CORPORATE RESOURCES
OVERVIEW AND SCRUTINY COMMITTEE
27 February 2017

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. 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 second 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.

8. With the approval of the new General Data Protection Regulation (GDPR) ,which has been ratified by the European Parliament and comes into effect in the UK on 25 May 2018 , there is a move away from seeing the law as a box ticking exercise, and instead to work on a framework that can be used to build a culture of privacy that pervades an entire organisation.

9. The GDPR requires a significant amount of work to be undertaken right across the Council to ensure we can be compliant with the requirements when they come into force :-

    a. All information assets need to be captured
    b. We need to tell people the identity and contact details of the Data Controller
    c. Contact details of the Data Protection Officer which is a new statutory role which public sector organisations will be required to have.
    d. Be able to state the legal basis for data processing
    e. Tell recipients of personal data if it is going to be transferred outside the EEA

f. Advise of the data retention period
g. Advise of any statutory or contractual obligations to process the data
h. Advise of the consequences of failing to provide the data
i. Advise of the right to withdraw consent
j. Advise of the right to lodge a complaint
k. Reduces the timescale for responding to a subject access request from 40 calendar days to 1 month
l. Changes in consent – consent has to be explicit and unambiguous, cannot rely on implied consent
m. Need consent from children over 16 or their parents depending upon the age of the child
n. Embed a culture of privacy by design and data minimisation
o. Monitor, review and assess data processing procedures, building in triggers for reviews as appropriate
p. Review all data sharing agreements
q. Create a privacy policy and data breach management policy

10. A Corporate working party has been established to ensure that the Council can be ready to meet its obligations under the GDPR.

11. **Internal Audit** -To support management in their responsibility to install and maintain effective internal control systems, Internal Audit's Strategic Plan includes an audit of Information Governance. The audit assesses the adequacy of current controls against the following objectives:

    a. The Information Governance Framework in place;
    b. The Information Governance Structure in place;
    c. That an up to date Register of Information is in place
    d. The Incident Management Procedures in place for identifying, reporting and preventing data breaches; and
    e. That performance reporting is carried out on a regular basis

12. Records management -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

13. 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

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

Training

15. The Deputy Senior Information Risk Owner (Siro), attended training at Durham Council in October 2016. A briefing was carried out in October for the leadership team and all new information asset assistants have been appointed to review information asset registers. Training is scheduled to begin in March and will continue throughout 2017 not only for information asset assistants but for all staff to raise awareness of their data handling responsibilities.

Data breach reporting

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

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 they need to take.

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.

The incident reporting inbox is an inbox which internal audit access and can investigate in relation to serious breaches.

Month	Data breach	outcome
Jan 2016	Report sent out containing information about another family	Report recovered
March 2016	Report sent to wrong address as wrong address recorded on carefirst	Report recovered – staff underwent training
April 2016	Bag stolen containing diary with confidential information	Reported to the police - bag not recovered
April 2016	Email sent containing sen statement to the wrong family	Report retrieved and correct report given. Complainant complained to the Information Commissioner who found that there had been a data breach but took no enforcement action- refresher training provided for all staff
May 2016	Email sent to the wrong recipient	Email retrieved
July 2016	Invite to a CP conference sent to the wrong recipient	Letter retrieved and destroyed
Oct 2016	Confidential information sent to the wrong address	Information retrieved and sent to the correct address- staff member given refresher training
Nov 2016	Confidential information sent to the wrong address	Information retrieved training action plan in place for staff member

Dec 2016	Protected address given to father	Internal investigation taking place not yet concluded – matter to be reported to the Information Commissioner

Should a complaint be made to the Information Commissioner or a breach is reported to the Information Commissioner by the Council, the Information Rights Officer liaises with the Information Commissioner to reach a satisfactory outcome.

Regulation of Investigatory Powers Act 2000 (RIPA)

Background

16. This is the second 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.

17. 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.

18. 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.

19. 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 – this involves using volunteer adults or children to attempt to make test purchases

20. 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.

21. 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.

22. The Protection of Freedoms Act 2012 amended RIPA to restrict when councils can use RIPA. 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)

23. 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;
    - 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.

.

24. 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.

25. Only authorising officers can be permitted to authorise a covert surveillance exercise.

Arrangements

26. 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.

27. 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 before the proposed surveillance activity takes place.

28. The Investigatory Powers Tribunal can hear complaints from any person aggrieved at 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.

29. The Act designates various roles to officers, these roles are held by specific Council officers as follows:

- Senior Responsible Officer (SRO) – this role is held by the Service Director, Human Resources and Litigation. 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

30. 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

31. Gateshead Council uses its power under RIPA when it is appropriate to do so.
    - In 2016 the powers were used twice – both for illegal tobacco sales
    - 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

32. 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 all been addressed. All officers received refresher training in November 2015.

33. In July 2016 the Council was re-inspected by the Surveillance Commissioner and found to be fully compliant with the requirements of RIPA

Recommendation

34. 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.

Contact: Deborah Hill EXT: 2110