Use of Data in the Council

Contact Officer: Dan Kennedy / Naveed Mohammed
Telephone: 01895 250 495 / 277 263

REASON FOR ITEM

Following a request from the Chairman, this paper presents an update on how data is gathered and used in the Council to support the delivery of corporate priorities.

SUGGESTED COMMITTEE ACTIVITY

It is recommended that the Committee:

1. Note the update.
2. Question officers about the update.

INFORMATION

Background

The Council delivers over 700 services to the 100,214 households that comprise the London Borough of Hillingdon. As part of this, the Council routinely gathers a wide spectrum of data it needs to ensure services are being delivered in the most effective and efficient way. In doing so, like many organisations, the Council has to pay due regard to prevailing legislative requirements that govern the collection, storage and use of especially personal, sensitive data. Furthermore, given the voluminous nature of the data that is gathered - the Council has, at its disposable a variety of mechanisms to 'make sense of the data' from the use of basic spreadsheets through to the use of more bespoke databases and data mining software.

This paper will provide an overview of the arrangements in place, including use of case study examples demonstrating how data has been used, and whether to shape service delivery or enable the council to discharge its responsibilities.

It is important to note at the outset that, given the depth and breadth of data that is compiled and used by the Council, this paper is not intended to provide an exhaustive list of how data is used. Rather it will provide a general overview and an attempt to answer the following questions

1. What are the roles and responsibilities for the gathering and management of data across the Council?
2. What data does the Council hold/gather?
3. What arrangements are in place to store data and ensure its security?
4. How is data interrogated?
5. How is data used to help Hillingdon Council discharge its responsibilities and shape service provision?
6. Future arrangements?

Allocation of roles and responsibilities

Roles and responsibilities for the gathering and management of data are dispersed across the authority. In broad terms, the Council operates a corporate business performance function which has responsibility for the interrogation and analysis of data. Ownership of the data, including its compilation and data quality, rests with service areas.

What data does the Council hold/gather?

As mentioned previously, the Council provides over 700 services to local residents. The provision of these services relies on the effective and efficient gathering of service data, whether this relates to demographics and understanding the make-up of clients, how efficiently functions are being delivered and measuring outcomes achieved (i.e. what difference the services provided are making for Hillingdon residents).

Whilst the data that is gathered is likely to fall into these three categories, the specifics of what is collected will differ depending on the service area.

Table 1

Directorate	Examples of Functions	Examples of data gathered
Administration	Legal, Policy and Partnerships, Democratic Services	HR data, Office of National Statistics data, Greater London Authority data store including census, labour market trends.
Finance	Business Assurance, Revenues and Benefits, corporate finance	Council tax collection, business rates, benefits information, debtors.
Resident Services	Public Health, Education, Planning, HR, Housing, Sport and Culture, Community Safety, Libraries, Waste and Refuse	Health profile, school places, Strategic Needs Assessment, crime types, school attainment, library footfall, books issued.
Adults, Children and Young People's Services	Safeguarding, Early Intervention, Children and Adult's social care, disability services	Service demand, business processes, Special Educational Needs numbers, children's centres, employment and training figures for young people, Youth Offending, caseloads, length of time of cases.

Whilst by no means an exhaustive list, the range of data set out in Table 1 provides a good demonstration of the breadth of data that is gathered across directorates. Much of this will be gathered directly by services, either from clients or from in-house systems. There are, however, particular data streams that rely on contributions from partner agencies or external systems. For instance:

- Community Safety - data on crime types and trends, including benchmarking data, is obtained from the Metropolitan Police, as well as accessing third-party data sites such as IQuanta.

- Public Health - data on local health profiles are available from Public Health England. Data on prevalence rates for specific conditions are available from Department of Health or from local Clinical Commissioning Group partners.

- Young People Not in Education, Employment or Training (NEETs) - the Council does not collect data directly on local NEET numbers. Like other West London Councils, a commissioned provider gathers and supplies this data, including analysis.

- Office of National Statistics data - Much of the data on Census statistics is housed on Office of National Statistics websites including 'Neighbourhood Statistics'. This includes all the figures on socio-economic profiles, population trends, sub-national projections etc.

- Subject to the needs of the service and/or project, the Council may, from time to time, utilise other data sources for the purposes of triangulation and adding greater depth to the intelligence being gathered.

- Finally, wherever appropriate and needed, the Council will often access and share more sensitive data to prevent and identify instances of fraud. This is particularly the case in revenues and benefits and housing.

What arrangements are in place to store data and ensure its security?

Storing Data

Outside of the more routine collection of national statistics via Excel (all stored on the LBH network), specific service-related data sets are stored on databases relevant to those areas.

Ensuring data security

Given the stringent statutory requirements in this area, information governance is an important element of the Council's work. The Council has clear duties to protect the information held about members of the public and/or its employees (as well as confidential information pertaining to legally or commercially sensitive data). Breaches of the Data Protection Act through loss or mishandling of personal data are criminal offences that can result in large fines (up to £500,000). Given this, the Council has an overarching Information Governance Policy (2015) that regulates how LBH proprietary and client, partner or supplier information, when created, stored, transmitted or communicated is protected from unauthorised access, use, modification or destruction. At the heart of the policy are seven key principles that require adherence. This includes:

- **Confidentiality** - Appropriate measures must be taken to ensure LBH proprietary, private or client information is accessible only to those authorised to have access.
- **Integrity** - The accuracy and completeness of LBH information must be maintained and all changes or modifications affecting that information must be authorised, controlled and validated.
- **Availability** - Information must be available to authorised individuals when required. In the event of a disaster or malicious attack, the Council's information and the systems critical to the ongoing activities of the Council must be recoverable.
- **Authentication** - All persons and systems seeking access to information, or to LBH networked computer resources must establish their identity to the satisfaction of the Council.

- **Access Control** - The privilege to view or modify information, computer programs or the systems on which the information resides, must be restricted to only those whose job functions absolutely require it.
- **Auditing** - Use access and activity on each of the council's computers, firewalls and networks must be recorded and maintained in compliance with all security, retention, legislation and regulatory requirements.

In addition to these policy principles, the Council provides further explicit direction and training to employees on the storage, handling and use of data including the need to;

- Keep information safe and secure including the use of robust passwords, being security aware when entering or leaving the building and only using authorised equipment;
- Checking who information is being shared with;
- Using email carefully and responsibly including use of secure email when receiving or transmitting sensitive data, and using blind copy where necessary;
- Not storing personal data on local hard drives, laptops or mobile devices;
- Keeping data secure when working away from the office; and,
- Taking extra care when taking information outside the office.

The Council's Information Security Officer has responsibility for the maintenance of the security policies which are owned by the Hillingdon Information Assurance Group (HIAG). All managers are responsible for implementing the security policies within their respective areas.

A copy of the Council's Information Security statement is provided in Appendix A.

How in Data interrogated?

The Council has a wide-variety of tools at its disposal for interrogating data. Wherever possible standard reporting tools that can connect to the service specific IT systems are used. In addition, the Council has access to a number of subscribed services that provide interrogated data. This includes access to Fisher Family Trust - a bespoke service providing analytical support for education data and Iquanta which performs a similar function for community safety data. Although part of a wider SLA (and as such not strictly a subscription service) the Council also utilises support from contracted providers such as West London Partnership Unit (Connexxions) that provide an analytical service for NEET data.

Whilst each of the above examples have related to service-specific tasks, there have more recently been occasions where the Council has needed to analyse data across multiple services. A good example here is the Troubled Families programme. As part of the latter, the Council has needed to identify family households that have been flagged under various categories including persistent school absence/truancy, anti-social behaviour, long-term unemployed etc. Adopting a single-service approach would not be useful in this context and so the Council utilised a software solution that is able to look across multiple databases and 'flag' names that (re)appear. To date, this approach has been critical in enabling the Council to identify over 800 eligible families.

How is data used to help Hillingdon Council discharge its responsibilities and shape service provision?

Whilst like many councils, Hillingdon is required to gather data for the purposes of statutory returns (including in Adult Social care, Children's Services and Housing). The primary purpose of the vast majority of data collected is to ensure the Council is appropriately discharging its responsibilities and helping aid future service development.

In respect of the former, data collected in social care, planning etc, helps build a picture of how efficiently the Council is meeting targets, for instance, in the processing of planning applications or discharging statutory social care requirements.

In addition to the above 'process measures', the Council regularly uses data to help shape service delivery, whether this is part of ongoing work or one-off projects. An example of this includes the Joint Strategic Needs Assessment which is the overarching data store which helps shape and inform future commissioning plans.

Case studies have been provided as appendices which provide further detail on this.

Future arrangements?

The Council is committed to continuing to use data to intelligently drive forward service improvement. As part of the BID programme, the interrogation of data forms a key element of any service review.

Whilst this new approach will continue across the range of scheduled BID reviews, the Council is equally committed to using data to improve frontline services to residents in day-to-day service delivery improving practice in its more traditional operations. A key priority here is enabling staff, including senior managers, get access to 'live data', the alignment of service and financial data and finally more sophisticated supply/demand modelling to help anticipate and plan for future service needs.