Audit and Standards Committee Report

Report of:	**Director of Business Change and Information Solutions**
Date:	**June 11th 2019**
Subject:	**Information Governance Annual Report**
Author of Report:	**Mark Gannon** **Director of Business Change and Information Solutions,** **Senior Information Risk Owner**

Summary:

Information Governance is the generic term used to describe how an organisation manages its information, particularly in respect to legislative and regulatory requirements. This report seeks to provide assurance around the policies, processes and practices employed to ensure we meet those requirements.

Recommendations: to note the annual information governance update

Background Papers: None

Category of Report: OPEN

Statutory and Council Policy Checklist

Financial Implications
NO:
Legal Implications
YES
Equality of Opportunity Implications
NO
Tackling Health Inequalities Implications
NO
Human rights Implications
NO:
Environmental and Sustainability implications
NO
Economic impact
NO
Community safety implications
NO
Human resources implications
NO
Property implications
NO
Area(s) affected
None
Relevant Cabinet Portfolio Member
Olivia Blake
Is the item a matter which is reserved for approval by the City Council?
NO
Press release
NO

REPORT TITLE: Information Governance Annual Report for 2018/19

1.0	**INTRODUCTION**
1.1	This report has been written to provide an overview of the Information Governance arrangements and performance at the Council for the last financial year and to provide assurance around the policies, processes and practices employed to ensure we meet our legal requirements.
2.0	**BACKGROUND**
2.1	Information Governance is a common term for the distinct, but overlapping disciplines of data protection, access to information, information security, investigatory powers, information and records management, information sharing, information quality and information assurance.
2.2	The ultimate purpose of Information Governance is to help an organisation to understand its information needs and responsibilities, to define the rules for the management of information flowing in, out and around the business, to maximise the value of information while minimising the risks.
2.3	Effective Information Governance enables the Council to understand and comply with its legal and administrative obligations, manage and reduce risks, protect privacy and confidentiality, and support services to deliver the best services possible to the right people at the right time.
2.4	The Information Governance landscape is complex and subject to laws and regulations and recommended codes of practice. The key laws include the General Data Protection Regulations 2016 (GDPR), Data Protection Act 2018 (DPA), Freedom of Information Act 2000 (FOIA), Environmental Information Regulations 2004 (EIR), and Regulation of Investigatory Powers 2000 (RIPA). The Council can be called upon to demonstrate its compliance with these laws and regulations by members of the public, partner agencies, accrediting bodies, and Regulators such as the Information Commissioner, the Surveillance Camera Commissioner and the Investigatory Powers Commissioner. These Commissioners have powers to impose penalties, including monetary penalties and custodial sentences on organisations or individuals who breach the laws and regulations.
2.5	To enable the Council to understand and shape the Information Governance activity across the Council and ensure compliance, it has nominated specific information governance roles to officers: Senior Information Risk Owner, Portfolio Information Risk Owners, Caldicott Guardians, Senior Responsible Officer (RIPA) and the Data Protection Officer. These roles attend the Information Governance Board, which is subsequently supported by key officers and working groups to help embed information governance practice.

3.0	**DATA PROTECTION LAWS**
3.1	On May 25th 2018, the General Data Protection Regulations 2016 and the Data Protection Act 2018 came into force. The new laws intended to modernise data protection practice in the digital age and introduced some key changes: 1. Making Data Controllers more accountable for the personal data they process and requiring them to demonstrate compliance with the laws; 2. Giving data subjects greater rights to better control how their personal data is being processed; 3. Providing the Information Commissioner greater enforcement powers including the power to issues fines up to €20 million or 4% of annual turnover for non-compliance with the law.
3.2	Throughout 2018/19, the Council has worked to review and develop its data protection practice and included: 1. **Discovery:** to identify the business activities that process personal data and to gather information to determine if the processing complies with data protection law. The scope of the discovery focused primarily on the activities processing large amounts of personal data or where the processing was considered to be high risk (e.g. confidentiality) to create the Council's Record of Processing Activity, but has extended to review where the data is held, particularly the ICT systems and security arrangements. 2. **Awareness:** to raise awareness among staff of the legal changes and the need to always comply with the data protection principles to ensure personal data is processed fairly, lawfully and transparently; used for specific purposes; processed using the minimum necessary; accurate; processed only for as long as necessary; protected from loss or unauthorised or unlawful processing. This has been carried out in a number of ways including through data protection drop in sessions and training workshops; briefings, newsletters and updates; e-learning and supporting literature. 3. **Implementation**: to review current arrangements and take the necessary actions to help embed good data protection practice into business as usual, for instance writing and publishing policies and procedures, privacy notices, information sharing agreements, data processing agreements and data protection impact assessments; handling data subject requests (right to know, right of access, right to be forgotten); logging and investigating information security incidents.

3.3	Data protection compliance remains a key priority for the Council and is currently logged on the Council's Risk Register (Resources Risk ID 352 – High). Work will continue throughout 2019/20 to ensure good practice is understood and embedded into business as usual and that the right evidence is available as and when required to reduce the risk to an acceptable level.
4.0	**SUBJECT ACCESS REQUESTS**
4.1	Data protection law provides data subjects with a number of rights to better understand and make decisions about the personal data a Data Controller processes about them (articles 14-22). The most commonly used right is article 15, the right of access, which is known as a Subject Access Request (SAR).
4.2	All SARs are logged by the Council's Information Management team, triaged and allocated to individual services to respond to.
4.3	SARs have to be answered within a legal time limit and the Council's Information Governance Board has set the target that 85% of SARs should be answered in time. The Council has not yet managed to reach this target and in 2013 logged the handling of SARs as a risk on the Corporate Risk Register and reported to EMT because it breaches the law, but also impacts the customer and can result in the Information Commissioner's intervention (Resources Risk ID 196).
4.4	In 2018/19, the Council handled 294 subject access requests and answered in 74% in time (see Appendix A). This is a significant achievement because in 2017/18, the figures were196 requests and only 49% answered in time, the lowest performance since the records started in 2014/15. This meant 2018/19 started having to handle the outstanding requests as well as the new requests which had increased in number by 33%. The biggest increase of request was for historic social care children's information, which are often complex and time-consuming because the information can span many years and include very sensitive material about the data subject and third parties that needs to be read and redacted before disclosure. In June 2018, the Information Commissioner's Office (ICO) contacted the Council because they had had a couple of complaints about the Council's handling of their requests. The ICO asked for monthly updates, including information about our late requests and the actions we intended to take to improve. The updates concluded in January 2019 when the ICO confirmed it was satisfied with the Council's approach and progress. Since June 2018, procedures and processes have been updated, services and portfolios have worked better together, senior managements has committed more resources, staff have become more confident in their disclosure decision making, which have resulted in performance improving every quarter.

4.5	In addition to the above, the ICO has corresponded with the Council on 8 separate occasions concerning subject access requests: 3 cases related to personal data disclosed incorrectly through a SAR response, but were closed with no ICO action; 5 cases related to late SAR responses, of which 4 were upheld and handled accordingly.
4.6	The handling of SARs remains a priority for 2019/20 and current performance suggests the Information Governance Board's target of 85% can and will be met and the Issue likely to be closed.
5.0	**FREEDOM OF INFORMATION (FOI) AND ENVIRONMENTAL INFORMATION (EIR) REQUESTS**
5.1	The Council is legally required to respond to requests for information under the Freedom of Information Act 2000 (FOIA) and the Environmental Information Regulations 2004 (EIR). Responses must be within 20 working days and confirm if the information is held and provide the information or the reasons why it cannot be disclosed (exemptions).
5.2	FOIs and EIR requests are logged by the Council's Information Management team, triaged and allocated to individual services to gather the information. Services provide a response to the IM team to check and then respond to the customer.
5.3	In 2018/19, the Council received 2284 requests and answered 97% in time (appendix B). This exceeds the Council's Information Governance Board target of responding to 95% of requests in time. The IM team also monitor the late requests (74) to identify and address any issues that may present a risk to performance.
5.4	The FOI and EIR provider requesters to the appeal about the way their request has been handled (aka Internal Review). The Council handled 81 Internal Reviews in 2018/19 of which the majority were resolved: either the Council changed its position and released information or upheld the original decision and was accepted by the requester.
5.5	Of the 81 Internal Reviews, 15 cases were reported by the requester to the Information Commissioner's Office to investigate further. Of these 15 cases, the Council resolved 4 informally with the customer; the ICO upheld 7 cases in favour of the Council and partially upheld the remaining 4.
5.6	In spite of the successful handling of the requests, internal reviews and ICO enquiries, the Council recognises that the double and sometimes triple handling of requests can be time-consuming and will look to reduce the number of internal reviews and ICO enquiries over the course of 2019/20.

6.0	**OPEN DATA**
6.1	The Council is committed to open data to support the Council's transparency agenda and routinely publishes information about its services, key decisions and expenditure.
6.2	The Council had a dedicated open data platform called Socrata and published approximately 30 datasets to help comply with the Freedom of Information Act 2000, Protection of Freedoms Act 2012, and the Local Transparency Code 2015. The Socrata contract expired in March 31st 2018, so the Council started to use ESRI as the alternative.
6.3	To date approximately 20 datasets have been published onto ESRI site. During the move away from Socrata, it was apparent governance was needed to clarify what data should be published and why and ensure it is accurate, meaningful, owned and regularly updated. This was recognised as an information governance risk and logged as such on the Corporate Risk Register (Resources Risk ID 366 - Moderate). As a result, further work has been carried out an action plan put in place to relaunch the need and use of open data to help demonstrate the Council's commitments to openness, transparency and public accountability.
7.0	**INFORMATION SECURITY INCIDENTS AND PERSONAL DATA BREACHES**
7.1	The Council is required to log, assess and mitigate information security risks, incidents and breaches. Incidents can be events that have happened or are near misses that affect or are likely to affect the confidentiality, integrity and availability of information. Where an incident occurs and affects personal data, this is a personal data breach. Data protection law requires organisations to notify the Information Commissioner's Office of the personal data breaches that have a high and ongoing risk to the data subjects affected.
7.2	In 2018/19, 248 incidents were logged through the Council's information security incident process; 116 of these incidents were classed as personal data breaches. The majority of the breaches involved customer personal data and were caused by human error with information being lost or stolen or emails or post being delivered to the wrong person. Of these breaches, 7 were considered to meet the serious threshold and were reported to the Information Commissioner's Office.
7.3	The Information Commissioner has the power to take enforcement action against an organisation for non-compliance to data protection, which includes data breaches, but data subjects can also make a separate claim to compensate against damage and distress. The Council has paid approximately £60k in such claims in the last few years.
7.4	Incidents and data breaches have been reported by all Portfolios. The Services that handle sensitive personal data are at greater risk because an incident or

	breach is more likely to have a greater impact on the customer or data subject and meet the threshold to notify the Information Commissioner.
7.5	There is therefore a continuing and critical need to manage the information we have, safely and securely, to continue to implement sound data protection practice, and ensure all staff are aware of their responsibilities and have received and completed all the necessary training relevant to their role
8.0	**INVESTIGATORY POWERS COMMISSIONER**
8.1	The Council is entitled to use the Regulation of Investigatory Powers Act 2000 (RIPA) and Investigatory Powers Act 2016 to carry out covert surveillance as part of its statutory duties. All applications must be approved by a Magistrate before covert surveillance can be carried out.
8.2	The Council must fully document all the applications it makes for covert surveillance including the use of Covert Human Intelligence Sources and make the documents available for inspection when required. The Council makes an annual return to the Investigatory Powers Commissioner's Office, which confirms the number of applications that have been considered and submitted to a Magistrate (see appendix D).
8.3	In 2018, the Council made 4 applications for Directed Surveillance that were all granted by the Magistrate and have since been cancelled; the term cancelled meaning the period of time authorised to carry out the surveillance has expired.
8.4	The Investigatory Powers Commissioner has the power to inspect an organisation to ensure its covert surveillance process and documentation is in place and compliant with the law. The Council was inspected on January 9th 2017 and usually occur every 3 years, so an inspection in the next 12 months is likely.
8.5	The Council continues to review its covert surveillance governance arrangements and has during 2018/19: updated its Intranet content, produced staff guidance about RIPA, and launched an e-learning module, with specific emphasis of staff using social media to look up customers or other third parties for information or monitoring purposes.
9.0	**INFORMATION GOVERNANCE RISK AND ISSUES**
9.1	In 2018/19, the Council logged 34 Information Governance Risks and 4 Issues on its Risk Register. These varied in severity – High to Low – covering the themes: Legal Compliance (data protection) and Loss of Data; Data Retention and Records Management; Loss of Systems and Applications; Cyber Security and Systems Vulnerability; Information Security and Data Quality.
9.2	The risks are reported to the relevant senior managers every quarter – Senior

	Management Teams or the Executive Management Team – to ensure the risks are being progressed or to highlight any issues that affect the treatment plan. The Information Governance Risks are also reported to the Information Governance Board with an accompanying report to confirm the status of the risk and issue including the impact of the treatment and residual risk (see appendix E)
9.3	The recent reports have identified the need to revisit the current information governance risks to group or rationalise the risks of a similar nature, so that the mitigations can be planned and implemented to the benefit the eider risk rather than a single service risk. This is likely to result in fewer risks being recorded on the risk Register, but give rise to a series of sub-risks with specific action and treatment plan to make it more clear the risk has been mitigated to an acceptable level, for instance with the Cyber Security and Data Protection risks.
10.0	**INFORMATION SECURITY & CYBER SECURITY**
10.1	Information security is about the protection of information or more specifically its confidentiality, integrity or availability. The Council is required to take appropriate security measures to protect information, particularly personal data, from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to information transmitted, stored or otherwise processed.
10.2	Information security has been embedded into Council practice for at least a decade and is applied as routine business. Governance is in place and policies and practices reviewed on a regular basis. The Council has previously been accredited to the Government's Public Services Network, which requires a minimum level of security controls to be in place, but the Council is not currently accredited. The Council has a number of low-risks that it needs to mitigate to fully comply with the PSN requirements. These risks are expected to be resolved when the Council moves to its new IT providers, but the delay leaving the Capita contract has subsequently delayed the re-submission for PSN accreditation. This is expected to be resolved during 2019/20.
10.3	Throughout the year, the Council has prepared for the change in IT provision and reviewed the IT assets it has and uses as well as the business processes and procedures that will need to be in place post-Capita. This has enabled the Council to better understand its IT and the information security risks. This work has helped the Council to successfully complete the NHS Data Protection and Security Toolkit, which allows the Council to continue to receive NHS data for its public intelligence work.
10.4	Cyber Security is a sub-set of Information Security and focuses on the protection of ICT systems and their components (i.e. hardware, software, data and infrastructure). The Council logged Cyber Security as a corporate risk in 2016 following Government advice that cyber security was a national threat (Resources Risk ID 290 – High).

10.5	The Council has, like other public authorities, experienced cyberattacks during 2018/19 e.g. phishing emails, Distributed Denial of Service, all of which have been managed with minimal disruption to the Council; the DDOS affected access to the Council's website for approximately 1 working day.
10.6	The Council is committed to improving its Cyber Resilience to better understand the threat landscape and take the necessary precautions to prevent or minimise cyber threats and took part in the Local Government Association (LGA) Cyber Resilience Stocktake in August 2018. The Stocktake analysis rated the Council as Amber-Amber, on par with many other local authorities, and identified areas of good practice and areas for improvement. The LGA subsequently invited local authorities to bid for money to help address some of the improvement areas. The Council applied for funding to pay for specialist Information Security training and was awarded £10,000.
10.7	In addition to the LGA Stocktake, the Council's Internal Audit carried out a review of the Council's Cyber Security arrangements and made a number of recommendations to improve governance (policies, security models and framework), training and awareness.
10.8	For 2019/20, the Council intend to complete the Internal Audit Report recommendations and has committed officers to attend the Cyber Resilience Pathfinder sessions being run by the Ministry of Housing, Communities and Local Government, and will apply for the external certificates for Cyber Essentials and Cyber Essentials Plus.
11.0	**RECORDS MANAGEMENT**
11.1	Records Management is the practice of managing records with the intention of ensuring they are accurate, reliable and available until they are disposed or permanently preserved. Effective records management can underpin business practice, support decision making and improve efficiencies, whereas ineffective records management can hinder operations and present a risk.
11.2	In 2018/19, records management was identified as an area for improvement and the inconsistent practice of keeping and destroying records was logged onto the Corporate Risk Register Record (Resource Risk ID 360 and 364). The Council subsequently reviewed and updated its retention schedule and invited services and officers to provide feedback with additions or alterations.
11.3	The Council also has a project to engage with Council services to help clarify the records management arrangements in place and any issues or obstacles and to identify the work and actions needed to improve and embed records management practice into the Council's culture. The Records Management project gathered evidence through discussions and workshops and presented the findings back to the stakeholders and to senior management.

11.4	The records management project's findings were well received and an action plan has been drafted to deliver the key actions throughout 2019/20, which includes: guidance, training and awareness, better use of information technology to automate records management processes, especially retention and disposal, better understanding of management responsibility to own the information processed within their service area. Moreover, the move away from Capita presents the Council with the unique opportunity to review and remove the electronic documents and records that it no longer needs.
12.0	**TRAINING**
12.1	Information governance is essential to ensure staff and other authorised users or processers of council information or systems understand and accept their responsibilities to handle information lawfully and safely. In the event of any complaint, incident or data breach, the Commissioner's ask for confirmation to what training provision is in place and whether the employee involved in the matter has completed the training available.
12.2	The Council has a range of information governance related training from the general awareness to bespoke sessions on key topics, for instance general training includes the Information Management e-learning, Cyber Security Videos, Regulation of Investigatory Powers e-learning, which hare available thought the Sheffield Development Hub. Bespoke training has also been available and delivered to officers needing greater knowledge in key governance areas, which has included data protection awareness sessions, data protection impact assessments, privacy notices, information sharing, etc.
12.3	The take up and completion of information governance training varies. For example, the Information Management e-learning module or its alternative, the Keep It Safe leaflet, are mandatory for all employees and authorised users using council information, but figures provided by HR in March 2019 confirmed only 56% of staff had completed the training. In contrast, attendance to taught courses has proven to be more popular, but reaching much smaller audiences per session.
12.4	The matter has been raised at the Information Governance Board and there will be a greater push for staff to be made aware of the training that is available and to increase the completion numbers. This will include reviewing and possibly changing the existing training methods to enable services to develop the relevant knowledge and skills to embed information governance in their working life and better protect the information they handle and ultimately our customers.

Appendix A: FOI and EIR Requests Response Performance 2018/19

2018/19				
Quarter	**Received**	**On Time**	**Late**	**Compliance Rate (%)**
Q1 - Apr-Jun	556	544	12	98
Q2 - Jul-Sep	547	529	18	97
Q3 - Oct-Dec	573	553	20	97
Q4 - Jan-Mar	608	584	24	96
Annual Totals	**2284**	**2210**	**74**	**97**

Appendix B-1: Subject Access Request Performance 2018/19

2018/19				
Quarter	**Received**	**On Time**	**Late**	**Compliance Rate (%)**
Q1 - Apr-Jun	68	37	31	54
Q2 - Jul-Sep	68	42	26	62
Q3 - Oct-Dec	68	56	12	82
Q4 - Jan-Mar	90	83	7	92
Annual Totals	**294**	**218**	**76**	**74**

Appendix B-2: Subject Access Request Performance 2018/19

Place Portfolio	Requests Received	Answered (In Time)	Answered (Late)	In Progress (In Time)	In Progress (Late)	Compliance (%)
CCTV	41	40	1	0	0	98
Env. Protection	6	6	0	0	0	100
Highways	1	1	0	0	0	100
Housing	66	61	5	0	0	92
Licensing	2	2	0	0	0	100
Parking	3	1	2	0	0	33
Total	**119**	**111**	**8**	**0**	**0**	**93**

People Portfolio	Requests Received	Answered (In Time)	Answered (Late)	In Progress (In Time)	In Progress (Late)	Compliance (%)
Adults Commissioning	3	2	1	0	0	67
Adults Social Care	10	7	3	0	0	70
Children's Social Care	98	50	48	0	0	51
Education / SEND	4	2	2	0	0	50
Social Care (Both)	3	2	1	0	0	67
Total	**118**	**63**	**55**	**0**	**0**	**53**

Resources Portfolio	Requests Received	Answered (In Time)	Answered (Late)	In Progress (In Time)	In Progress (Late)	Compliance (%)
BCIS	2	2	0	0	0	100
Customer Services	13	10	3	0	0	77
Human Resources	17	12	5	0	0	71
Revenue & Benefits	11	11	0	0	0	100
Total	**43**	**35**	**8**	**0**	**0**	**81**

Cross Portfolio	Requests Received	Answered (In Time)	Answered (Late)	In Progress (In Time)	In Progress (Late)	Compliance (%)
HR, Social Care, Housing	14	10	4	0	0	71
Total	14	10	4	0	0	71

Whole Council	Requests Received	Answered (In Time)	Answered (Late)	In Progress (In Time)	In Progress (Late)	Compliance (%)
Total	**294**	**219**	**75**	**0**	**0**	**74**

Appendix C: Reported Information Security Incidents and Personal Data Breaches

C-1 Monthly Figures

Information Security Incidents and Personal Data Breaches 2018/19					
Month	**Total**	**Incidents**	**Data Breaches**		**Data Breaches Reported to ICO**
Apr	**12**	2	10		1
May	**17**	15	2		0
Jun	**29**	20	9		0
Jul	**28**	23	5		0
Aug	**20**	11	9		2
Sep	**26**	13	13		1
Oct	**20**	7	13		0
Nov	**22**	12	10		0
Dec	**9**	6	3		0
Jan	**21**	11	10		0
Feb	**30**	8	22		2
Mar	**14**	8	6		1
Total	**248**	**136**	**112**		**7**

C2 – Category of Information Security Incidents

	Cyber Attack	Disclosed in Error	Lost in Transit	Lost or Stolen ICT	Lost or Stolen Papers	Non-secure disposal	Online Disclosure	Inappropriate Access (physical records)	Web Site	Total
Apr-Jun	0	28	3	0	1	0	0	1	0	33
Jul-Sep	2	34	5	0	4	0	1	1	0	47
Oct-Dec	3	19	1	1	0	0	0	1	0	25
Jan-Mar	2	17	2	1	3	1	0	0	1	27
	7	**98**	**11**	**2**	**8**	**1**	**1**	**3**	**1**	**132**

C3 – Category of Personal Data Breaches

	Disclosed in Error	Lost in Transit	Lost or Stolen Hardware	Lost or Stolen Paperwork	Online Disclosure	Totals
Apr-Jun	23	0	0	1	1	25
Jul-Sep	23	0	0	4	0	27
Oct-Dec	21	1	1	3	0	26
Jan-Mar	33	1	0	2	2	38
	100	**2**	**1**	**10**	**3**	**116**

C4 – Summary of personal data breaches investigated by the ICO

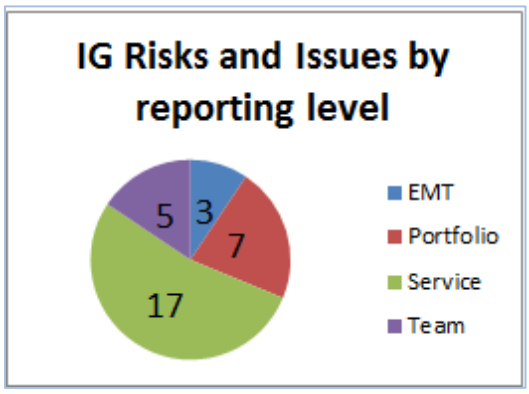
SCC Ref.	Case Opened	Summary of the personal data breaches investigated by the Information Commissioner's Office	INCIDENT TYPE
2017/156	26/04/2018	Data subject's sensitive personal data was disclosed in error to a third party. Reported to the ICO. ICO reviewed the case, but recommended staff are reminded of obligations to keep information safe and for the Council to ensure staff have completed relevant training.	Disclosed in Error
2017/293	10/08/2018	Disclosure made within a SAR. This was not a formal notification to the ICO, merely an email explaining a breach as the individual was going to complain to the ICO and we wanted to give them some background. The ICO did not respond, so case assumed to be closed.	Disclosed in Error
2017/299	17/08/2018	Personal data disclosed in error to third parties. The incident was investigated and reported to the ICO. The case was closed with no further actions.	Disclosed in Error
2017/306	13/09/2018	Personal data disclosed in error as part of a witness statement. The incident was investigated and reported to the ICO. The case was closed with no further actions.	Disclosed in Error
2018/413	08/02/2019	Data subject's personal data disclosed as part of a routine business action. The incident was investigated and reported to the ICO. The case was closed and although the ICO didn't take any formal action, recommended that procedures should be in place when handling sensitive information.	Disclosed in Error
2018/425	18/02/2019	The unredacted version of a document was sent to the third parties involved in a case, so too much information was disclosed. The incident was investigated and reported to the ICO. The case was closed with no further actions.	Disclosed in Error
2018/381	19/03/2019	The ICO contacted the Council because of a reported data breach. The Council had already logged the incident and confirmed that it was not a data breach because the data subject whose name had been disclosed was deceased. The Council had reviewed its practice and the ICO closed the case with no further action.	Disclosed in Error

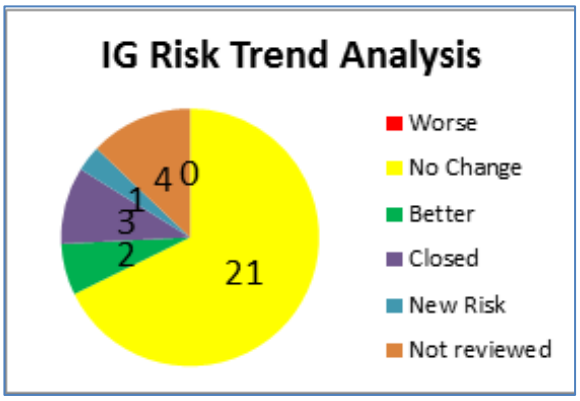
Appendix D: Investigatory Powers Commissioner Office Return

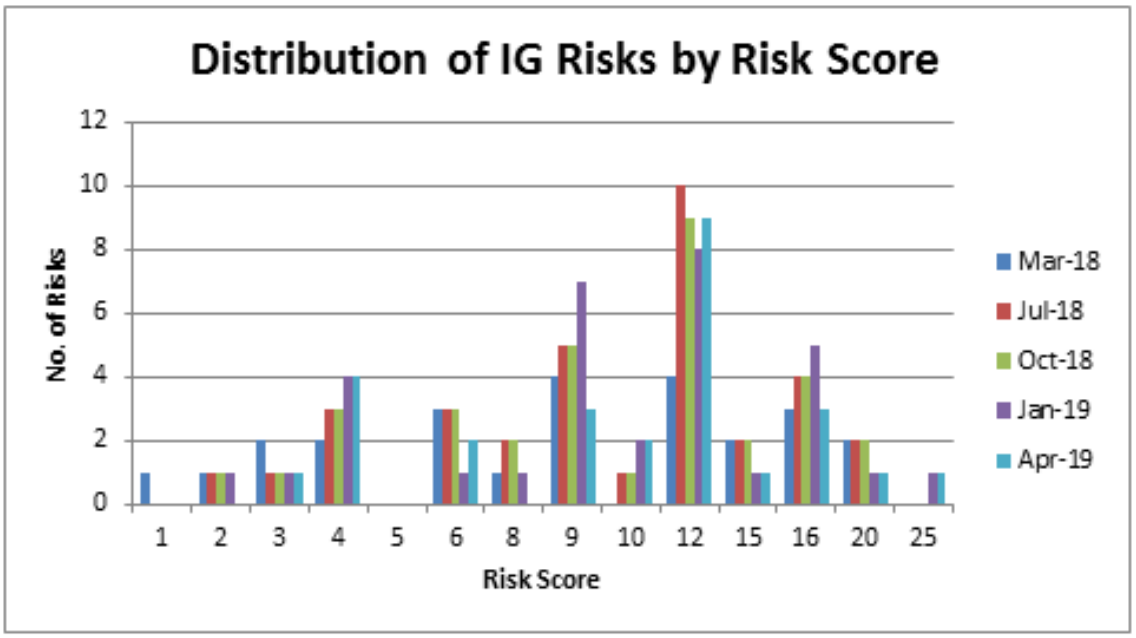
Sheffield City Council		Enter Stats below
Covert Human Intelligence Sources (CHIS) & Juvenile Covert Human Intelligence Sources (Juvenile CHIS)	The number of applications made for a CHIS authorisation?	0
	Of these, the number of applications made for a Juvenile CHIS authorisation?	0
	The number of CHIS authorisations successfully granted?	0
	Of these, the number of Juvenile CHIS authorisations successfully granted?	0
	The number of urgent applications made for a CHIS warrant?	0
	Of these, the number of urgent applications made for a Juvenile CHIS authorisations?	0
	The number of CHIS authorisations granted in an urgent case?	0
	Of these, the number of Juvenile CHIS authorisations granted in an urgent case?	0
	The number of CHIS authorisations that were renewed?	0
	The number of CHIS authorisations that were cancelled?	0
	The number of CHIS authorisations extant at the end of the year?	0
	The age of the Juvenile CHIS at the time of the authorisation's issue? (to be completed in rows below)	0
	Juvenile CHIS age at application	0
	Quantity	0
	Juvenile CHIS age at application	0
	Quantity	0
	Juvenile CHIS age at application	0
	Quantity	0
	Juvenile CHIS age at application	0
	Quantity	0
	Juvenile CHIS age at application	0
	Quantity	0
	Juvenile CHIS age at application	0
	Quantity	0
Directed Surveillance (RIPA & RIPSA)	The number of applications made for a Directed Surveillance authorisation?	4
	The number of Directed Surveillance authorisations successfully granted?	4
	The number of urgent applications made for a Directed Surveillance authorisation?	0
	The number of Directed Surveillance authorisation granted in an urgent case?	0
	The number of Directed Surveillance authorisations that were cancelled?	2
	The number of Directed Surveillance authorisations extant at the end of the year?	2

Appendix E: Information Governance Risks and Issues 2018/19

As of the end of March 2019:







Currently for the 28 risks reported (April 2019):

- 6 (21%) risks with a residual risk score of 15 or above (red rating)
- 16 (57%) risks with a residual risk score of between 5 and 12 (amber rating)
- 5 (18%) risks with a residual risk score of between 1 and 4 (green rating)
- 1 (4%) risks with no residual risk score allocated

This page is intentionally left blank