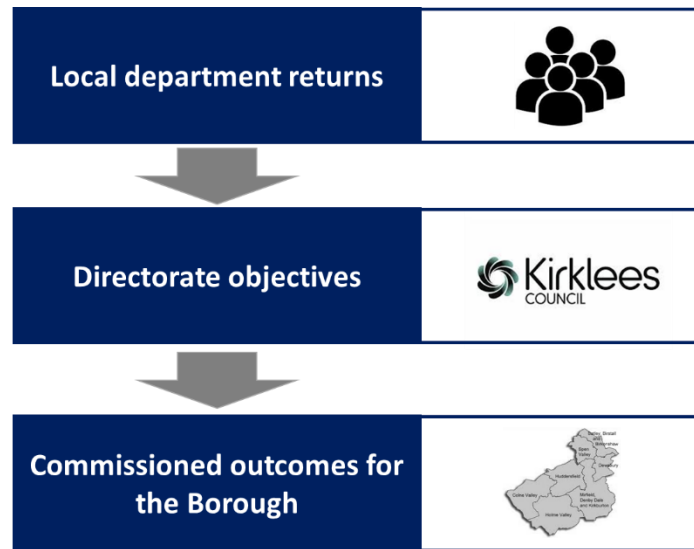
Figure 1 the value of information

Strategy objectives

During development of this strategy, we spoke with many staff across the organisation. Throughout these conversations, key themes consistently emerged. These themes have become the overarching objectives of the strategy. These are:

- To ensure we are embedding the requirements of the General Data Protection Regulation (GDPR)
- Using information to create a resource for decision making
- To unlock the value of data, where it sits and how it travels, allowing the Council to have a strategic overview of its information
- Support culture change – to improve awareness of the importance of information management and embed excellent IM practices throughout the organisation
- To improve citizen experience through 'tell us once'
- Train staff understand the value of information – in order to maximise access to high quality information in order for all staff to be able to unlock the value within
- Encourage collaborative working – by breaking down communication and technological barriers that prevent information from being shared appropriately
- Implement a more proactive information management function – focussing on communications, training and prevention rather than remediation
- Embed a collaborative culture - where knowledge is actively shared without compromising confidentiality
- Services work closely with IG and IT - to ensure appropriate infrastructure is available to support excellent information management

Information management principles

The following principles have been agreed:

- Better informed citizens and businesses
- Information is a valued asset
- Information is managed
- Information is fit for purpose
- Information is standardised and linkable

- Information is reused
- Information is published
- Information is stored once, so there is a single version of the truth wherever possible
- Knowledge is captured and used
- Information will be owned and proactively managed
- Information will be shared with partners', subject to relevant IG controls

Benefits

Whilst not necessarily immediately obvious, good information management provides many benefits to us all. These include:

For citizens

- Citizens are better informed
- Information is captured once and not repeated
- Better informed staff that are able to deal with queries and transactions quickly and accurately
- Confidence that the Council is using their personal information appropriately
- Better use of funding to ensure that Council money is used in the most appropriate way

For staff

- Access to high quality information needed to perform your job
- Confidence in knowing what to share and when it is appropriate to share
- Easier to search and use information, reducing wasted time trying to find or validate information
- Better awareness of your responsibilities resulting in a reduced risk of breaching policy or legislation
- Reducing the number of information access requests received by publishing more information as standard

Corporate Organisation - including members

- The Organisation and Members are better informed
- Members respond effectively to caseload enquiries
- Officers are confident their recommendations are based on true data and have strong evidential foundations
- Members are confident their decisions are effective and appropriate

For the business

- Enable the Council to assist with shared outcomes with Partners
- Reduce the risk of an information breach and resulting fine from the Information Commissioner
- Increase the efficiency of Council resources
- Access to accurate information in order to support policy and decision making
- Ability and preserved reputation of providing the highest quality service to its citizens
- Improved organisational knowledge of the information collected by teams

Challenges

Council funding pressures are well documented, and it has become a constant challenge to find more efficient and modernised ways of working in order to continue providing services with limited funding.

Becoming an intelligence led organisation is a significant shift from the way the Council currently operates, which we recognise will not happen overnight. Our organisational culture must adapt to a new more self-sufficient way of working. We recognise asking staff to work in a more digital way can be daunting and are committed to supporting staff through this change.

Across the business, the following challenges that may affect the ability of this strategy to be implemented have been identified, along with our proposed mitigation actions:

Challenge	Mitigating activities
Organisation going through significant change	New projects implemented with 'privacy by design and default' so that information risks are identified early in the process
Proliferation of information across many areas	An information asset register to be completed by all teams. This documents all information assets held by the Council and provides a firm basis for managing information moving forward. Agile working and collaboration technology to be implemented through the advanced adoption of Office 365, reducing the need for duplicate information stores
Staff being asked to do more with less (become more self-sufficient)	Training and support provided by the IG and IT teams
Current levels of IT competence & confidence with staff – being asked to work more digitally	Training and regular, bite size communications to support staff with new ways of working
Lack of control with records management	Centralised paper records storage and a new electronic document management system. Full information asset register to be completed to document all information assets held by the Council. This provides a firm basis for managing records moving forward.
Risk reporting and management	Information risks to be managed through the IG Board.
How to manage and recognise subject access requests	Training and communications for all staff.
Operational management and ownership of IG issues	Team managers asked to enhance understating and management of IG risks, with support from the IG team.

High level action plan

This section details the activities that will be undertaken to support implementation of this strategy. A summary of activity is shown in the diagram below.

Situation now	Activities	Future target
▪ IT decisions not focused on improving business needs ▪ The value of information is not always a high priority ▪ Current culture: information management is not important ▪ Isolated working procedures ▪ Overprotection with data ▪ Information Governance efforts are reactive, instead of proactive ▪ Lack of communication between services ▪ Organisational knowledge is lost during staff turnover ▪ Kirklees needs to prepare for the introduction of new data legislation (GDPR)	Development of the information asset register Information management strategy EDRMS Website and transparency review Consolidation of paper records in a central on-site repository Survey to identify perception of information governance Mobile and agile working	▪ Clear strategy for information management ▪ Clarity about ownership and responsibility for data ▪ Clear understanding of risks and opportunities ▪ Quality information to make the best decisions ▪ Less wasted resources looking for information ▪ A culture of openness and accountability ▪ Fewer FOI / EIR requests ▪ Increased usage of data assets ▪ Reduction in off-site storage costs ▪ GDPR compliance and reduced risk of DPA breach

Figure 2 Future target model

Specific objectives

The following specific tasks are set to be achieved before 2021:

- Develop and maintain the information asset register
- Provide a simple and secure method for sharing confidential information
- Develop a programme of training and support for change
- Develop the intelligence hub – which will focus on data driven decision making for the Council
- Complete a meta data project that will improve the use of meta data and make information easier to use, retrieve and manage
- Build information management as standard into projects, processes and systems
- System rationalisation must be considered when purchasing new data driven systems
- Implement privacy by design and default where information governance considerations are taken into account at the start of new projects
- Proactively publish more information, in order to reduce information access demand and improve transparency for the general public

Current in-flight projects

The following projects are already underway:

- Implementation of the information asset register
- Mobile and agile working
- Digital by design
- Consolidation of paper records in a central on-site repository
- 'Spotlight' awareness raising
- Information Protection project – stage 1, labels and protective marking

Upcoming projects

The following project are planned to be mobilised soon:

- Website and transparency review
- Electronic Document Management System (EDRMS)
- Information Protection project – stages 2 and 3
- Development of the intelligence hub
- Survey to baseline current perception of staff around information governance in line with NHS Data Security and Protection Toolkit requirements

Training

We are committed to ensuring that staff have appropriate information governance training according to their role.

Training will be managed through the performance review system and linked with the People strategy.

Information Management training for all staff will be a development aim for 2019/20.

Standard offering for all staff

Standard data protection and information security training must be completed by all staff. The Council has invested in the Metacompliance 'Spotlight' solution that will deliver training in a more regular, bite size way that will support ongoing reminders and understanding of staff responsibilities.

Additional training for specialist staff

A training needs analysis will be undertaken to identify the training needs of employees that would benefit from advanced information management training, for example specialised courses for Information Asset Owners, General Data Protection regulations, or any of the topics in the table below.

Team managers are expected to liaise with the information governance team to plan relevant specialist training.

Confidentiality	Data Protection Act 2018	Freedom of Information
Records & document management	Information Security	Caldicott Principles
Appropriate information sharing	Incidents and data breaches	Information Risk Management

Figure 3 Example IM training courses

An example training needs analysis is included at Annex 1 for information.

Documents and records management

The supporting records management policy details specific requirements for document and records management.

However there are three key areas of document management that are identified for improvement as part of this strategy. These are:

Email

More and more valuable discussion and resulting decisions are taken by email. There is a risk that this information remains in personal email folders, where wider colleagues or departments have no knowledge that the information exists. Council records must be saved in a corporate file structure, able to be accessed by appropriate staff.

In order to encourage timelier document management, the IG Board will be implementing email policies and releasing guidelines to incorporate the new Office 365 tools when these are rolled-out to the Council.

Document retention

The Council will proactively monitor when records (electronic - including information held in line of business systems, and paper) have been held for the required retention period, to ensure that information is not being kept longer than necessary. The Council will develop a Corporate Retention and Disposal Policy and maintain records of disposal. The Information Asset Owners will approve their services Retention Schedules and disposal logs with Information Asset Coordinators ensuring Services maintain their retention and disposal schedules.

The Information Protection Project will utilise the Office 365 tools to embed retention schedules within documents and enable the auto deletion function which comes with the new system. Proposals for this implementation will come to the IG Board for sign-off.

Archiving

Work is currently underway to consolidate paper records in the new central archive facility at Red Doles Lane. This is a formal, structured way of managing paper records ensuring that proper inventories are used to support retrieval, and identify records ready for disposal or permanent preservation.

The IG Board has approved the requirement for maintaining records based on the individual rather than the department those individuals accessed.

Electronic records management is being tackled by the Electronic Records Management task group, which will identify key risk areas and propose solutions for IG Board consideration.

Information access

The Council provides the public access to information via the Freedom of Information Act, the Data Protection Act (for personal data) and the Environmental Information Regulations. Data sets are available through the Council's Observatory feature and this is provided by the Intelligence department to achieve the requirements of the Local Government Transparency Code (2014).

There are a number of changes required to current processes in order to remain compliant with changing legislation and ways of working. These are:

- GDPR reduces the time for responding to a DPA request from 40 to 30 days
- The Information Commissioner expects 90% compliance of FOI requests within the 20 working day limit
- The Council wants to reduce the demand (number of requests) by publishing more information proactively, allowing staff time to be repurposed
- The Council wants to ensure exemptions are applied fairly and appropriately, for example with regard to vexatious FOI requests. This may require collaboration across departments.
- The Local Government Transparency Code (2014) requires services to release data in a more accessible format

Publishing

We will publish a transparency and publication strategy by the end of 2018/19. This will cover how we proactively publish more information to (1) the public, via the website and (2) internally for use by the intelligence team.

We will analyse freedom of information requests received by the Council, to understand common or regularly requested information and use this identify information that could be published more proactively.

The transparency strategy will also provide a framework to ensure that the intelligence team is aware of all data assets within the Council using the information asset register entries, and can use these easily to support its work. The Council is committed to ensuring the intelligence team has access to timely, accurate and consistent information.

Business continuity

The IG Board is responsible for the ongoing management of business continuity for data, ensuring risks are discussed and appropriate plans are prepared, should any adverse events take place.

Information security

Cyber-attacks are a significant organisational risk. Attacks are becoming more sophisticated and frequent. The Council's Cyber Security Strategy has received sign-off at IG Board and Executive Team. This strategy will be implemented over 2019/20 to ensure the Council is as protected as possible against future attacks.

There are a number of technical measures that IT implement in order to prevent information security breaches, however preventing breaches requires all staff to be vigilant. Spam email or 'phishing' attacks are on the rise, and can trick staff into releasing information and causing a breach. We will implement regular communications and training throughout the course of this strategy, to remind and keep staff up-to-date with best practice recommendations.

Evidential weight

Disciplined information management will ensure the Council can evidence proper processes and show that information has not been mishandled, should it be admissible to a court.

Partnership working

Kirklees partners with a number of formal and voluntary organisations in order to provide services to local residents. We recognise the importance of transparent data sharing between partners, and as such commit to the following:

- All partners are expected to sign an Information Sharing Agreement with the Council
- Information is regularly published and made available which allows partners to plan services
- We will share information appropriately, and only when supported by an information sharing agreement
- We will publish transparent privacy notices to the public for all activities where personal data is collected or used

Measures of success

The IG Board will monitor the implementation of this strategy. It will use the following measures to track success:

- GDPR Self-Assessment reporting
- Information security reporting figures
- Information access requests compliance figures
- Data Security and Protection Toolkit assurance rating
- Ongoing involvement of IG Team resources within Services

A successful strategy creates a Council which by April 1st 2021 is:

- Meeting the ICO's minimally acceptable compliance rates for GDPR, FOI and EIR
- Effectively managing all records, both paper and electronic
- Proactively sharing appropriate data with partners, with effective sharing agreements in place and reviewed annually
- Managing information security incidents and mitigating risk through thorough training and procedural improvement practices
- Privacy by Design and Default is embedded within working practices
- Publishing information to the public, improving transparency and reducing information access demand

The success of this strategy will be monitored at IG Board meetings and reported in the Annual IG Report, which is approved by IG Board annually and presented to Elected Members for challenge at Corporate Governance and Audit Committee.

Appendix 1 – Example training needs analysis

Topic	Mandatory	Upper tier example content	Job roles
Confidentiality	Any particular confidentiality issues / wider threats Examples of consent forms / where to find them	Access to national data sets	Caldicott Guardian IG / records manager Frontline staff Team leader / Manager
Data protection (DPA)	Overview of the number of requests in the last year / month	How to deal with complex subject access requests	IG / records manager Team leader / manager FOI / SAR officers
Freedom of Information (FOI)	Specific 'where to go' advice. Overview of the number of requests in the last month / year	Complex FOI requests	IG / records manager Team leader / manager FOI / SAR officers
Records and document management	Show pictures of your file structure / off site archive procedure. Contact details of your records manager / where to go for advice. Point to any guidance available on the intranet.	File structures Scanning technology	IG / records manager Team leader / manager Frontline staff
Information security	Specific password requirements, screenshots of the different systems. Different access controls for different systems? Physical security. Business continuity overview	o	IG / records manager Team leader / manager IAO / IAA Frontline staff
Caldicott principles	Introduction to the principles The role of the Caldicott Guardian		Caldicott Guardian IG / records manager Team leader / manager
Appropriate information sharing	What agencies do we share with at the moment	o National projects o Working with partners	Caldicott Guardian IG / records manager Frontline staff Team leader / manager
Systems overview	Any particularly important IG factors relating to the systems that staff member will use	o System audits	IG / records manager Team leader / manager IAO / IAA SIRO

Topic	Mandatory	Upper tier example content	Job roles
Incidents and data protection breaches	How to identify and report an incident	o Incident management o Route cause analysis o When to report to HSCIC o When to report to ICO o HSCIC incident reporting tool	Caldicott Guardian IG / records manager Front line staff Team leader / manager IAO / IAA SIRO
Secondary uses of information	What is considered a secondary use	o Consent and fair processing o Anonymisation and pseudonymisation	Public health Caldicott Guardian SIRO

Appendix C - GDPR Self-Assessment

Background
In the 11 months of 2018/19 following the May 2018 GDPR implementation, the Council has received an increase in Subject Access Requests of 37%, Freedom of Information/ Environmental Information Regulation requests of 10% and Information Security Incidents of 38% with two incidents reported to the Information Commissioner. This is reflective of the situation with other West Yorkshire Authorities.

Services have been working towards establishing GDPR requirements as part of their business as usual activities. The IG team have supported all services with this work, the GDPR Implementation task group has met monthly and there has been very positive interaction across the Council.

Self-Assessment Results Summary
The IG Team ran a Self-Assessment for Council Services to measure their work towards compliance against the 10 GDPR deliverables. These Self-Assessments had a 100% response rate and the results were reported to Executive Team and all of the Information Asset Owners.

The first GDPR Self-Assessment was conducted through October 2018, against 9 of the deliverables. GDPR had only been in place for around 5 months and therefore Services were expected to be performing at a 'Planning' or 'Developing' level. There was a selection of responses from 'Not started' through to 'Established way of working' however most of the responses were within the 'Planning' or 'Developing' levels.

The second GDPR Self-Assessment was conducted throughout March 2019, against all 10 GDPR deliverables. As GDPR had been in place for almost 12 months, Services were expected to be performing at an Implementing or Established way of working level. Whilst there was still a mixture of response levels from Services, the levels were more focussed on the Implementing and Established way of working areas.

The graphs of the results for both Self-Assessments against each deliverable are shown below.

The Information Asset Owners (Service Directors) received the detailed spreadsheet with each Service's scores and comments. The IG team are working with the Information Asset Coordinators and Services, to support their process development and progress compliance into the Established way of working level.

These scores have been presented to the IG Board for comment and further action.

September 2018	March 2019
1. Governance Not started (1) 2% Planning (12) 23% Developing (24) 45% Implementing (15) 28% Established way of working (1) 2%	**1. Governance** Not started (1) 3% Planning (1) 3% Developing (9) 29% Implementing (17) 55% Established way of working (3) 10%
2. Assurance Not started (-) Planning (9) 17% Developing (26) 49% Implementing (15) 28% Established way of working (3) 6%	**2. Assurance** Not started (-) Planning (1) 3% Developing (9) 29% Implementing (17) 55% Established way of working (4) 13%
3. Third party management Not started (4) 8% Planning (15) 30% Developing (19) 38% Implementing (10) 20% Established way of working (2) 4%	**3. Third party management** Not started (1) 3% Planning (1) 3% Developing (11) 37% Implementing (12) 40% Established way of working (5) 17%

4. Data collection and use

- Not started (1): 2%
- Planning (13): 26%
- Developing (25): 50%
- Implementing (9): 18%
- Established way of working (2): 4%

4. Data collection and use

- Not started (1): 3%
- Planning (3): 10%
- Developing (10): 32%
- Implementing (13): 42%
- Established way of working (4): 13%

5. Retention and disposal

- Not started (1): 2%
- Planning (16): 31%
- Developing (23): 45%
- Implementing (11): 22%
- Established way of working (-)

5. Retention and disposal

- Not started (-)
- Planning (2): 6%
- Developing (12): 39%
- Implementing (15): 48%
- Established way of working (2): 6%

6. Individuals' rights

- Not started (3): 6%
- Planning (19): 37%
- Developing (12): 23%
- Implementing (18): 35%
- Established way of working (-)

6. Individuals' rights

- Not started (1): 3%
- Planning (2): 6%
- Developing (3): 10%
- Implementing (15): 48%
- Established way of working (10): 32%

7. Information security

- Not started (4): 8%
- Planning (19): 37%
- Developing (23): 44%
- Implementing (6): 12%
- Established way of working (-)

7. Information security

- Not started (-)
- Planning (2): 6%
- Developing (19): 61%
- Implementing (7): 23%
- Established way of working (3): 10%

8. Systems and technology

Not started (1)	2%
Planning (6)	12%
Developing (30)	58%
Implementing (14)	27%
Established way of working (1)	2%

8. Systems and technology

Not started (-)	
Planning (-)	
Developing (16)	52%
Implementing (11)	35%
Established way of working (4)	13%

9. Training and awareness

Not started (-)	
Planning (27)	51%
Developing (9)	17%
Implementing (13)	25%
Established way of working (4)	8%

9. Training and awareness

Not started (-)	
Planning (1)	3%
Developing (1)	3%
Implementing (21)	68%
Established way of working (8)	26%

This deliverable was not measured in September 2018

10. Staff data

Not started (1)	3%
Planning (5)	17%
Developing (12)	40%
Implementing (9)	30%
Established way of working (3)	10%

Appendix D – DPA Annual Report

Data Subject Access Requests:
Data Protection Act 1998
General Data Protection Regulation
Data Protection Act 2018

Annual Report 2018-19

Executive Summary

This report details how the Council has performed throughout 2018-19 in respect of requests for access to personal information received and processed in line with the data protection legislation, ie:

- the Data Protection Act 1998 (DPA98) which was repealed on 24 May 2018
- the General Data Protection Regulation (GDPR) which was enacted on 25 May 2018
- the Data Protection Act 2018 (DPA18) which received Royal Assent on 23 May 2018

During 2018-19, Kirklees Council received 79 more requests (a 35.4% increase) for access to personal information than it did in the previous 12 months, increasing from 223 in 2017-18 to 302 in 2018-19.

The Council's performance in terms of compliance with the legislative timescales has decreased from the previous year, from 83% to 73%. The number of requests responded to within the statutory timescale (40 calendar days under the DPA98 and one month under the GDPR) is well below the ICO's minimum expectation of 90% compliance. At the time of writing, 17 subject access requests received during 2018-19 remain unanswered and are well past the one month deadline for responding. The GDPR allows for the deadline to be extended by an additional 2 months in certain circumstances. All of the outstanding requests are now unfortunately past this extended timescale.

The Council's performance in terms of the time taken to respond to requests has also decreased when looking at the average response time for dealing with requests; it was 28 calendar days in 2017-18 and, taking into account the overdue requests, is already at 36 calendar days.

The Council did introduce the GDPR timescale of one month some 6 months before GDPR came into force, and initial findings from this were encouraging. However, the large increase in the number of requests received since GDPR was enacted has had a significant negative impact.

The Council needs to make significant improvements to ensure that information and records are managed efficiently and effectively and resources are available to ensure compliance with the legislative timescales. It also needs to make sure that it advises applicants as soon as it is known that there may be a delay and keep them informed of progress.

Regionally, from the West Yorkshire Councils which have submitted annual figures, there has been an increase in the number of requests, two other Councils having had between 29.% and 45% more than in the previous year.

Guidance on dealing with requests for access to personal information continues to be reviewed and shared with officers dealing with requests.

Lindsay Foody
Information Access & Security Officer   22 July 2018

Contents:

1. **Introduction**

2. **Summary of the Legislation**

3. **Kirklees Context**

4. **Statistics:**

    a. Numbers of Requests
    b. Time Taken to Respond to Requests
    c. Requests by Directorate
    d. Outcomes

5. **Information Commissioner**

    a. Powers
    b. Complaints Received re Kirklees

1. Introduction

This report discusses the main events of the year 2018-19 in relation to requests made under the data protection legislation, along with recommendations for improvements to the processes. The data protection legislation is:

- the Data Protection Act 1998 (DPA98) which was repealed on 24 May 2018
- the General Data Protection Regulation (GDPR) which was enacted on 25 May 2018
- the Data Protection Act 2018 (DPA18) which received Royal Assent on 23 May 2018

2. Summary of the Legislation

Article 15 of the GDPR gives individuals important rights including the right to know what information is held about them. The GDPR helps to protect the interests of individuals by obliging organisations to manage the personal information they hold in an appropriate way.

Article 5 of the GDPR sets out seven key principles which lie at the heart of the general data protection regime. Article 5(1) requires that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals *('lawfulness, fairness and transparency')*;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes *('purpose limitation')*;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed *('data minimisation')*;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay *('accuracy')*;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals *('storage limitation')*;

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures *('integrity and confidentiality')*.

3. Kirklees Context

The Council maintains five data protection fee payer register entries as data controllers:

Kirklees Metropolitan Council	Z575071X
Electoral Registration Officer For Kirklees Metropolitan Council	Z605248X
Superintendent Registrar for Kirklees Metropolitan Council	Z4939146
Kirklees Youth Offending Team	Z5437178
Returning Officer for Kirklees Metropolitan Council	ZA060314

The Information Governance Team, which manages the process of receiving and responding to requests made to the Council under information access legislation, comprises:

- One full-time Information Governance Manager
- one full-time Information Access & Security Officer,
- three full-time and one part time Information Governance Officers (one full-time post is temporary from October 2018 to May 2020)
- one full-time and three part-time Business Support Officers

The Team sits in The Democracy Service, within the Governance & Commissioning part of the Corporate directorate.

The Information Governance Team works with a network of Co-ordinators located within the different service areas across the Council, who arrange for information requested to be collated and draft responses to be signed off by nominated managers.

4. Statistics:

a) Numbers of Requests

The number of requests for access to personal information received between 1 April 2018 and 31 March 2019 has increased by 35.4% from figures reported last year, from 223 to 302, averaging at 25.1 requests per month compared to 18.5 per month in 2017-18.

Monthly	Number
April 2018	19
May 2018	19
June 2018	34
July 2018	32
August 2018	26
September 2018	18
October 2018	34
November 2018	23
December 2018	17

Quarterly	Number
Quarter 1	72
Quarter 2	76
Quarter 3	74

|				
January 2019	29			
February 2019	22	Quarter 4	80	
March 2019	29			
Total	**302**	**Total**	**302**	

The following chart plots the monthly figures from the above table:
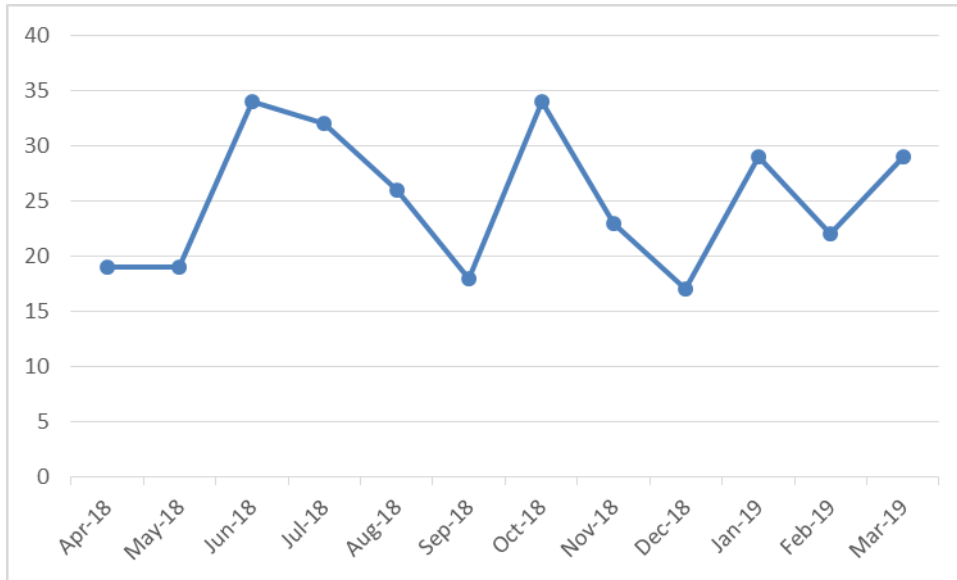
Year on year figures are:

Quarters	2011-12	2012-13	2013-14	2014-15	2015-16	2016-17	2017-18	2018-19
Qtr 1	35	29	47	56	54	57	69	72
Qtr 2	32	43	49	51	36	40	59	76
Qtr 3	45	40	45	37	40	42	35	74
Qtr 4	65	36	53	53	57	62	60	80
Totals	**177**	**148**	**194**	**197**	**187**	**201**	**223**	**302**
% Change	*+127%*	*-16%*	*+31%*	*+2%*	*-5%*	*+7.5%*	*+11%*	*+35.4%*

The following chart plots the totals received annually from the above table:
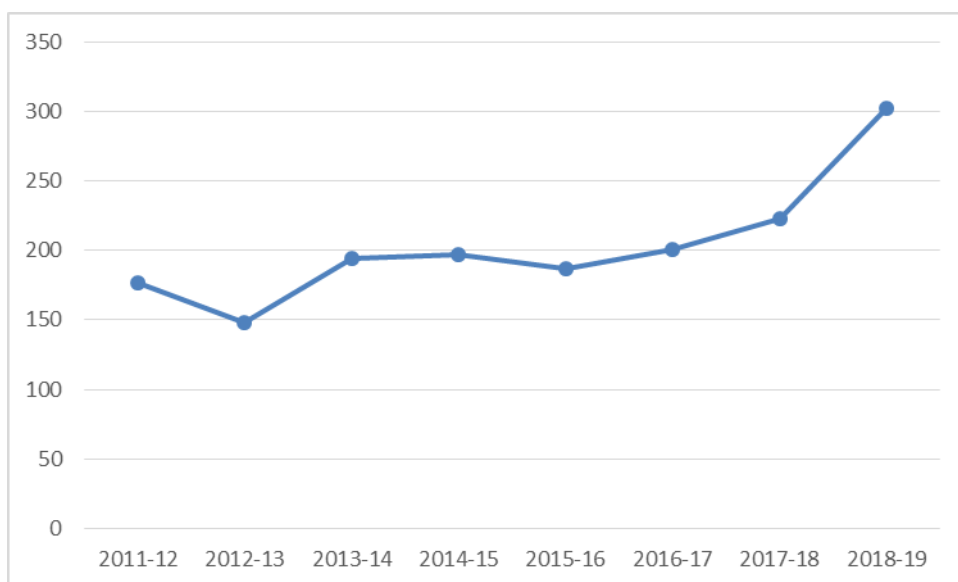
b) Time Taken to Respond to Requests

The DPA98 required data controllers to reply to requests for access to personal information promptly and within 40 calendar days of receipt. There was no provision to extend the time for compliance.

The GDPR requires data controllers to reply to requests for access to personal information without undue delay and, at the latest, within one month of receipt. The GDPR allows for an extension of the time to respond by a further two months if the request is complex or the data controller has received a number of requests from the individual.

In 2018-19 the Council dealt with 33 requests under the DPA98 and 269 requests under the GDPR.

The Council responded to 73% of requests received within the deadline; this compares with 83.5% in 2017-18, showing a decrease in compliance. There is significant scope for improvement and the Council's compliance falls short of the ICO's minimum expectation of a 90% compliance rate.

Requests Received		Legislative Deadline *		* Response Within 10 Calendar Days of Deadline	
Monthly	Number	Number	%	Number	%
April 2018	19	17	89%	18	95%
May 2018	19	18	95%	19	100%
June 2018	34	25	74%	28	82%
July 2018	32	20	63%	22	69%
August 2018	26	21	81%	22	85%
September 2018	18	14	78%	15	83%
October 2018	34	24	71%	24	71%
November 2018	23	18	78%	19	83%
December 2018	17	11	65%	13	76%

January 2019	29		18	62%	24	83%
February 2019	22		15	68%	15	68%
March 2019	29		15	52%	18	62%
Total	302		216	Av 73%	237	Av 80%

* legislative deadlines are 40 calendar days under the DPA98 and one month under the GDPR

It is noted that the Council's performance under the DPA98 in April and May 2018 is significantly better than under the GDPR, when the deadline was reduced by a quarter and the number of requests started to rise.

At the time of writing, 17 subject access requests received during 2018-19 remain unanswered. The Council is exploring options for tackling this.

The average response time in 2017-18 was 28 calendar days; this compares with 36 calendar days in 2018-19, which shows a downturn in performance on the time taken to respond to requests.

c) Requests by Directorate

The total figure in this section is 362 which is higher than the 302 total number of requests received because 16.6% of the 302 requests received (60) were for information held by two or more services.

The figures below show the total number of requests each dealt with, so for example, where a request was made for personal information and this was sent to both Adults Services and Exchequer & Welfare, the same request is counted twice in the table below.

Note: Requests which related to information held by a large number of areas of the Council are recorded just once as "Council-wide".

Directorate	2018-19	Percentage of Total Received
Chief Executive's Office	6	1.66%
Adults (social care, public health, commissioning)	51	14.09%
Children Services (social care and learning)	187	51.66%
Communities, Transformation & Change	15	4.14%
Economy & Infrastructure (Place)	37	10.22%
Resources	57	15.75%
Council–wide	8	2.21%
KNH	1	0.28%
Total	362	100.00%

d) Outcomes

Outcome	2018-19	Percentage of Total Requests Received
Supplied (in whole or in part)	167	55.30%
Refused	3	0.99%
Not Held	34	11.26%
Discontinued	81	26.82%
Outstanding / Suspended	17	5.63%
Total	**302**	**100.00%**

At the time of writing, the responses to 17 requests remain outstanding.

Where requests are refused in whole or in part, this is because one of the exemptions from disclosure applies, including personal information relating to a third party, same or similar requests, legal privilege, etc.

5. Information Commissioner

The Information Commissioner's Office (ICO) is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

a) Powers

The ICO has a number of options available for taking action to change the behaviour of organisations and individuals that collect, use and keep personal information, including criminal prosecution, non-criminal enforcement and audit. The ICO also has the power to serve a monetary penalty notice on a data controller.

The ICO's regulatory activity (and activity in support of regulatory activity) includes:

- *conducting assessments of compliance with the DPA and GDPR, PECR, e-IDAS, NIS, FOIA and EIR;*
- *issuing information notices;*
- *issuing 'urgent' information notices under the DPA, requiring individuals, controllers or processors to provide information on not less than 24 hours' notice;*
- *applying for a court order requiring compliance with the information notice issued under the DPA, if the recipient does not provide a full and timely response;*
- *issuing assessment notices under DPA;*
- *issuing 'urgent' assessment notices under the DPA, requiring controllers or processors to allow us to undertake an assessment of whether they are compliant with the data protection legislation, on not less than 7 days notice;*
- *issuing no-notice (or short notice) assessment notices under the DPA where we have reasonable grounds to suspect that the controller or processor has failed or is failing to comply with certain provisions of the data protection legislation or has committed or is*

- *committing an offence under the DPA, allowing us to undertake an assessment on less than 7 days notice;*
- *producing codes of practice about data sharing and direct marketing, and any other codes of practice that we are required to produce under the legislation we cover;*
- *conducting assessments of cross-border data transfers and corporate groups' binding corporate rules;*
- *overseeing data protection impact assessments;*
- *conducting audits and assessments under IPA and other information rights legislation;*
- *overseeing the establishment of data protection certification mechanisms;*
- *encouraging the development of codes of conduct, and accrediting bodies to monitor compliance with codes of conduct;*
- *requiring a controller or digital service provider to inform an individual of a personal data breach;*
- *issuing a warning where proposed action threatens non-compliance with data protection legislation;*
- *issuing a reprimand for infringements of relevant data protection legislation;*
- *issuing practice recommendations under FOIA and EIR and decision notices detailing the outcome of an ICO investigation into an individual's case under FOIA or EIR;*
- *issuing enforcement notices orders requiring specific actions by an individual or organisation to resolve breaches (including potential breaches) of applicable information rights obligations. An 'urgent' enforcement notice under the DPA may be used to require action to resolve breaches or potential breaches of the data protection legislation, on not less than 24 hours' notice;*
- *certifying contempt of court should an authority fail to comply with an information notice, decision notice or enforcement notice under FOIA and EIR;*
- *administering fines by way of penalty notices in the circumstances set out in section 155 of the DPA;*
- *administering fixed penalties for failing to meet specific obligations (e.g. a failure to pay the relevant fee to the ICO); and*
- *prosecuting criminal offences before the courts.*

Source: https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf

b) Complaints Received re Kirklees

The Information Commissioner's Office made the Council aware of 7 complaints they had received about Kirklees in respect of data protection; this is an increase on the previous year's 4 complaints made to the ICO. The ICO did not consider regulatory action was required in any case.

Summary	Outcome

Contact details of a previous home owner available via system on Council site	ICO considers that it appears that the data concerned constitutes personal data within the meaning of the Data Protection Act 1998. This is because the data includes the names and email addresses of individuals. ICO decision, is that no further action is necessary at this stage because the incident appears to have been contained due to the remedial action undertaken by the Council in this instance.
Inaccurate data held	ICO notes that all amendments have now been completed and advises that the Council must be mindful when recording information, and ensure that personal data processed is kept accurate. In light of the response from the Council the ICO does not intend to take any further action on this matter.
Complaint that not all information disclosed in response to SAR	Based on the information provided, it does not appear that there is any further information outstanding that should be provided to the applicant and the ICO therefore does not require Kirklees Council to take any further action.
Complaint that not all information disclosed in response to SAR	ICO is satisfied with the response provided and notes that the Council believes it has provided a full response to the subject access requests. ICO is also satisfied with any exemptions applied.
Complaint that Council failed to provide information requested in SAR and failed to respond within statutory timeframe	ICO requires review of SAR and for Council to respond to complainant as soon as possible. ICO has closed the case.
Complaint that Council failed to provide information requested in SAR and document with information obscured	ICO is satisfied that the Council is taking the appropriate steps to address the issues raised in the complaint and will not need to write to the Council again in relation to this matter unless new information becomes available to them.
Complaint that Council failed to locate document and excessively redacted information provided in response to SAR	ICO asked that another copy of document is sent and requires no further action.

Freedom of Information Act 2000 and Environmental Information Regulations 2004

Annual Report 2018-19

Executive Summary

This report details how the Council has performed throughout 2018-19 in respect of information access requests received and processed under the Freedom of Information Act 2000 (FoI) and Environmental Information Regulations 2004 (EIR).

The Council received 1,660 requests during 2018-19 which is 147 more than the number received in 2017-18, which is a 10% increase.

The Council's compliance rate for responding to requests has increased to 89% which is just below the expectation that 90% of responses should be sent out within deadline, although a 2% improvement on the previous year's rate.

Compliance rates have fluctuated greatly over the 12 months, ranging from 81.3% in June 2018 up to 96.3% in November 2018.

The average response time for 2018-19 was 14.7 working days.

Regionally, from the West Yorkshire Councils which have submitted annual figures, there has been a significant in the volume of requests received, with Kirklees seeing the lowest increase at 9.7%, two other Councils having had increases of between 11.5% and 22.2% from the previous year.

The number of internal reviews carried out of the responses to requests has increased slightly on the previous year, from 29 in 2017-18 to 33 in 2018-19. Just under half (15) were dealt with within the timescale set out in the EIR and suggested by the ICO for FoI; the Council has some work to do to ensure that internal reviews are concluded in a more timely manner.

The number of complaints made to the ICO has decreased by 4, from 5 in 2017-18 to 1 in 2018-19. The ICO issued a Decision Notice to the Council directing the Council to disclose the information withheld; this was appealed to the First Tier Tribunal (Information Rights) which determined that only some of the information should be disclosed and the remainder withheld as the Council had originally done.

Lindsay Foody
Information Access & Security Officer

22 July 2019

Contents:

1. **Introduction**

2. **Summary of the Legislation**

   a. Freedom of Information Act 2000
   b. Environmental Information Regulations 2004

3. **Kirklees Context**

4. **Statistics:**

   a. Numbers of Requests
   b. Sources of Requests
   c. Requests by Directorate
   d. Time Taken to Respond to Requests
   e. Outcomes
   f. Internal Reviews

5. **Information Commissioner**

   a. Powers
   b. Complaints Received re Kirklees
   c. Decision Notices
   d. Tribunals

1. Introduction

This report discusses the main events of the year 2018-19 in relation to requests made under the Freedom of Information Act 2000 (FoI Act) and the Environmental Information Regulations 2004 (EIR), along with recommendations for improvements to the processes.

2. Summary of the Legislation

The legislation gives the public rights of access to information held by public authorities. They allow requests to be made by anyone, from anywhere.

a) Freedom of Information Act 2000

The FoI Act has created a general right of access to information held by public authorities. People have the right to be told whether particular information is held in recorded form, and if so, to have a copy of it. Requests for information must be made in writing.

The Act places a number of obligations on public authorities in the way that they respond to information requests, and it also creates a number of exemptions. In particular, personal information about the person requesting information is exempt, because it is available under the GDPR , which also exempts private information about people than the data subject.

Other exemptions include information which is:-

- available by other means;
- intended for future publication;
- held in confidence;
- prejudicial to commercial interests;
- held for investigations and proceedings or law enforcement;
- environmental information, available under the EIR.

In many cases the exemption is not absolute, and we have to take account of the public interest before information can be refused.

The FoI Act also requires the Council to publish a number of classes of information in a Publication Scheme .This scheme commits an authority to publishing important information as part of its normal business activities so that people do not need to make specific requests.

b) Environmental Information Regulations 2004

The EIR give enhanced access to environmental information, by giving members of the public and others the right to access environmental information held by public authorities. A request can be made by letter, email, telephone or in person.

The regulations apply to most public authorities and to any organisation or person under the control of a public authority who has environmental responsibilities. This can include some private companies or public private partnerships, for example companies involved in energy, water, waste and transport.

Environmental information is divided into the following six main areas:

- the state of the elements of the environment, such as air, water, soil, land;
- emissions and discharges, noise, energy, radiation, waste and other such substances;
- measures and activities such as policies, plans, and agreements affecting or likely to affect the state of the elements of the environment;
- reports, cost-benefit and economic analyses used in these policies, plans and agreements;
- the state of human health and safety, contamination of the food chain and cultural sites and built structures (to the extent they may be affected by the state of the elements of the environment).

Environmental information should be proactively made available, and for information which is not already available, the default position is to make information available on request, but the Regulations allow public authorities to refuse requests for information in specific circumstances; these are called 'exceptions'.

3. Kirklees Context

The Information Governance Team, which manages the process of receiving and responding to requests made to the Council under information access legislation, comprises:

- One full-time Information Governance Manager
- one full-time Information Access & Security Officer,
- three full-time and one part time Information Governance Officers (one full-time post is temporary from October 2018 to May 2020)
- one full-time and three part-time Business Support Officers

The Team sits in The Democracy Service, within the Governance & Commissioning part of the Corporate directorate.

The Information Governance Team works with a network of Co-ordinators located within the different service areas across the Council, who arrange for information requested to be collated and draft responses to be signed off by nominated managers.

4. Statistics:

a) Numbers of Requests

The number of Freedom of Information (FoI) and Environmental Information (EIR) requests received between 1 April 2018 and 31 March 2019 has increased by 147 (9.7%) from the

previous year; an increase which averages at 138 requests per month compared to 126 per month in 2017-18:

Monthly	Number
April 2018	152
May 2018	136
June 2018	166
July 2018	162
August 2018	139
September 2018	111
October 2018	136
November 2018	135
December 2018	93
January 2019	163
February 2019	121
March 2019	146
Total	**1660**

Quarterly	Number
Quarter 1	454
Quarter 2	412
Quarter 3	364
Quarter 4	430
Total	**1660**

The following chart plots the figures from the above table:

Number of requests received by month:
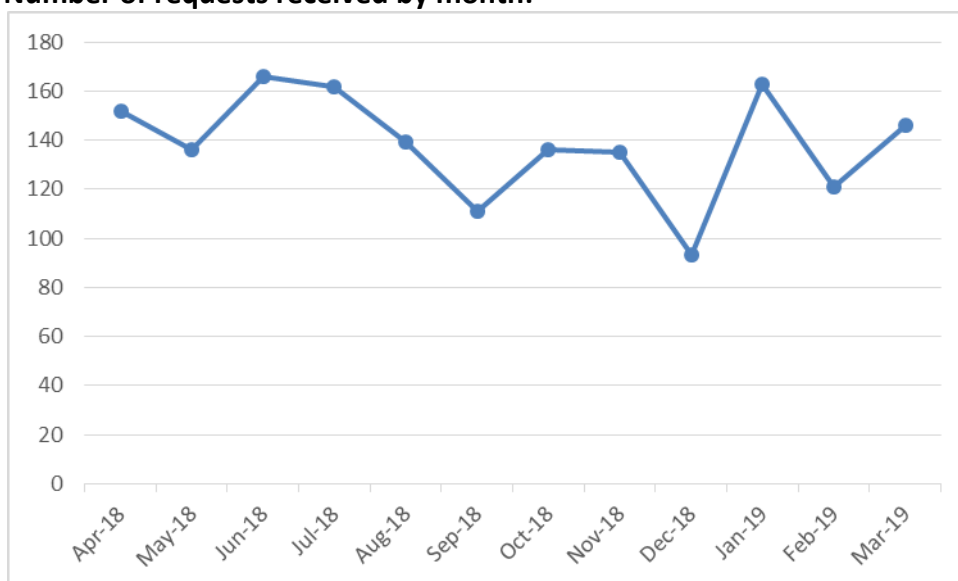
The general trend over the last 10 years is an increase in volume and follows a significant dip in 2017-18 from the previous year:

Qtrs	2009-2010	2010-2011	2011-2012	2012-2013	2013-2014	2014-2015	2015-2016	2016-2017	2017-2018	2018-2019
Qtr 1	135	185	299	332	283	353	336	417	374	454
Qtr 2	182	180	263	273	356	357	350	398	367	412
Qtr 3	193	197	248	218	384	352	361	397	341	364
Qtr 4	194	305	327	343	404	436	450	424	431	430
Totals	**704**	**866**	**1,137**	**1,166**	**1,427**	**1,498**	**1,497**	**1,636**	**1,513**	**1,660**
%Change	*+40%*	*+19%*	*+24%*	*+2%*	*+18%*	*+5%*	*0%*	*+8%*	*-7.5%*	*+9.7%*

The following chart plots the totals received annually from the above table:
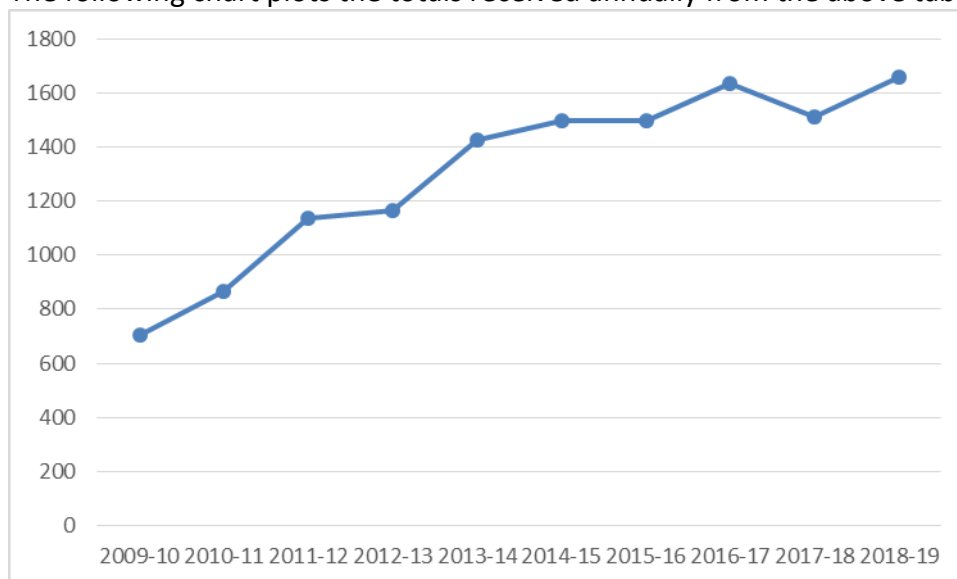
b) Sources of Requests

Whilst both the FOI Act and the EIRs require an applicant to provide a valid name and address, applicants are under no obligation to say why the information is required, or whether they are applying as an individual or on behalf of an organisation. Some applicants do choose to provide this information voluntarily when making a request. The following tables are based on the limited information provided and so should be treated with a degree of caution.

Source of Request 2017-18	Number	% of Total Requests Received
Business	361	21.75%
Clubs, Societies & Charities	69	4.16%
Individuals	179	10.78%
Media	247	14.88%
Other	589	35.48%
Pressure Group (Local & National)	163	9.82%
Research & Academic	52	3.13%
Totals	**1,660**	**100.00%**

Source of Request - Comparison	2017-18	2018-19	Difference
Business	307	361	+54
Clubs & Societies	77	69	-8
Individuals	172	179	+7
Media	250	247	-3
Other	491	589	+98
Pressure Group (Local & National)	150	163	+13
Research & Academic	66	52	-14
Totals	**1,513**	**1,660**	**+147**

Requests which are classified above as 'Other' are generally where the addresses and content of the requests, give little clue as to the requester's identity, background, or the intended use of the information. This is particularly the case with email requests.

c) Requests by Directorate

The total figure in this section (2,222) is higher than the total number of requests received (1,660) because 562 requests were for information held by two or more services. The figures below show the total number of requests each Directorate dealt with, so, for example, where a request was made for information about Social Workers in Adults Services, this was sent to both Adults and HR, and the same request is counted twice times below.

Requests which related to information potentially held by all areas of the Council, for example, for registers of gifts and hospitality, are recorded just once as "Council-wide".

Occasionally, the Council receives requests for information which the Council does not hold and which are transferred on to the public authority which does hold that information, for example, requests about Trading Standards are passed on to West Yorkshire Joint Services, and requests for information held by schools are passed on to the school in question. These are transferred on to the appropriate organisation, with the agreement of the applicant, and recorded as "Not Council – Other Organisation".

Directorate	2018-19	% of Total Requests Received
Children's Social Care & Learning	334	15.03%
Adults' Social Care	119	5.36%
Commissioning & Health Partnerships	29	1.31%
Council-wide	7	0.32%
Communities, Transformation & Change	165	7.43%
Chief Executive's Office	15	0.68%
KNH	62	2.79%
Economy & Infrastructure (formerly Place)	755	33.98%
Public Health	39	1.76%
Resources	686	30.87%
Not Council – Other Organisation	11	0.50%
Total	**2,222**	**100.00%**

d) Time Taken to Respond to Requests

The Act and the Regulations require public authorities including the Council to reply to information requests within 20 working days either providing the information or saying why it cannot be provided.

In 2018-19 1,471 (88.9%) requests were responded to within 20 working days. This is slightly under the threshold that triggers the Information Commissioner's Office's (ICO) monitoring of public authorities when responding to freedom of information requests which is 90%, and is an improvement in performance on 2017-18 (86.9%).

Overall, 93.4% of requests received a response within 25 working days, and although there is nothing within the legislation relating to this timescale, it does demonstrates that where deadlines are being missed, the majority are responded to fairly quickly afterwards, with a many being only a day or two late. This indicates that exceeding the 90% response rate is achievable with some more planning.

Requests Received		Legal Deadline of 20 Working Days		Response Within 25 Working Days	
Monthly	Number	Number	%	Number	%
April 2018	152	132	86.84%	144	94.74%
May 2018	136	123	90.44%	124	91.18%
June 2018	166	135	81.33%	148	89.16%
July 2018	162	144	88.89%	154	95.06%
August 2018	139	130	93.53%	136	97.84%
September 2018	111	105	94.59%	108	97.30%
October 2018	136	118	86.76%	124	91.18%
November 2018	135	130	96.30%	131	97.04%
December 2018	93	84	90.32%	86	92.47%
January 2019	163	141	86.50%	149	91.41%
February 2019	121	105	86.78%	110	90.91%
March 2019	146	124	84.93%	135	92.47%
Total	1,660	1,471	88.93%	1,549	93.40%

The Council met or exceeded the ICO's expected compliance rate in 5 months of the year.

e) Outcomes

The FoI Act and the EIRs have a limited number of circumstances under which requested information can be withheld. Under the FoI Act these are called 'exemptions' and under EIR these are called 'exceptions'. There are 8 'absolute' FoI exemptions, the remainder are 'qualified' which means that the Council has to consider whether the public interest in withholding the information outweighs the public interest in providing it or not. Under EIR, all the exceptions are qualified.

The legislation assumes that requested information will be disclosed unless one or more of the exemptions or exceptions is engaged. Of the 1,660 requests received during 2018-19, the Council provided the information requested on the majority of occasions. Where an applicant subsequently withdrew their request, this was recorded as 'Discontinued'. On occasions, the Council is asked for information which is does not hold, for example, trading standards or crime information, which is held by other organisations and not the Council; requests may also for information which the Council does not already hold and has no requirement to hold, for example, the number of times a particular birth certificate has been viewed/ordered – in these cases the outcome is recorded as "Not Held".

In a small number of cases, the Council has refused to either confirm or deny whether it holds any requested information. The FoI Act allows a public authority to do this only where a confirmation that requested information is or is not held would in itself reveal information that falls under an exemption. This is called a 'neither confirm nor deny' (NCND) response.

Outcome	2017-18	% of Total Requests Received
Supplied (all or in part)	1,041	62.71%
Refused (all or in part)	447	26.93%
Not Held (and referred)	108	6.50%
Discontinued (and duplicate)	63	3.80%
Neither Confirm Nor Deny	1	0.06%
Total	**1,660**	**100.00%**

Some requests were refused, in whole or in part, and the relevant exemption or exception applied. In some cases, two or more FoI exemptions applied to information requested in a single request, and so the total number of times exemptions or exceptions were applied will exceed the total number of requests received.

During 2018-19 480 exemptions / exceptions were applied (in whole or in part) to 448 requests (this number includes 1 request for which information was not held for the purpose of the FoI Act and is recorded as 'Not Held' in the table above as well as the 1 case which are recorded as 'Neither Confirm Nor Deny'):

FoI Exemptions / EIR Exceptions Applied			2018-19	% Total Requests Refused
EIR	reg12(4)(b)	Manifestly unreasonable	10	2.08%
EIR	reg12(5)(a)	International relations, defence, national security, public safety	1	0.21%
EIR	reg12(5)(b)	The course of justice, fair trial, conduct of a criminal or disciplinary inquiry	1	0.21%
EIR	reg12(5)(d)	Confidentiality of public authority proceedings when covered by law	1	0.21%
EIR	reg12(5)(e)	Confidentiality of commercial or industrial information when protected by law to cover legitimate economic interest	3	0.63%
EIR	reg12(5)(f)	Confidentiality of commercial or industrial information when protected by law to cover legitimate economic interest	1	0.21%
EIR	reg13	Personal data	40	8.33%
FoI	s12	cost of compliance exceeds appropriate limit	77	16.04%
FoI	S14	Repeated or vexatious request	16	3.33%
FoI	s21	Information reasonably accessible by other means	159	33.13%
FoI	s22	Information intended for future publication	1	0.21%
FoI	s24	National security	1	0.21%
FoI	s3(2)(a)	Not held for the purposes of the FoI Act	1	0.21%
FoI	s31	Law enforcement	58	12.08%
FoI	s38	Health and safety	1	0.21%

FoI	s40	Personal information		89	18.54%
FoI	s41	Information provided in confidence		1	0.21%
FoI	s42	Legal professional privilege		2	0.42%
FoI	s43	Commercial interests		17	3.54%
			Total	**480**	**100.00%**

f) Internal Reviews

Where an applicant is unhappy with the response received to their information request they can ask for an internal review of the handling of the request / response received.

Internal reviews are carried out by officers in Legal Services who have had no input to the original response. The FoI Act does not specify a timescale for completing internal reviews, but the ICO requires these to be done promptly within a reasonable timescale, which he considers to be 20 workings days from receipt of the request. The EIRs require internal reviews to be completed within 40 workings days of receipt of the request.

In 2018-19 the Council carried out 33 internal reviews, compared with 29 in 2017-18:

Monthly	Number received	Responded to within Deadline	% in deadline	Average Time to respond (working days)
April 2018	4	2	50%	28.5
May 2018	2	1	50%	19
June 2018	2	2	100%	19
July 2018	2	2	100%	19.5
August 2018	1	1	100%	16
September 2018	6	4	67%	21.67
October 2018	2	1	50%	12
November 2018	6	1	17%	51
December 2018	3	0	0%	45.5
January 2019	2	1	50%	22
February 2019	3	0	0%	45
March 2019	0	0	0%	0
Total	**33**	**15**	**49%**	**Av: 24.96**

At the time of writing, 1 internal review decision remains outstanding and is overdue.

Internal Review Outcome	2018-19	% of Total Requests Received
Discontinued	3	9.09%
Not Upheld	15	45.45%
Partially Upheld	3	9.09%
Upheld	11	33.33%
Open (and overdue)	1	3.03%
Total	**33**	**100.00%**

Although there is no timescale for completion of internal reviews which is set out in the FoI legislation, the Council would wish to see a significant improvement in the timescales for FoI reviews.

5. Information Commissioner

The Information Commissioner's Office (ICO) is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

a) Powers

There are a number of tools available to the ICO for taking action to help organisations follow the legislation they cover. They include non-criminal enforcement and assessments of good practice.

The ICO's regulatory activity (and activity in support of regulatory activity) includes:

- *conducting assessments of compliance with the DPA and GDPR, PECR, e-IDAS, NIS, FOIA and EIR;*
- *issuing information notices;*
- *issuing 'urgent' information notices under the DPA, requiring individuals, controllers or processors to provide information on not less than 24 hours' notice;*
- *applying for a court order requiring compliance with the information notice issued under the DPA, if the recipient does not provide a full and timely response;*
- *issuing assessment notices under DPA;*
- *issuing 'urgent' assessment notices under the DPA, requiring controllers or processors to allow us to undertake an assessment of whether they are compliant with the data protection legislation, on not less than 7 days notice;*
- *issuing no-notice (or short notice) assessment notices under the DPA where we have reasonable grounds to suspect that the controller or processor has failed or is failing to comply with certain provisions of the data protection legislation or has committed or is committing an offence under the DPA, allowing us to undertake an assessment on less than 7 days notice;*
- *producing codes of practice about data sharing and direct marketing, and any other codes of practice that we are required to produce under the legislation we cover;*
- *conducting assessments of cross-border data transfers and corporate groups' binding corporate rules;*
- *overseeing data protection impact assessments;*
- *conducting audits and assessments under IPA and other information rights legislation;*
- *overseeing the establishment of data protection certification mechanisms;*
- *encouraging the development of codes of conduct, and accrediting bodies to monitor compliance with codes of conduct;*
- *requiring a controller or digital service provider to inform an individual of a personal data breach;*
- *issuing a warning where proposed action threatens non-compliance with data protection legislation;*

- *issuing a reprimand for infringements of relevant data protection legislation;*
- *issuing practice recommendations under FOIA and EIR and decision notices detailing the outcome of an ICO investigation into an individual's case under FOIA or EIR;*
- *issuing enforcement notices orders requiring specific actions by an individual or organisation to resolve breaches (including potential breaches) of applicable information rights obligations. An 'urgent' enforcement notice under the DPA may be used to require action to resolve breaches or potential breaches of the data protection legislation, on not less than 24 hours' notice;*
- *certifying contempt of court should an authority fail to comply with an information notice, decision notice or enforcement notice under FOIA and EIR;*
- *administering fines by way of penalty notices in the circumstances set out in section 155 of the DPA;*
- *administering fixed penalties for failing to meet specific obligations (e.g. a failure to pay the relevant fee to the ICO); and*
- *prosecuting criminal offences before the courts.*

Source: https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf

b) Complaints Received about Kirklees

The ICO made the Council aware of 1 complaint they had received about Kirklees' handling of FoI and EIR requests, a decrease of 4 from the 5 notified in 2017-18:

Summary	Outcome
Complaint about redaction of information under redaction of document under r12(5)(e) and r12(5)(f)	ICO served Decision Notice on Council to disclose the information requested or appeal to the First-tier Tribunal (Information Rights) **See Decision Notice FS50729956 below**

c) Decision Notices

When a complaint is made under the FOI Act against a public authority, the ICO investigates the facts behind the complaint and may then issue a decision notice. This is the Commissioner's view on whether or not the public authority has complied with the FoI Act or the EIR and can include legally binding steps for the public authority to follow.

When a decision notice is issued, the ICO informs both parties of their right to appeal to the First-tier Tribunal (Information Rights).

The ICO published the following Decision Notice in relation to the one complaint made about Kirklees in 2018-19:

Kirklees Metropolitan Council
The complainant has requested information about land adjacent to a Redrow housing development in Huddersfield. Kirklees Metropolitan Borough Council disclosed some information and withheld other information under the exceptions for commercial

confidentiality (regulation 12(5)(e)) and interests of the information provider (regulation 12(5)(f)). The Commissioner's decision is that Kirklees Metropolitan Borough Council has failed to demonstrate that regulation 12(5)(e) and regulation 12(5)(f) is engaged. The Commissioner requires the public authority to disclose the requested information to the complainant. This decision notice is currently under appeal to the Tribunal. FOI 10: View a PDF of Decision notice FS50729956

Source: *https://icosearch.ico.org.uk/s/search.html?query=FS50729956&collection=ico-meta&profile=_default*

d) Tribunals

One appeal to the First Tier Tribunal (Information Rights) was lodged during 2018-19 in respect of ICO Decision Notice **FS50729956** in October 2018. The FTT hearing date was 25 April 2019. The FTT determined that only some of the information should be disclosed and the remainder withheld as the Council had originally done. FTT Case EA/2018/0218 refers.

Appendix F – Local Government Transparency Code

	2017		2018		2019		2020	
	MUST be published	**Recommended for publication**	**MUST be published**	**Recommended for publication**	**MUST be published**	**Recommended for publication**	**MUST be published**	**Recommended for publication**
Expenditure Exceeding £500	🟢	🟢	🟢	🟢	🟢	🟢		
	2 identifiers are not published: - Summary of purpose - Unrecoverable VAT		1 identifier is not published: - Unrecoverable VAT Personal data redacted where appropriate.		1 identifier is not published: - Unrecoverable VAT			
Government Procurement Card Transactions	🟢	🟢	🟢	🟢	🟢	🟢		
	3 categories are not published: - VAT - Summary of purpose - Merchant Category		2 categories are not published: - VAT - Summary of purpose Personal data redacted where appropriate.		2 categories are not published: - VAT - Summary of purpose			
Procurement information	🟢	🟡	🟢	🟡	🟢	🟡		
	Publishing contracts on Yortender £5k & above is not prescribed by procurement and £20k still remains the limit. Now publishing on Contracts Finder [.gov.uk site] – publishing >£25k as this is what is stipulated to procurement for non central government. The code asks for >10k.							

	2017		2018		2019		2020	
	MUST be published	**Recommended for publication**	**MUST be published**	**Recommended for publication**	**MUST be published**	**Recommended for publication**	**MUST be published**	**Recommended for publication**
Local Authority Land	(amber)	(red)	(amber)	(amber)	(amber)	(amber)		
	1 definite category is not published: - Land or building asset The Electronic Property Information Mapping Service [EPims] is currently being trialled by the service. The type of date upload and frequency is being considered.		1 definite category is not published: - Land or building asset The Electronic Property Information Mapping Service [EPims] is currently being used by the service to publish this information too. The frequency of publication still remains yearly and not more frequent as stated in the 'recommended' element.		1 definite category is not published: - Land or building asset The Electronic Property Information Mapping Service [EPims] is currently being used by the service to publish this information too. The frequency of publication still remains yearly and not more frequent as stated in the 'recommended' element.			
Grants to voluntary, community & social enterprises and organisations	(green)	(red)	(green)	(red)	(green)	(red)		
	It is currently an annual publication due to the manual collation that is required so difficult to move to a dynamic or more frequent reporting schedule. Not possible to disaggregate by various sectors as currently not recorded.							
Organisation Chart	(green)	(green)	(green)	(green)	(green)	(green)		
	It is currently an annual publication due to the manual collation that is required so difficult to move to a dynamic or more frequent reporting schedule.							

	2017		2018		2019		2020	
	MUST be published	**Recommended for publication**	**MUST be published**	**Recommended for publication**	**MUST be published**	**Recommended for publication**	**MUST be published**	**Recommended for publication**
Trade Union Facility Time	🟢	N/A	🟢	N/A	🟢	N/A		
	There are no "Recommended" Requirements							
Parking Account	🟡	N/A	🟡	N/A	N/A Publication Date Due	N/A		
	It is currently an annual publication due to the manual collation that is required so difficult to move to a dynamic or more frequent reporting schedule. Not possible to disaggregate by various sectors as currently not recorded. Published in August/September when the accounts are finalised.							
Controlled Parking Space	🟢	🟢	🟢	🟢	🟢	🟢		
	The information requested is available. Accessibility could be improved by offering aggregated figures [although this is not specified precisely in the guidance].							
Senior Salaries	🔴	N/A	🟡	N/A	🟡	N/A		
	Information received from service is still not fully compliant. The code requires listed responsibilities for all positions with a salary of £50,000 upwards [not just for the first 3 tiers]. It is also missing budget levels & staffing numbers associated with each officer.		Information received from service is still not fully compliant. The code requires listed responsibilities for all positions with a salary of £50,000 upwards [not just for the first 3 tiers]. It is also missing budget levels & staffing numbers associated with each officer.		Information received from service is still not fully compliant. The code requires listed responsibilities for all positions with a salary of £50,000 upwards [not just for the first 3 tiers]. It is also missing budget levels & staffing numbers associated with each officer.			

	2017		2018		2019		2020	
	MUST be published	**Recommended for publication**	**MUST be published**	**Recommended for publication**	**MUST be published**	**Recommended for publication**	**MUST be published**	**Recommended for publication**
Constitution	🟢	N/A	🟢	N/A	🟢	N/A		
	Direct feed to web link – if content changes, link will update.							
Pay Multiple	🟢	N/A	🟢	N/A	🟢	N/A		
	No comment to add							
Fraud	🟢	🟢	🟢	🟢	🔴	🔴		
	Data now includes spend on investigation & fraud.				Problems with data extraction tools is preventing an update. Will be published when these have been fully resolved.			
Social Housing Asset Value	🟢	N/A	🟢	N/A	N/A Publication Date Due	N/A		
	Data routinely published in the month of September		Data routinely published in the month of September		Data routinely published in the month of September			
WasContract	Not applicable for Kirklees.							

Anna Bowtell
Research & Intelligence Manager
Performance & Intelligence Service
September 2019