CORPORATE RESOURCES
OVERVIEW AND SCRUTINY COMMITTEE
29 February 2016

TITLE OF REPORT: **Annual Report –Information Governance and the Council's use of powers under the Regulation of Investigatory Powers Act 2000**

REPORT OF: **Mike Barker, Strategic Director, Corporate Services and Governance**

Summary

This report provides the Committee with an overview of arrangements for Information Governance across the Council, including the annual reporting of data breaches. It also provides details of the Council's use of covert surveillance and offers assurance that when authorising covert surveillance the Council is compliant with the requirements of the Regulation of Investigatory Powers Act 2000 (RIPA).

Information Governance

Introduction

1. This is the first annual report to the Committee regarding the Council's Information Governance framework. It aims to provide the Committee with the legislative context within which the Council manages a range of sensitive information and personal data, compliance with relevant guidance and good practice, and the Council's performance in this area over the last twelve months. It is therefore intended to form an important part of the Council's Overview & Scrutiny Framework, alongside other annual performance reporting.

Background

2. Public trust in the way public services handle and share data is increasingly important, particularly in the context of greater digital storage and transfer of information. Service users expect easier access to services and a 'one stop' delivery experience. They want to be in control of their interactions with council services and for those services to be delivered at lower cost, more quickly and based on individual needs. This lies at the very core of what all local public services strive to do, and in Gateshead is captured within our policy objectives as set out in the Council Plan 2015-20 and our Digital Strategy.

3. Success in this area depends on many factors, but effective and secure exchange and management of information is vital for both good service delivery, and for compliance with an increasingly onerous and prescriptive legislative framework at both a national and European level. The public and regulatory bodies must have

confidence in the way that any data we hold is treated, taking privacy and confidentiality into account, and that it is kept safe from misuse. Without that assurance service users are unlikely to engage, services will be less efficient and much poorer as a result, and we face stiffer penalties if found to be failing to meet our legal responsibilities..

4. In 2010 the Local Government Association produced data handling guidelines for local authorities. Those guidelines, which were revised in 2014, set out the steps that every local authority should take to monitor and control the management of information and to mitigate the risk should personal information be lost or data protection systems fail. The Council's approach to information governance is based on these guidelines.

5. The Council recognises that there must be a systematic and planned approach to the management of its information. This will ensure that from the time a record is created, until its disposal, standards and handling will be consistent across the organisation and that the record can be tracked throughout its lifecycle to ensure it serves the needs of the Council and its stakeholders, and complies with relevant legislation.

6. The way the Council manages its information is also crucial to maintain effective and efficient business operations. Information management is about providing an integrated records and information system to ensure quick, efficient and consistent access to records across the organisation. Public sector organisations have more demands than ever before to be open and transparent. The introduction of the Freedom of Information Act 2000, on 1 January 2005 and the government's transparency agenda means anyone can request information from the Council. This can be achieved quickly and efficiently if effective information management systems are in place.

7. The Council has an Information Charter and an Information Strategy. The strategy provides a framework which enables the Council to manage its information efficiently, recognising its value as a corporate asset for the delivery of effective, appropriate and transparent services.

Information Governance Structure

8. **Accountable Officer** – this role is assigned to the Chief Executive. The Accountable Officer has overall accountability for information governance across the Council and must provide thorough assurance, including a statement of internal control, to demonstrate that all risks are effectively managed and mitigated. The Accountable Officer is required to sign any undertaking with the Information Commissioner should a data breach occur.

9. **Senior Information Risk Owner** – (SIRO) – this role is assigned to the Strategic Director, Corporate Services and Governance. The SIRO must determine how strategic business goals of the authority may be impacted by information risks and act as an advocate for information risk within senior management. He must oversee the development of an information risk policy, and strategy for implementing the policy, within the governance framework. The role must accept

ownership of risk assessment processes for information risk, provide written advice to the Accountable Officer on the content of the statement of internal control, and undertake information governance training at least annually.

10. Overall the role of the SIRO is to foster a culture that properly values, protects and uses information. One aspect of this is to ensure that awareness training is conducted at the appropriate level and to monitor understanding and ability periodically. A further aspect is to establish and chair (or delegate chairing to the Deputy SIRO) a Corporate Information Governance Group whose remit is to report back to senior management on a regular basis.

11. **Deputy SIRO** – this role has been assigned to the Information Rights Officer. The role is generally to assist the SIRO including, for example, in the collation of information from Information Asset Owners and Information Asset Assistants.

12. **Information Asset Owner** - this role is assigned to every other Strategic and Service Director. An Information Asset Owner needs to be identified for each of the information assets the Council holds, referenced and co-ordinated according to council function, based on the local authority function list produced by the Records Management Society of Great Britain. They are responsible for maintaining day to day information governance practice within their service area. They need to understand and monitor:

    - what information assets are held, and for what purpose
    - how information is created, amended or added to over time
    - who has access to the information

13. **Information Asset Assistants** - this role has been assigned to senior managers within each service. They assist the Information Asset Owners to fulfil their role by acting as the first point of contact for staff who may have information governance queries. Their role is to ensure:

    - policies and procedures are followed
    - potential or actual security incidents are identified
    - Information Asset Owners are consulted on incident management
    - Information Asset Registers are accurate and maintained up to date

14. **Individual Responsibility** – all Council staff are responsible for any information which they create or use: they must ensure that they create and maintain appropriate records in relation to their work at the Council and to manage those records in accordance with the Council's information security and data protection policies and procedures.

    - All staff should:
        - make sure that records are complete and legible
        - keep records where they can be found
        - keep records up to date
        - keep track of records
        - make sure confidential records are kept secure
        - follow the Council's records retention schedules for all records

- destroy records in accordance with the Council's retention schedules.

15. **Internal Audit** will be responsible for conducting an annual information audit. The aims of the audit are:

- to identify which business functions create which records
- to identify what these records are used for, where and how they are kept
- to identify how information is tracked within each service area
- to identify if appropriate access controls are in place
- to identify business critical records, which are necessary for the organisation's daily business and legal obligations
- to identify existing disaster recovery arrangements and undertake a gap analysis
- to identify the level of staff awareness of information management issues information protection and disaster recovery

16. An essential part of the information management role is protecting records from elements such as floods, fire, theft and loss. The Council follows the National Archives Records Management Recovery plans standard for the management of government records. This standard is a best practice benchmark for all organisations creating or holding public records.

Information Storage

17. Storage of the Council's paper based records is reviewed annually in line with retention periods and records are destroyed or transferred to archive if required.

Risk Assessment

18. Information governance is included in the Council's Strategic Risk Register.

Training

19. The SIRO, Deputy SIRO and all Information Asset Owners received training at the end of December 2013 from Dilys Jones Associates ('DJA', a nationally recognised training provider on information governance). Information Asset Owners received training in 2014 from the Deputy SIRO in relation to the completion of information asset registers and all registers were completed by the end of 2014.

20. In 2015 the SIRO received further training from DJA at a regional event on SIRO roles and responsibilities.

21. On-line training modules on information governance are in the process of being developed and will be rolled out across the Council during 2016/2017.

Data Breach Reporting

22. Data breaches can be reported to the Information Rights Officer or via the incident reporting mail inbox.

23. The SIRO is informed in the event of a data breach and the Information Rights Officer provides advice to the service concerned about what remedial action needs to be taken. The SIRO makes a determination whether the incident has to be reported to the Information Commissioner in line with the Information Commissioner's guidance on data breach reporting.

24. The incident reporting inbox is an inbox which internal audit access and they can choose to investigate serious breaches.

Month	Data Breach	Outcome
Feb 2015	SEN record sent to the wrong person	Record retrieved. Complainant complained to the Information Commissioner. The Commissioner was happy with the action the Council had taken. Staff received training
June 2015	Theft of database containing service user details by two former employees	Reported to the Information Commissioner for him to prosecute. He declined to prosecute
Aug 2015	Confidential report sent to the wrong family (child protection)	Report retrieved - family informed
Aug 2015	Complainant who asked to remain anonymous wrongly identified	Apology given to the complainant. Staff given training
Oct 2015	e-mail sent to the wrong recipient	Email recalled. Wrong recipient contacted email retrieved
Dec 2015	Chairs' report sent to the wrong family (child protection)	Report retrieved - family informed

25. Should a complaint be made to the Information Commissioner or a breach reported to the Information Commissioner's Office (ICO) by the Council, the Information Rights Officer liaises with the ICO and the complainant to reach a satisfactory outcome. The ICO may also decide to take enforcement action against the Council: this may be in the form of criminal prosecution, non-criminal enforcement and audit. The ICO also has the power to serve a monetary penalty notice on a data controller. To date, there has been no formal enforcement action taken against the Council for data breaches.

<u>Regulation of Investigatory Powers Act 2000 (RIPA)</u>

Background

26. This is the first report in relation to the Council's use of RIPA. It was recommended in the new codes of conduct produced by the Office of the Surveillance Commissioner at the end of last year, that Councils should report their use of RIPA to elected members at least annually.

27. RIPA provides a statutory mechanism (i.e. 'in accordance with the law') for authorising directed and covert surveillance and the use of Covert Human intelligence Sources (CHIS). It also permits public authorities to compel telecommunications and postal companies to obtain and release communications data in certain circumstances. It seeks to ensure that any interference with an individual's rights under Article 8 of the European Convention is necessary and proportionate. In doing so, RIPA seeks to ensure that both the public interest and the human rights of individuals are suitably balanced.

28. Covert surveillance involves monitoring, observing, listening to persons, watching or following their movements, and is carried out in such a way that the subject of the surveillance is unaware it is taking place.

29. There are two types of covert surveillance that the Council can use:
    - directed surveillance – this involves observing, following or watching the subject of the surveillance
    - CHIS – in relation to the Council's functions, this involves using volunteer adults or children to attempt to make test purchases

30. Typically this council uses RIPA in relation to benefit or council tax fraud when information is received that a claimant has someone living with them or is working and claiming benefits. Surveillance will be used to watch the property to see if there is any evidence of another person living there. If evidence is found the subject of the surveillance will be invited in for an interview under caution.

31. The Council uses CHIS (normally members of staff or child volunteers), when it receives information that, for example, a householder is selling illegal tobacco or a shop is selling age restricted products such as alcohol, cigarettes or fireworks to underage children. The CHIS will be used to attempt to make a test purchase. If the test purchase succeeds then the subject of the surveillance is invited in for an interview under caution.

32. The Protection of Freedoms Act 2012 amended RIPA to restrict when councils can use the powers it provides. An authorisation for directed surveillance or CHIS can only be made by councils now if certain conditions are met:

    - that the authorisation is for the purpose of preventing or detecting crime
    - the criminal offence is or would be an offence which is punishable, whether on summary conviction or indictment , by a maximum term of at least 6 months imprisonment or
    - is an offence under:

- Section 146 of the Licensing Act 2003 (sale of alcohol to children
- Section 147 of the Licensing Act 2003 (allowing the sale of alcohol to children)
- Section 147A of the Licensing Act 2003 (persistently selling alcohol to children)
- Section 7 of the Children and Young Persons Act 1933 (sale of tobacco etc. to persons under 18)

33. Covert surveillance should only be used in exceptional circumstances when necessary information cannot be uncovered by overt means – open CCTV or officers patrolling with visible body worn video cameras. The decision to use covert surveillance must take into account the issue of proportionality - the surveillance must not be excessive in relation to the seriousness of the problem it seeks to address.

    The Council must ensure that:
    - all covert surveillance exercises conducted by the Council comply with the requirements of RIPA and
    - all authorisations contain the detail of the surveillance which is to be permitted and why the authorising officer believes the surveillance to be necessary. To demonstrate the necessity of the covert surveillance all authorisations must mention all other possible means of discovering the desired information and the reason for their rejection.

.

34. Councils are not permitted to undertake intrusive surveillance i.e. tapping phone lines or any surveillance inside private property or placing tracking devices on a subject's vehicle or person.

35. Only duly appointed authorising officers can be permitted to authorise a covert surveillance exercise.

Arrangements

36. The Council's compliance with RIPA is independently audited periodically by two Commissioners: the Office of the Surveillance Commissioner and the Office of the Communications Surveillance Commissioner. The Home Office has produced a code of conduct in relation to covert surveillance. The Commissioner audits how the Council has used its powers under the Act and how well it has complied with the code of practice.

37. In addition, the Protection of Freedoms Act 2012 amended RIPA, meaning that before a surveillance exercise can take place, an application which has been authorised by an authorising officer has to be approved by a magistrate.

38. The Investigatory Powers Tribunal can hear complaints from any person aggrieved by the conduct carried out in challengeable circumstances within one year. The tribunal can award compensation or can quash or cancel any authorisation and can order the destruction of records of any information obtained by exercising any power.

39. The Act designates various roles which are held by specific Council officers as follows:
    - Senior Responsible Officer (SRO) – this role is held by the Service Director, Human Resources and Litigation. The SRO is responsible for:
        - ensuring that all authorising officers are of an appropriate level of seniority and have had training
        - the integrity of the process in place within the public authority to authorise directed and intrusive surveillance and interference with property or wireless telegraphy
        - compliance with Part II of the 2000 Act, Part III of the 1997 Act and with the codes of practice
        - engagement with the Commissioners and inspectors when they conduct their inspections, and where necessary, overseeing the implementation of any post inspection action plans recommended or approved by a Commissioner

    - RIPA Co-ordinating officer - this role is held by the Litigation Manager and Information Rights Officer. The role is responsible for:
        - maintaining the central record of authorisations
        - collating the original applications/authorisations, review, renewals, cancellations
        - oversight of the submitted RIPA documentation
        - organising the RIPA training programme
        - raising RIPA awareness within the Council

40. Authorising Officer - these roles are assigned to service managers or above who have been trained to authorise requests for directed surveillance and the use of CHIS.

    RIPA does not:
    - make lawful conduct which is otherwise unlawful
    - prejudice or disapply any existing powers available to the Council to obtain information by any means not involving conduct that may be authorised under this Act. For example, it does not affect the Council's current powers to obtain information via the DVLA or to get information from the Land Registry as to the ownership of a property.

Statistics

41. Gateshead Council uses its power under RIPA when it is appropriate to do so.
    - In 2015 the powers were used five times - on four occasions for illegal tobacco sales and once for counterfeit goods.
    - In 2014 the powers were used four times - on two occasions for counterfeit goods, once for benefit fraud and once for illegal tobacco.
    - In 2013 the powers were used 5 times – on four occasions for illegal tobacco and once for theft.

Inspection

42. The Surveillance Commissioner inspected the Council in June 2015. He made a few observations about the number of authorising officers and recommended that training of authorising and requesting officers was undertaken more frequently. He also suggested that reports be made to elected members about the use of RIPA and recommended some minor amendments to the Council's policy. The issues raised have been addressed. All officers received refresher training in November 2015.

Case studies

43. Council officers enter a pub on a number of occasions and behave as ordinary customers to covertly observe whether there is compliance with the smoke free legislation. If they find non-compliance they leave the premises and colleagues equipped with covert video recording equipment record the activities of offenders (those smoking and those in charge of the bar). Is RIPA authorisation available?

    - Yes – directed surveillance
    - Yes - CHIS authorisation
    - Yes – intrusive authorisation required
    - No – surveillance outside RIPA

44. The trading standards team has received complaints that a local individual is advertising fake goods on facebook to their facebook friends. When he is contacted through official channels he denies everything. You cannot access his facebook page as you are not a friend. In any event the Council blocks access to facebook. An officer who has a personal facebook account volunteers to "friend" the target in order to access his facebook page thus allowing investigations into what goods are being offered for sale. The team asks him to print out the relevant pages and give him a list of questions to ask the target. Is RIPA authorisation available?

    - Yes – directed surveillance
    - Yes – CHIS authorisation
    - Yes – intrusive surveillance
    - No – surveillance outside of RIPA

45. You are line manager for a difficult employee. He is off sick with a bad back. Other staff have reported that he is doing building and decorating works and that he advertises in a local shop. Officers go to the shop and see his advert. They take the number and then ring pretending to be a customer inviting him to come to a house to give a quote for work. Is RIPA authorisation available?

- Yes - directed surveillance
- Yes - CHIS authorisation
- Yes – intrusive surveillance
- No - surveillance outside of RIPA

Recommendation

46. The Corporate Resources Overview and Scrutiny Committee is asked to endorse the information in the annual report, and satisfy themselves that the Information Governance is operating satisfactorily and that the Council uses the powers under the Regulation of Investigatory Powers Act appropriately.