

Information Governance Annual Report

2017/18

Contents

Executive Summary	3
Introduction.....	4
Background	5
Work completed through 2017/18.....	6
NHS IG Toolkit Accreditation	6
Data Protection	7
<i>Disclosures</i>	7
General Data Protection Regulation (GDPR).....	7
Freedom of Information Act 2000 & Environmental Information Regulations 2004	8
<i>Cost of Fol requests</i>	8
<i>Internal reviews and Complaints</i>	8
Open Data	9
Data Sharing	10
Information Security	10
Governance.....	11
Training and Awareness.....	12
Information Risk Management.....	12
Information Governance Resources and Budget	13
Legislation Changes	14
Work Programme for 2018/19	15
Conclusion.....	15
Appendices.....	17
Appendix A – IG Board Terms of Reference.....	18
Appendix B – DPA Annual Report	22
Appendix C – Fol and EIR Annual Report.....	34
Appendix D – Local Government Transparency Code	49

Executive Summary

This Information Governance Annual Report sets out how the Council has performed throughout 2017/18 against the Council's 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.

An outline for the work programme for 2018/19 is provided towards the end of this report, to enable Members to understand how IG is being further developed and embedded within the Council.

There have been significant achievements throughout the year including:

- Achievement of the Level 2 Accreditation for the NHS IG Toolkit with a score of 73% - an increase from 2016/17 evidencing an improved IG culture across the Council
- The introduction of an electronic Information Sharing Gateway to improve the administration of information sharing between the Council and Partners
- The launch of an online information security incident form, allowing a simple and risk assessed reporting for information security incidents
- Strong development of IG concepts supported by Agilisys, an IG Consultant
- New IG positions were created and filled to support the establishment of a robust IG culture across the organisation
- Significant strides made in preparation for the new General Data Protection Regulation legislation, including the provision of significant support for Councillors

These achievements required 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.

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.

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. This is an important foundation for the intelligence 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
- Information Governance Strategy which incorporates
 - Information Governance Policies
 - Information Sharing Policies and Guidance
 - Records Management Policies and Guidance
 - Information Security Policies and Guidance

The IG Framework and its corresponding Strategy is updated annually to reflect the changes required to develop IG to support a more effective use of Council information.

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). The Terms of Reference for the Board are updated annually and the ones in place for 2017/18 can be found in Appendix A. They have recently been updated again in 2018/19 and membership/employee titles updated.

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 achievements made within 2017/18 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 Service Directors, who are also known as Information Asset Owners, have had training throughout November to help them understand how they will manage the 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 Council's Records Management Plan, has continued to be developed in accordance with the Model Records Management Plan requirements of the

Keeper of Records Scotland, and is being implemented across all Services to ensure the Councils records are logged and managed effectively in compliance with the Records Management Policy and deadline with the rollout of new technologies.

- The central Archive was opened the Red Doles Lane site, and it is currently being filled in order to eventually contain all paper records which the Council holds.
- Training for all employees is now available to ensure a robust IG culture is embedded throughout the organisation.

Work completed through 2017/18

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.

NHS IG 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.

For Local Authorities this Toolkit focuses on the following topic areas:

1. Information Governance Management
2. Confidentiality & Data Protection Assurance
3. Information Security Assurance
4. Care Records Assurance

Achieving this standard requires significant resource investment and compliance with rigorous IG standards by the whole organisation. Whilst the Council has achieved level 2 consistently since 2015/16, it has to also evidence a record of improvement as working towards level 3. The track record of 'working towards level 3' has continued into 2017/18, the results are shown below:

Financial Year	IG Toolkit Score
2015/16	66%
2016/17	71%
2017/18	73%

The score of 73% is a very strong assessment, which is verified by Internal Audit and signed off by the IG Board prior to any submission being made to NHS Digital. It demonstrates the strong and continued positive change across Council departments towards effective and secure information governance.

In 2018/19 the IG Toolkit is being replaced by the Data Security and Protection Toolkit, which will have different requirements to the previous toolkit and therefore this will be the final statement of this type within the Annual Reports.

Data Protection

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

Data protection requests are currently managed 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 an increase of 11% on last year from 201 in 2016/17 to 223 in 2017/18.

The response rate by Kirklees Council to these requests has increased slightly from 82% compliance in 2016/17 to 83.5% compliance in 2017/18. This is well below the ICO's required compliance rate of 90% within 40 calendar days. More detail on these figures can be found in Information Governance **Board**

Terms of Reference

(Updated May 2017)

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, Councillors, Contractors and Partners on IG related matters
- Address Information Security risks and establish a risk management framework;
- Establish, monitor and enforce legal compliance with regards to Information Governance including authorising and approving Data Sharing Agreements;
- 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.

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 and Senior Support 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 2017/18 these will include:

- GDPR Implementation Team – this group will meet every fortnight with representation from each service area. The aim is to support each other to implement preparation required to achieve GDPR compliance in May 2018

Board membership

The Board is made up of Council Officers, with all Directorates represented. The 2017/18 membership is outlined in Appendix A

Appendix A

Information Governance Board Membership 2017/18

Chair -	Julie Muscroft (SIRO) – Service Director for Legal, Governance and Commissioning
Commissioning & Health Partnerships	Saf Bhuta (Caldicott Guardian) – Directorate Lead for Performance, Intelligence and Business Systems
Democracy Service	Carl Whistlecraft – Head of Democracy
	Katy Deacon - Information Governance & Senior Support Manager
	Lindsay Foody – Information Access & Security Officer
IT -	Andrew Brammall – Head of IT and Change
	Terence Hudson – IT Operational Manager
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 -	Helen Rhodes – Senior Communications Officer
Learning Service	Martin Green – Head of Localities Offer – Children & Families
Safe & Cohesive Communities	Warren Ellis – Communities Service
Public Health -	Sean Westerby – Emergency Planning & Business Continuity Manager
Investment & Regeneration	Adele Buckley - Head of Regeneration, Environment and Funding
	Jane Lockwood – Procurement Strategy and Advice Manager

Appendix B.

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 of 40 days to assist with monitoring performance around disclosures.

In 2017-18 the Council received 435 disclosure requests which is a very slight decrease of less than 0.2% on the number received in 2016-17 (436) and achieved a 94% response rate within 40 days, which is an improvement on the 91% rate in 2016-17

General Data Protection Regulation (GDPR)

In May 2016 a new Regulation was passed which brings all European countries into line with the same rules around data protection. The GDPR came into force in May 2018. Many of the concepts and principles of the Data Protection Act 1998 (DPA) are the same within the GDPR however there are some new elements and some significant enhancements, so the Council has needed to approach data protection differently in order to remain compliant.

The GDPR places greater emphasis on the documentation that the Council, as a data controller, must keep to demonstrate their accountability. Compliance with GDPR will require the Council to review our approach to information governance and how we must manage data protection as a corporate issue.

Throughout 2017/18 the Information Governance Board has increased the work started in 2016/17 to adapt policies, increase training, identify all information assets and strengthen arrangements with partners to ensure the Council remains compliant with the new legislation. Further information about GDPR can be found in the [Legislation Changes](#) section of this report.

Freedom of Information Act 2000 & Environmental Information Regulations 2004

This section details how the Council has performed throughout the 2017/18 year in respect of information access requests received and processed under the Freedom of Information Act 2000 (Fol) 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 1,513 requests during 2017-18 which is 122 less than the number received in 2015-16, which is a 7.5% decrease.

The Council's compliance rate for responding to requests has increased to 87% which is below the Information Commissioner's Office (ICO) current minimum standard of 90% of responses should be sent out within deadline.

Compliance rates have fluctuated greatly over the 12 months, ranging from 73% in June 2017 up to 94.5% in January 2018;

The average response time for 2017-18 was, at the time of writing, 14.5 working days.

The decrease in the volume of requests received is a common theme across most of the West Yorkshire Councils, Kirklees has the highest increase at 7.5%, two other Councils having had decreases of between 1.4% and 6% from the previous year.

Cost of Fol requests

The Council estimates the average cost of responding to Fol requests is £269 per request. This results in an estimated cost of responding to FOI requests at £408,128.

Internal reviews and Complaints

The number of internal reviews carried out of the responses to requests has decreased significantly on the previous year, from 80 in 2016-17 to 29 in 2017-18. Two-thirds were dealt with within the timescale set out in the EIR and suggested by the ICO for Fol; 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 9, from 14 in 2016-17 to 5 in 2017-18. The ICO did not take any regulatory action against the Council in any of the cases they have made a decision on. Two ICO Decision Notices from 2016-17 was appealed to the First Tier Tribunal (Information Rights) in 2017-18; one was dismissed and the other was upheld.

The IG Board reviews Fol 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 Fol requests in a more timely and consistent manner was recognised with new response procedures have been established for 2018/19.

More detail on the Fol and EIR response rates for 2017/18 is included in the Freedom of Information Act 2000 and Environmental Information Regulations 2004 Annual Report in Appendix C.

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.

For 2017 & 2018, this local emphasis on requesting data that meets the recommended element of the code has continued and some compliance improvements from 2016 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 2017/18 can be found in Appendix D.

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.

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.

During 2017/18 a new approach for information sharing has been adopted by the Council. This approach is known as the [Information Sharing Gateway](#) (ISG) which has been developed by the Lancashire & Cumbria IG Group in order to improve and modernise the administration and risk assessment of information sharing in the public sector. The IG Board received representation from Leeds City Council to explain the ISG and the board agreed that this would be a very effective way forward for Council information sharing. The IG Team has been setting up and developing the gateway for the Council since February 2018 and this will be the approach adopted for information sharing mechanisms for 2018/19.

Information Security

This area of work has received significant focus during the 2017/18 financial year, in preparation for the new requirements being brought in by GDPR. The Council has had to improve awareness and reporting of information security incidents. With this, the process to identify and escalate those incidents deemed as security breaches has also had to be modified and improved.

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

In January 2018, a new online reporting tool 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 through the final quarter of the year.

By the end of March there were **93** Information Security incidents reported in 2017/18. These incidents are recorded by the Information Governance Team and each incident was considered by at least one IG Officer and, where appropriate, raised to Senior Managers for assessment against criteria for reporting to the ICO. Each of these incidents is investigated and training and communications implemented to mitigate against repeated incidents of these types.

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.

During 2017/18, two incidents were considered to meet the criteria which require notification to the ICO. In each case, the ICO was satisfied with the action taken and planned to be taken by the Council to mitigate against any impact on the individual(s) and made recommendations relating to training and staff communications.

Governance

Throughout 2017/18 the IG Board focus has adjusted from the focus on the IG Toolkit requirements to a broader GDPR focus in addition to the recognised activities from the IG Action plan.

There a strong corporate understanding of Information Governance and the opportunities it presents. We have strong commitment from the New Council Transformation budget to put in place more resources to develop the IG culture and facilitate Services to establishing robust IG practices. The Council commissioned Agilisys, a national IG consultant, to come in and work with the IG team to develop a strong IG Strategy, Records Management Plan, Publication and Transparency framework and establish an organisation Information Asset Register. This work took nine months and resulted in some excellent pieces of work for the Council to take forward and develop further. These pieces of work link back to the IG Framework discussed earlier and will play a part in strengthening this framework for the future. The resulting work will be included within the Information Management Strategy planned for approval in summer 2018 and details will be included in the 2018/19 Annual Report.

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 intelligence work.

The IG Board performs a council-wide, strategic role for Information Governance, supported by more operational task groups. In 2017/18 the task groups were adjusted to focus solely on GDPR preparation. The GDPR Implementation Task Group met every fortnight from October 2017 to the end of the 2017/18 year. More detail of the work of this group can be found in the section [Legislation Changes](#).

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, councillors, 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 to ensure that every individual working within the Council can access IG training as required. A new approach to IG Training was purchased under IG Board instruction in 2016 which ensures all users of IT equipment access news updates relating to IG matters in addition to the mandatory training.

Information Risk Management

Information Risk encompasses all the challenges that result from an organisation's need to control and protect its information. Poorly managed information could lead to a material impact on the Council's operation. Information risks can affect the Council:

- financially
- operationally
- they can damage reputation
- they can lead to regulatory sanctions

The purpose of information risk management (IRM) is to reduce the Council's information risks to an acceptable level and to keep them under control in a manageable way, rather than try to eliminate them entirely. The IG Board has a standing agenda item for IRM, which means that any identified risks are highlighted and resulting action agreed, to keep the risk manageable and mitigating actions effective.

Information Governance Resources and Budget

In 2016/17 the Transformation Fund paid for three temporary IG Officers and the time of a consultant to carry out specific activities to improve the approach for the Council moving forward. In 2017/18, the IG Officer posts were filled and operating successfully across the areas of Records Management, Data Protection Compliance Information Sharing, Information Security and GDPR preparation.

Legislation Changes

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

The 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 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 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.

Throughout the year, it has also been important to support councillors with their preparation for the new legislation, as ward members are classed as Data Controllers for their ward work and therefore have strengthened responsibilities under GDPR. Presentations have been made to leading members, Group Business Managers and political Groups where officers have been invited. This support will

continue throughout the coming financial year, to ensure that councillors are comfortable with their responsibilities under GDPR.

The IG Board and Executive Team have been updated regularly throughout the year on progress towards GDPR compliance. By the end of 2017/18 significant progress had been made across many services, however as the legislation only came into force on May 25 2018 it was identified that there is still work to be done in the coming financial year.

Work Programme for 2018/19

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

GDPR Assurance project – a project to identify the status of each Service with regards to GDPR preparations. This project will identify key areas for further support and provide opportunities to access the support required. This will be carried out in the form of an online self-assessment in September 2018. Following this assessment and the subsequent support they receive, Services will be asked complete a further self-assessment in March 2019 to identify how well they are complying with GDPR..

Record Management and Asset Mapping – GDPR has highlighted an number of key areas which require further development. The councils information asset register is one of these in addition to the ongoing development and adoption of the records management plan.

Information protection - this project builds upon the records management plan highlighted throughout 2017/18 financial year that concentrates solely on the protection of electronic information. This project will run alongside the council's rollout of new technology to all officers and Councillors.

Information Management Strategy – following the work with Agilisys, the draft Information Management Strategy was agreed with Executive Team. This will be rolled out to the Council through 2018/19 and help link the specific GDPR work from 2017/18.

Improvements to Freedom of Information (Fol) and Transparency – significant work was carried out by Agilisys around open data, transparency and Fol 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.

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 will be preparing a Cyber Security Strategy for ET approval.

Conclusion

As was identified in 2016/17, there is now a much better understanding of information governance across the organisation. This has been aided by the significant involvement from services into GPPR preparation, but it has also been helped by the wider understanding of the organisation to be intelligence and open data agenda.

The positive work carried out by Agilisys during this financial year has meant that great strides have been made in some specific areas. It is now the job of the IG Board, supported by the IG team, to get these high-level strategies implemented throughout 2018/19.

The work throughout this financial year has increasingly focused on GDPR preparation. Whilst it has been important to carry on certain development activities, the changes that have been required in order to start all services focusing on GDPR compliance have meant that the work, particularly in the latter half of the year, has been solely on GDPR preparation.

To support this, the IG team have adjusted the approaches to information request compliance, meaning that since September 2017 the new GDPR timescales have been in effect. As can be seen from the results identified, this has made some positive impact however it has also highlighted areas of concern for the coming financial year.

There has been some considerable effort from certain services in relation to GDPR preparation, and these services have fed in to the wider Council situation to help colleagues in other services improve and change as required. The ongoing work to help to ensure GDPR compliance by the end of 2018/19 will benefit from the commitment of all services.

The work required to ensure GDPR compliance is in place across the organisation will take time and will be on-going thereafter (as was DPA 1998 compliance previously), however there will be a much clearer picture relating to how each service is complying with GDPR requirements available for the committee at the end of the 2018/19. If required, a summary report can be brought in early 2019 to update the committee on progress made within the 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 a half yearly update would be useful.

Appendices

Appendix A – IG Board Terms of Reference

Information Governance Board

Terms of Reference

(Updated May 2017)

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, Councillors, Contractors and Partners on IG related matters
- Address Information Security risks and establish a risk management framework;
- Establish, monitor and enforce legal compliance with regards to Information Governance including authorising and approving Data Sharing Agreements;
- 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.

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 and Senior Support 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 2017/18 these will include:

- GDPR Implementation Team – this group will meet every fortnight with representation from each service area. The aim is to support each other to implement preparation required to achieve GDPR compliance in May 2018

Board membership

The Board is made up of Council Officers, with all Directorates represented. The 2017/18 membership is outlined in Appendix A

Appendix A

Information Governance Board Membership 2017/18

Chair -	Julie Muscroft (SIRO) – Service Director for Legal, Governance and Commissioning
Commissioning & Health Partnerships	Saf Bhuta (Caldicott Guardian) – Directorate Lead for Performance, Intelligence and Business Systems
Democracy Service	Carl Whistlecraft – Head of Democracy
	Katy Deacon - Information Governance & Senior Support Manager
	Lindsay Foody – Information Access & Security Officer
IT -	Andrew Brammall – Head of IT and Change
	Terence Hudson – IT Operational Manager
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 -	Helen Rhodes – Senior Communications Officer
Learning Service	Martin Green – Head of Localities Offer – Children & Families
Safe & Cohesive Communities	Warren Ellis – Communities Service
Public Health -	Sean Westerby – Emergency Planning & Business Continuity Manager
Investment & Regeneration	Adele Buckley - Head of Regeneration, Environment and Funding
	Jane Lockwood – Procurement Strategy and Advice Manager

**Data Subject Access Requests
Data Protection Act 1998**

Annual Report 2017-18

Executive Summary

This report details how the Council has performed throughout 2017-18 in respect of requests for access to personal information received and processed under the Data Protection Act 1998 (DPA98).

During 2017-18, Kirklees Council received 22 more requests (an 11% increase) for access to personal information than it did in the previous 12 months, increasing from 201 in 2016-17 to 223 in 2017-18.

The Council's performance in terms of compliance with the legislative timescales increased slightly from the previous year, from 82% to 83.5%. The number of requests responded to within the statutory 40 calendar day timescale allowed under the DPA98 is well below the ICO's minimum expectation of 90% compliance.

The Council's performance in terms of the time taken to respond to requests appears to have improved when looking at the average response time for dealing with requests; it was 23.3 days in 2017-18 compared with 32.7 days in 2016-17. This does remain within the statutory 40 calendar day timescale allowed under the DPA98 and where the Council has not been able to respond within the statutory deadline this is generally because the requests are complex and voluminous.

The compliance rate has been of concern in the lead up to the implementation of the General Data Protection (GDPR) which is the new data protection legislation which came into force on 25 May 2018, and saw the time for compliance reduce from 40 calendar days to one month (so 28-31 calendar days depending on when the request was received). From September 2017, the Council implemented a 30 calendar day time for compliance for SARs to help colleagues dealing with SARs adjust their work ahead of GDPR coming in to force. During 2017-18 the Council responded to 71% of requests within 30 calendar days which is a significant improvement on 2016-17 when the Council responded to just 57% of requests within 30 calendar days. There remains work to do to meet the new, reduced time for compliance to meet the ICO's minimum standards but the statistics are encouraging.

The DPA98 did not provide for an extension of time to deal with requests. It is worth noting that the ICO does not take mitigating factors such as public holidays or lack of resources into account when making decisions about regulatory action to be taken. The Council does still need 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, three other Councils having had between 0.8% and 25.5% 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

23 August 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 2017-18 in relation to requests made under the Data Protection Act 1998, along with recommendations for improvements to the processes.

2. Summary of the Legislation

[Section 7](#) of the Data Protection Act 1998 (DPA98) gives individuals important rights including the right to know what information is held about them and the right to correct information that is wrong. The Act helps to protect the interests of individuals by obliging organisations to manage the personal information they hold in an appropriate way.

The DPA98 sets out eight principles governing the use of personal data with which data controllers must comply unless an exemption applies:

- **Principle 1 – Personal data shall be processed fairly and lawfully**
This means that any personal data collected by an organisation must be provided with the consent of the individual. To be seen as acting fairly, the organisation collecting personal data must be transparent and ensure individuals are fully informed and understand what will happen to their personal information.
- **Principle 2 – Personal data shall be obtained for one or more specified and lawful purpose(s)**
This means that collected information must only be held and used for the reasons given to the Information Commissioner’s Office (ICO) and the individual. Personal information must not be processed in any manner incompatible with the original purpose(s).
- **Principle 3 – Information collected must be adequate, relevant and not excessive**
This means that all data collected must be necessary to complete the needs of the data controller, who should not ask for or hold any personal data that is outside their concern. They will be in breach of the Data Protection Act if they hold data irrelevant to their purpose(s).
- **Principle 4 – Information collected must be accurate and up to date**
Data controllers must make every effort available to ensure the information they use is accurate. Inaccurate use could result in misrepresentation on behalf of the individual.
- **Principle 5 – Information must not be held for longer than is necessary**
The Data Protection Act states that a data controller must not hold onto data for any longer than is necessary. Retention schedules should be in place and records held

(including personal data) review regularly and any information no longer needed should be securely destroyed or archived as appropriate.

- **Principle 6 – Information must be processed in accordance with the individual’s rights**

This includes:

- A right of access to a copy of their information which is held;
- A right to object to processing their data;
- A right to prevent processing for direct marketing;
- A right to have inaccurate personal data rectified, blocked, erased, or destroyed;
- A claim to compensation for damaged caused by a breach of the Act.

- **Principle 7 – Information must be kept secure**

Data controllers have a duty to ensure personal information held is kept securely and appropriate technical and organisational measures taken to prevent unauthorised access and accidental loss, disclosure, destruction of or damage to it. Significant monetary penalties may be incurred for data protection breaches.

- **Principle 8 – Information should not be transferred outside the European Economic Area unless adequate levels of protection exist.**

This means that any personal information held by a data controller must not be stored overseas, unless adequate safeguards are met.

3. Kirklees Context

The Council maintains five 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 Council also maintains the register entries for its 69 Councillors who are Data Controllers in their own right in their capacity as Ward Councillors.

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 Access & Security Officer,
- two full-time and one part time Information Governance Officers
- one full-time and four 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 in order to collate information requested.

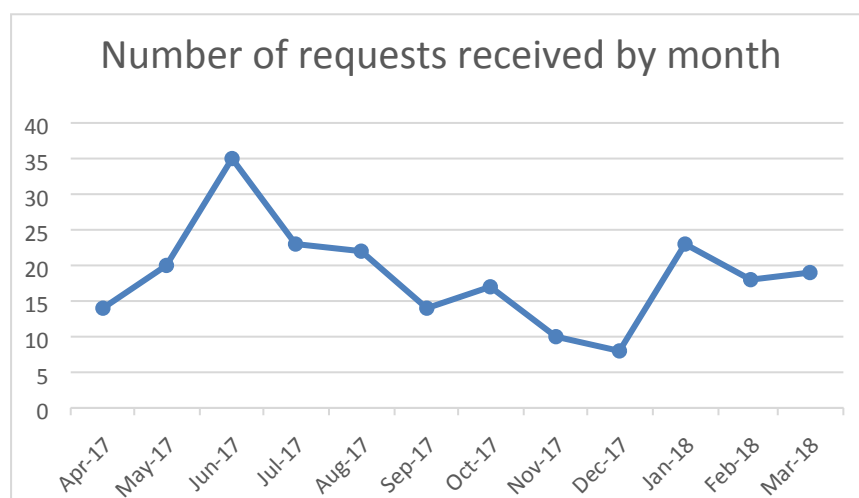
4. Statistics:

a) Numbers of Requests

The number of requests for access to personal information received between 1 April 2017 and 31 March 2018 has increased by 11% from figures reported last year, from 201 to 223, averaging at 18.5 requests per month compared to 17 per month in 2016-17.

Monthly	Number	Quarterly	Number
April 2017	14	Quarter 1	69
May 2017	20		
June 2017	35		
July 2017	23	Quarter 2	59
August 2017	22		
September 2017	14		
October 2017	17	Quarter 3	35
November 2017	10		
December 2017	8		
January 2018	23	Quarter 4	60
February 2018	18		
March 2018	19		
Total	223	Total	223

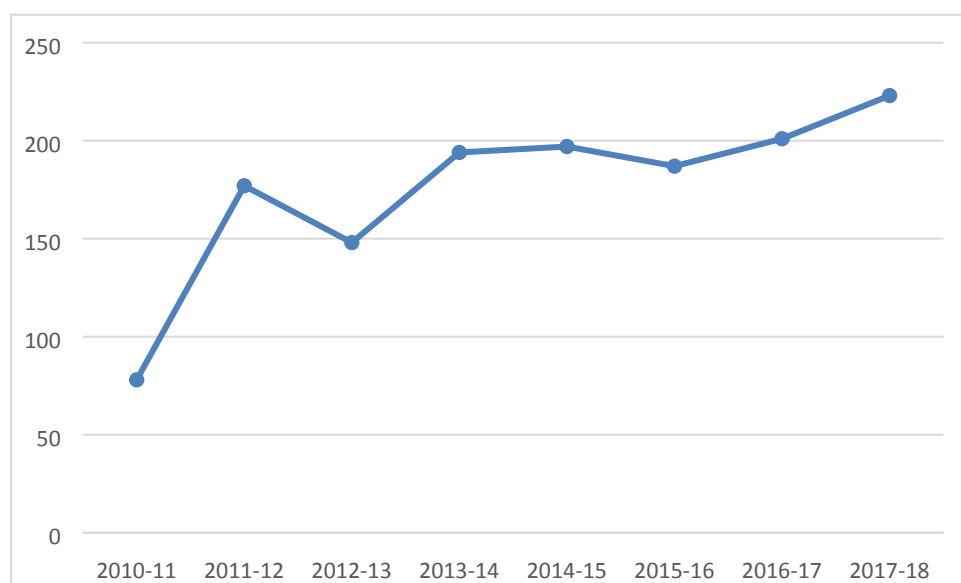
The following chart plots the figures from the above table:



Year on year figures are:

Quarters	2010-11	2011-12	2012-13	2013-14	2014-15	2015-16	2016-17	2017-18
Qtr 1	11	35	29	47	56	54	57	69
Qtr 2	17	32	43	49	51	36	40	59
Qtr 3	16	45	40	45	37	40	42	35
Qtr 4	34	65	36	53	53	57	62	60
Totals	78	177	148	194	197	187	201	223
% Change	n/a	+127%	-16%	+31%	+2%	-5%	+7.5%	+11%

The following chart plots the totals received annually from the above table:



b) Time Taken to Respond to Requests

The DPA98 requires data controllers to reply to requests for access to personal information within 40 calendar days. There is no scope in the Act for extending this.

Compliance with the 40 calendar day deadline is reported quarterly through PERFORM; targets and tolerances are:

Primary Ref No	PI Definition (Kirklees Action)	Target 2014-15	Tolerances					Factors influencing the setting of targets / tolerances
			R	RA	A	AG	G	
KI 366	% of Data Protection requests replied to within 40 calendar days	100%	79%	80%	85%	90%	100%	Legal compliance and the ICO's minimum expectation of performance is 90% No scope for extending deadline

In 2017-18 the Council responded to 83.5% of requests received within the deadline; this compares with 82% in 2016-17, showing a slight increase in compliance, but significant scope for improvement and the Council's compliance falls short of the ICO's minimum expectation of a 90% compliance rate.

Requests Received		Legal Deadline of 40 Calendar Days		Response Within 30 Calendar Days *	
Monthly	Number	Number	%	Number	%
April 2017	14	12	86%	11	79%
May 2017	20	16	80%	12	60%
June 2017	35	28	80%	28	80%
July 2017	23	21	91%	16	70%
August 2017	22	14	64%	9	41%
September 2017	14	13	93%	10	71%
October 2017	17	16	94%	13	76%
November 2017	10	9	90%	9	90%
December 2017	8	7	88%	5	63%
January 2018	23	17	74%	15	65%
February 2018	18	15	83%	16	89%
March 2018	19	15	79%	12	63%
Total	223	183	83%	156	71%

* The figures in the last 2 columns are shown only to identify the number of requests which were responded to within 30 days which is to become the legal deadline under GDPR

The average response time in 2017-18 was 23.3 days; this compares with 32.7 days in 2016-17, which shows an improvement in time taken to respond to requests.

c) Requests by Directorate

The total figure in this section is higher than the 223 total number of requests received because 12% of the 223 requests received (27) 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	2017-18	Percentage of Total Received
-------------	---------	------------------------------

Chief Executive's Office	1	0.4%
Adults (social care, public health, commissioning)	44	17.6%
Children Services (social care and learning)	110	44.0%
Communities, Transformation & Change	8	3.2%
Place	24	9.6%
Resources	57	22.8%
Council-wide	2	0.8%
KNH	3	1.2%
Not Council – Other Org	1	0.4%
Total	250	100.00%

d) Outcomes

Outcome	2017-18	Percentage of Total Requests Received
Supplied	109	48.9%
Refused (in whole or in part)	16	7.2%
Not Held	24	10.8%
Discontinued	73	32.7%
Outstanding / Suspended	1	0.4%
Total	223	100.00%

At the time of writing, the response to one request remains outstanding; the response is being chased.

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. [Part IV](#) of the DPA98 sets out the exemptions. [Section 8](#) of the DPA98 lists some of the circumstances in which a request need not be complied with.

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 main options (which the ICO may exclusively or any combination justified by the circumstances) are:

- *serve information notices requiring organisations to provide the Information Commissioner’s Office with specified information within a certain time period;*
- *issue undertakings committing an organisation to a particular course of action in order to improve its compliance;*
- *serve enforcement notices and ‘stop now’ orders where there has been a breach, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;*
- *conduct consensual assessments (audits) to check organisations are complying;*
- *serve assessment notices to conduct compulsory audits to assess whether organisations processing of personal data follows good practice;*
- *issue monetary penalty notices, requiring organisations to pay up to £500,000 for serious breaches of the Data Protection Act occurring on or after 6 April 2010*
- *prosecute those who commit criminal offences under the Act; and*
- *report to Parliament on issues of concern.*

Source: <https://ico.org.uk/about-the-ico/what-we-do/taking-action-data-protection/>

b) Complaints Received re Kirklees

The Information Commissioner’s Office made the Council aware of 4 complaints they had received about Kirklees in respect of data protection; this is a decrease on the previous year’s 6 complaints made to the ICO. The ICO considered it unlikely that the Council complied with the requirements of the DPA98 on one occasion only, and did not consider regulatory action was required in any case.

Summary	Outcome
Complaint about handling of an information security incident	The ICO considers it is likely that the Council has contravened the First Data Protection Principle in this case. Given the actions taken and to be taken, no further action required by ICO.
Complaint about handling of a subject access request	Response provided. No further action required by ICO.

Complaint that the Council has failed to provide a full response to a SAR within 40 days	ICO considers it is unlikely the Council has breach the DPA98. No further action required by ICO.
Complaint that the Council has failed to provide a complete response to a SAR	Further information disclosed to applicant. No further action required by ICO.

Appendix C – Fol and EIR Annual Report

**Freedom of Information Act 2000
and
Environmental Information Regulations 2004**

Annual Report 2016-17

Executive Summary

This report details how the Council has performed throughout 2017-18 in respect of information access requests received and processed under the Freedom of Information Act 2000 (Fol) and Environmental Information Regulations 2004 (EIR).

The Council received 1,513 requests during 2017-18 which is 122 less than the number received in 2016-17, which is a 7.5% decrease.

The Council's compliance rate for responding to requests has increased to 87% which is below the new expectation that 90% of responses should be sent out within deadline, although a significant improvement on the previous year's rate.

Compliance rates have fluctuated greatly over the 12 months, ranging from 73% in June 2017 up to 94.5% in January 2018.

The average response time for 2017-18 was, at the time of writing, 14.5 working days.

Regionally, from the West Yorkshire Councils which have submitted annual figures, there has mostly been a decrease in the volume of requests received, with Kirklees seeing the biggest decrease of 7.5%, two other Councils having had decreases of between 1.4% and 6% from the previous year. One Council has, however, reported a 10.6% increase in Fol/EIR requests.

The number of internal reviews carried out of the responses to requests has decreased significantly on the previous year, from 80 in 2016-17 to 29 in 2017-18. Two-thirds were dealt with within the timescale set out in the EIR and suggested by the ICO for Fol; 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 9, from 14 in 2016-17 to 5 in 2017-18. The ICO did not take any regulatory action against the Council in any of the cases they have made a decision on. Two ICO Decision Notices from 2016-17 was appealed to the First Tier Tribunal (Information Rights) in 2017-18; one was dismissed and the other was upheld.

Lindsay Foody
Information Access & Security Officer

23 August 2018

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 2016-17 in relation to requests made under the Freedom of Information Act 2000 (Fol 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 Fol 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 Data Protection Act 1998, which also exempts private information about other people.

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 Fol 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 Access & Security Officer,
- two full-time and one part time Information Governance Officers
- one full-time and four 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

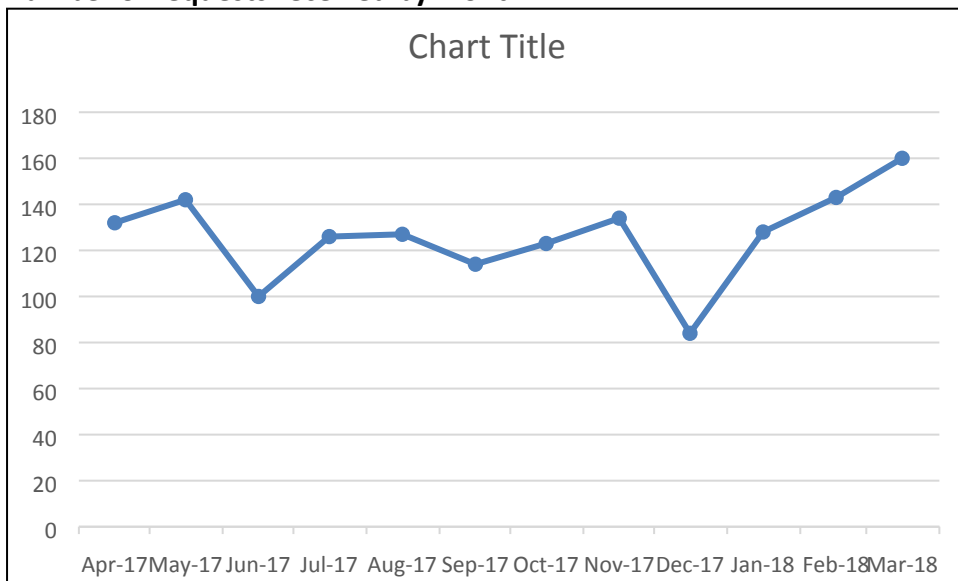
The number of Freedom of Information (FoI) and Environmental Information (EIR) requests received between 1 April 2017 and 31 March 2018 has decreased by 122 (7.5%) from the previous year; a decrease which averages at 126 requests per month compared to 136 per month in 2016-17:

Monthly	Number
April 2017	132
May 2017	142
June 2017	100
July 2017	126
August 2017	127
September 2017	114
October 2017	123
November 2017	134
December 2017	84
January 2018	128
February 2018	143
March 2018	160
Total	1,513

Quarterly	Number
Quarter 1	374
Quarter 2	367
Quarter 3	341
Quarter 4	431
Total	1,513

The following chart plots the figures from the above table:

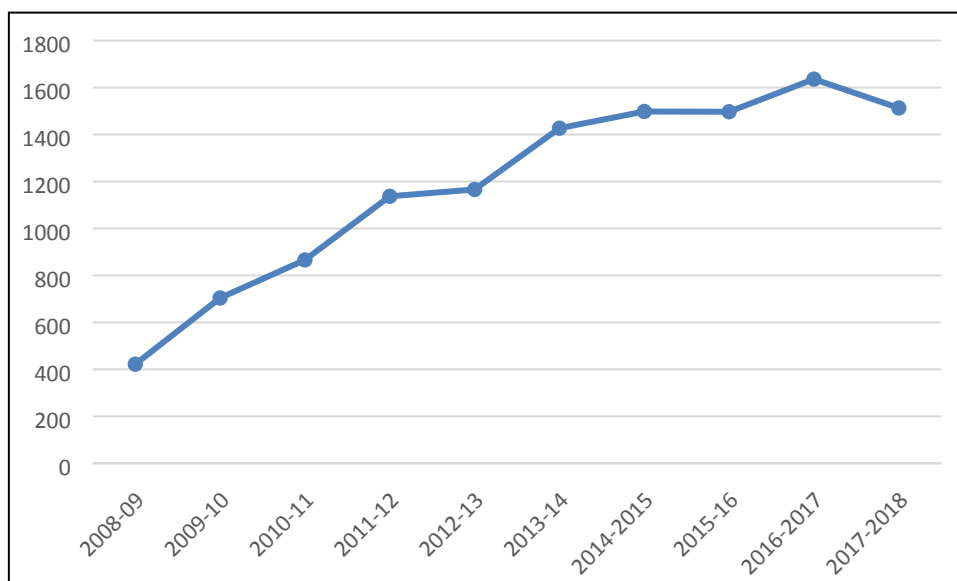
Number of requests received by month:



The decrease in volume is the first real dip in numbers over the past 10 years, although it plateaued in 2012-13 and again 2014-15 and 2015-16, before rising again in 2016-17:

Qtrs	2008-2009	2009-2010	2010-2011	2011-2012	2012-2013	2013-2014	2014-2015	2015-2016	2016-2017	2017-2018
Qtr 1	86	135	185	299	332	283	353	336	417	374
Qtr 2	106	182	180	263	273	356	357	350	398	367
Qtr 3	97	193	197	248	218	384	352	361	397	341
Qtr 4	133	194	305	327	343	404	436	450	424	431
Totals	422	704	866	1,137	1,166	1,427	1,498	1,497	1,636	1,513
<i>%Change</i>	<i>34%</i>	<i>40%</i>	<i>19%</i>	<i>24%</i>	<i>2%</i>	<i>18%</i>	<i>5%</i>	<i>0%</i>	<i>8%</i>	<i>-7.5%</i>

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	307	20.3%
Clubs, Societies & Charities	77	5.1%
Individuals	172	11.4%
Media	250	16.5%
Other	491	32.5%
Pressure Group (Local & National)	150	9.9%
Research & Academic	66	4.4%
Totals	1,513	100.00%

Source of Request - Comparison	2016-17	2017-18	Difference
Business	291	307	+16
Clubs & Societies	62	77	+15
Individuals	195	172	-23
Media	243	250	+7
Other	613	491	-22
Pressure Group (Local & National)	168	150	-18
Research & Academic	64	66	+2
Totals	1,636	1,513	-23

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 (2,037) is higher than the total number of requests received (1,513) because 524 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	2017-18	% of Total Requests Received
Children's Social Care & Learning	258	12.7%
Adults' Social Care	109	5.4%
Commissioning & Health Partnerships	31	1.5%
Council-wide	13	0.6%
Communities, Transformation & Change	135	6.6%
Chief Executive's Office	11	0.5%
KNH	89	4.4%
Place	722	35.4%
Public Health	48	2.4%
Resources	607	29.8%
Not Council – Other Organisation	14	0.7%
Total	2,037	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 2017-18 1,317 (87%) requests were responded to within 20 working days. This is under the threshold that triggers the Information Commissioner's Office's (ICO) monitoring of public authorities when responding to freedom of information requests which, as of March 2017, is 90%, and is an improvement in performance on 2016-17 (81%).

Compliance with the 20 working day deadline is reported quarterly through PERFORM; targets and tolerances are:

Primary Ref No	PI Definition (Kirklees Action)	Target 2016-17	Tolerances					Factors influencing the setting of targets / tolerances
			R	RA	A	AG	G	
KI 363	% of Fol and EIR requests responded to in 20 working days	100%	74%	75%	80%	85%	100%	Legal compliance is 100% and the ICO's minimum expectation of performance is 85%

Overall, 96% of requests received a response within 30 working days or less, and although there is nothing within the legislation relating to this timescale, it does demonstrate that where deadlines are being missed, the majority are responded to fairly quickly afterwards, with 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 30 Working Days	
Monthly	Number	Number	%	Number	%
April 2017	132	118	89.39%	127	96.21%
May 2017	142	121	85.21%	131	92.25%
June 2017	100	73	73.00%	92	92.00%
July 2017	126	114	90.48%	123	97.62%
August 2017	127	106	83.46%	120	94.49%
September 2017	114	96	84.21%	109	95.61%
October 2017	123	113	91.87%	118	95.93%
November 2017	134	117	87.31%	130	97.01%
December 2017	84	77	91.67%	82	97.62%
January 2018	128	121	94.53%	126	98.44%
February 2018	143	117	81.82%	140	97.90%
March 2018	160	144	90.00%	155	96.88%
Total	1,513	1,317	Av: 86.91%	1453	Av: 96.00%

The Council met or exceeded the ICO's expected compliance rate in 5 months of the year, which is a significant improvement in performance from the previous year when it achieved this in 2 of the 12 months.

KATY – SOMEONE ELSE PROVIDES THIS INFORMATION – OR DOES IT NEED TO COME OUT???

The Council estimates the average cost of responding to Fol requests is £267.08 per request. This results in an estimated cost of responding to FOI requests at £436,946.96.

e) Outcomes

The Fol Act and the EIRs have a limited number of circumstances under which requested information can be withheld. Under the Fol Act these are called 'exemptions' and under EIR these are called 'exceptions'. There are 8 'absolute' Fol 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 1,513 requests received during 2017-18, 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 it does not hold, for example, trading standards or crime information, which is held by other organisations and not the Council; requests may also be 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)	972	64.2%
Refused (all or in part)	400	26.4%
Not Held (and referred)	80	5.3%
Discontinued (and duplicate)	60	4.0%
Neither Confirm Nor Deny	1	0.1%
Total	1513	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 2016-17 607 exemptions / exceptions were applied (in whole or in part) to 479 requests (this number includes the 3 requests for which information was not held for the purpose of the FoI Act was requested and are recorded as 'Not Held' in the table above as well as the 3 cases which are recorded as 'Neither Confirm Nor Deny'):

FoI Exemptions / EIR Exceptions Applied			2017-18	% Total Requests Refused
EIR	reg12(4)(b)	Manifestly unreasonable	7	1.5%
EIR	reg12(4)(d)	Relates to unfinished documents or incomplete data	2	0.4%
EIR	reg12(4)(e)	Would involve disclosure of internal communications	0	0.0%
EIR	reg12(5)(b)	The course of justice, fair trial, conduct of a criminal or disciplinary inquiry	1	0.2%

EIR	reg12(5)(d)	Confidentiality of public authority proceedings when covered by law	1	0.2%
EIR	reg12(5)(e)	Confidentiality of commercial or industrial information when protected by law to cover legitimate economic interest	5	1.1%
EIR	reg12(5)(f)	Confidentiality of commercial or industrial information when protected by law to cover legitimate economic interest	5	1.1%
EIR	reg13	Personal data	38	8.4%
FoI	s12	cost of compliance exceeds appropriate limit	61	13.5%
FoI	S14	Repeated or vexatious request	5	1.1%
FoI	s21	Information reasonably accessible by other means	152	33.6%
FoI	s22	Information intended for future publication	0	0.0%
FoI	s24	National security	5	1.1%
FoI	s3(2)(a)	Not held for the purposes of the FoI Act	1	0.2%
FoI	S30	Investigations and proceedings conducted by public authorities	0	0.0%
FoI	s31	Law enforcement	30	6.6%
FoI	S36	Prejudice to the effective conduct of public affairs	0	0.0%
FoI	s38	Health and safety	0	0.0%
FoI	s40	Personal information	105	23.2%
FoI	s41	Information provided in confidence	9	2.0%
FoI	s42	Legal professional privilege	2	0.4%
FoI	s43	Commercial interests	23	5.1%
FoI	s44	Prohibitions on disclosure	0	0.0%
Total			452	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 working days from receipt of the request. The EIRs require internal reviews to be completed within 40 working days of receipt of the request.

In 2017-18 the Council carried out 29 internal reviews, compared with 80 in 2016-17.

The Council notes that in 2016-17 40% of all internal reviews requested (32) were made by two applicants, who each submitted multiple requests throughout the year (71, which was 4.34%

of all requests received) which accounted for the unusually high number of internal reviews requested during 2016-17:

The internal reviews carried out in 2017-18

Monthly	Number received	Responded to within Deadline	% in deadline	Average Time to respond (working days)
April 2017	1	0	0.0%	24
May 2017	2	2	100.0%	19
June 2017	1	0	0.0%	24
July 2017	2	2	100.0%	24
August 2017	3	1	33.3%	30
September 2017	1	1	100.0%	19
October 2017	5	4	80.0%	22
November 2017	4	4	100.0%	15
December 2017	2	2	100.0%	12
January 2018	2	2	100.0%	16
February 2018	2	1	50.0%	38
March 2018	4	2	50.0%	38
Total	29	21	Av: 67.8%	Av: 23.38

At the time of writing, 3 internal review decisions remain outstanding and are overdue.

Internal Review Outcome	2017-18	% of Total Requests Received
Not Upheld	17	58.6%
Partially Upheld	4	13.8%
Upheld	7	24.1%
Open (and overdue)	1	3.4%
Total	29	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 Freedom of Information Act, Environmental Information Regulations, INSPIRE Regulations and associated codes of practice. They include non-criminal enforcement and assessments of good practice.

Specifically, where authorities repeatedly or seriously fail to meet the requirements of the legislation, or conform to the associated codes of practice, the ICO can take the following action:

- *conduct assessments to check organisations are complying with the Act;*
- *serve information notices requiring organisations to provide the ICO with specified information within a certain time period;*
- *issue undertakings committing an authority to a particular course of action to improve its compliance;*
- *serve enforcement notices where there has been a breach of the Act, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;*
- *issue practice recommendations specifying steps the public authority should take to ensure conformity to the codes;*
- *issue decision notices detailing the outcome of the ICO’s investigation to publically highlight particular issues with an authority’s handling of a specific request;*
- *prosecute those who commit criminal offences under the Act; and*
- *report to Parliament on freedom of information issues of concern.*

Source: <https://ico.org.uk/about-the-ico/what-we-do/taking-action-freedom-of-information-and-environmental-information/>

b) Complaints Received about Kirklees

The ICO made the Council aware of 5 complaints they had received about Kirklees’ handling of Fol and EIR requests, a decrease of 9 from the 14 notified in 2016-17:

Summary	Outcome
Complaint about handling of an EIR request	Local resolution; additional information provided to applicant by agreement with the ICO and the applicant. No further action required by ICO.
Complaint that the Council has failed to provide a full response to an EIR within 20 workings days	ICO notes response not sent within deadline and requires response to be sent within 10 working days or receipt of letter; response sent in 10 days. No further action required by ICO.
Complaint about a late response to an Fol request	ICO notes a response was not sent within deadline but that the response has since been sent with an apology. No further action required by ICO.

Complaint about s40 redaction of personal information and a late response to an FoI request	ICO issued a decision notice upholding the complaint that a response was not sent within deadline, but not upholding the complaint about the application of s40(2) (personal information). See Decision Notice FS50703907 below
Complaint about a late response to an FoI request	ICO notes a response was not sent within deadline but that the response has since been sent with an apology. No further action required by ICO. The ICO acknowledges that a clerical error lay behind this failure, nevertheless she is obliged to find that the Council has breached section 10 of the Act.

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 one of the four complaints made about Kirklees in 2017-18:

Kirklees Metropolitan Council
11 Jun 2018, Local government

The complainant has requested information from Kirklees Council which concerns remarks made by a councillor at a public meeting, where the Councillor is alleged to have said that the complainant had cost the Council £38,000. The Council corrected the amount referred to by the complainant in his request and it provided him with a schedule of its calculation of how a figure of £11,000 was arrived at. The Council made some redactions from the schedule disclosed to the complainant by virtue of its application of section 40(2) of the FOIA. The Commissioner's decision is that Kirklees Council has correctly applied the provisions of section 40(2) to information it withheld from the complainant. The Commissioner has also decided that the Council has breached section 10 of the FOIA for failing to respond to the complainant's request within the required twenty working day compliance period.

FOI 10: Complaint upheld FOI 40(2): Complaint not upheld

[View a PDF of Decision notice FS50703907](#)

<https://search.ico.org.uk/ico/search/decisionnotice>

d) Tribunals

Two appeals to the First Tier Tribunal (Information Rights) were lodged during 2017-18:

One in respect of ICO Decision Notice [FS50660772](#) issued in September 2017. The appeal was subsequently dismissed. FTT Case EA/2017/0231 refers.

One in respect of ICO Decision Notice [FS50667566](#) issued in August 2017. The FTT upheld the appeal and requires the Council to provide a reply to the applicant's request, so far as it applies to the information in question, in accordance with the FTT finding that the Council holds this information. FTT Case EA/2017/0194 refers.

Appendix D – Local Government Transparency Code

Local Government Transparency Code

Progress Report

August 2018

Anna Bowtell





























Research & Intelligence Manager

SUMMARY

In 2015 & 2016, Kirklees Council published data & information, where available, to try to meet the requirements of the Local Government Transparency Code. Despite a recent consultation, the Transparency Code has not been updated since 2015 so we have been working with the same requirements as stipulated in the 2015 publication. The code has two elements; information which *must* be published and information that is *recommended* for publication. Between 2016 & 2018, there has been additional local emphasis on requesting data that meets the *recommended* element of the code. This is in preparation for an anticipated request for all authorities to meet the recommended criteria in the near future.













The published data can be found here:

<http://www.kirklees.gov.uk/beta/information-and-data/open-data-sets.aspx>

	2015		2016		2017		2018 – in progress	
	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		2 identifiers are not published: - Summary of purpose - Unrecoverable VAT		2 identifiers are not published: - Summary of purpose - Unrecoverable VAT		NOTE: expenditure data is currently under review and will be republished shortly	
Government Procurement Card Transactions								
	3 categories are not published: - VAT - Summary of purpose - Merchant Category		3 categories are not published: - VAT - Summary of purpose - Merchant Category		3 categories are not published: - VAT - Summary of purpose - Merchant Category		NOTE: expenditure data is currently under review and will be republished shortly	
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.							
	2015	2015	2016	2016	2017	2017	2018	2018
	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								
	2 definite categories are not published:		1 definite category is not published:		1 definite category is not published:		1 definite category is not published:	

	<ul style="list-style-type: none"> - Freehold or leasehold - Land or building asset <p>Queries about data accuracy & whether all assets stipulated are included in the list.</p>		<ul style="list-style-type: none"> - Land or building asset <p>Recommended involves more regular publication, publishing to the Electronic Property Information Mapping Service & more in-depth categories e.g. hectares/reasons.</p>		<ul style="list-style-type: none"> - Land or building asset <p>The Electronic Property Information Mapping Service [EPims] is currently being trialled by the service. The type of date upload and frequency is being considered.</p>		<ul style="list-style-type: none"> - Land or building asset <p>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.</p>	
Grants to voluntary, community & social enterprises and organisations								
	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								
	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.							
	2015		2016		2017		2018	
	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	DATA NOT COLLECTED & NOT RECEIVED			N/A		N/A
	There are no "Recommended" Requirements							
Parking Account								

		N/A		N/A		N/A		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.								
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		N/A
Only top 3 tiers were reported on. Job descriptions posted are out of date. There are no 'Recommended' requirements.			Salaries over £50,000 have been published. Job Descriptions & 'responsibilities' [including budget/services/ functions] requires work – currently with HR to gather JDs for publication.		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.	
	2015		2016		2017		2018	
	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		N/A
Direct feed to web link – if content changes, link will update.								
Pay Multiple		N/A		N/A		N/A		N/A

	No comment to add							
Fraud								
	Data received from service does not include the total £'s spent on investigation & fraud – 20% of the basic requirements for the code. Service is struggling with IT systems & change in officer ownership of the fraud section.				Data now includes spend on investigation & fraud.			
Social Housing Asset Value		N/A		N/A		N/A		N/A
	No comment to add		No comment to add		Data routinely published in the month of September		Data routinely published in the month of September	
Waste Contract	Not applicable for Kirklees.							

Anna Bowtell
Research & Intelligence Manager
Kirklees Intelligence & Performance Unit