Policy, Strategy and Partnerships

Data, Insight and Information Strategy

Cabinet – 05/10/2021

Appendix C – Engagement with Scrutiny

Summary

The draft Data, Insight and Information Strategy was offered to OSMB Leads for formal scrutiny, but the logistics of meeting timings and capacity within the OSMB work programme meant this was not possible.

Instead, OSMB Leads reviewed the draft strategy and submitted written questions to officers. These are reproduced below for transparency.

1. **Decision Pathways - what is the process for adding items to be monitored and to ensure that the data is qualified and up to date?**
   Every data source loaded is based on an 'as is' basis unless there is a legal reason not to, for example Benefits data. If this falls outside of the main Privacy Impact Assessment (PIA) for the data and analytics platform then we will either amend the PIA with Information Governance colleagues or create a new one as appropriate prior to any work commencing.

   We follow a standardised data classification process that enables sensitive data to be securely partitioned from non-sensitive data. Data that does not support analytics is excluded and will not be loaded into the Data and Analytics Platform. All data is secured and all access, use and attempts to access are recorded 24/7. Monitoring reports are live and monitored by the corporate teams supporting the Programme. The responsibility for accuracy remains with the Information Asset Owner and any identified inaccuracies will be reported to them for action.

2. **Breaking the silo mentality is very important, but so is information security - how will this be managed?**
   The corporate data and analytics platform increases data security for the Council as it provides a fully audited, secure environment that covers Extract, Load, Transformation and also consumption by end users. The access controls are based on 'zero access assumed', with changes on a business need basis documented in a Privacy Impact Assessment, and controlled through Azure Active Directory.

3. **What modifications will be made to the current council information access policy, and how will they be communicated to council employees?**
   Our corporate approach does not change the current information policy, it is designed to align to it and reduce risk of non-compliance. This notwithstanding, information about the Strategy and Programme will be communicated through internal communication channels including our Manager's Briefing. In areas directly affected, more localised communication will be undertaken including team briefings and training for affected colleagues.

4. **Logging is essential to the project's success, not just to see how often and which data items are accessed but also who is accessing the data. How will this be managed?**
   All access, use, activity is monitored against the individuals' Azure Active Directory account and all attempted access is recorded the same way. Monitoring reports are live and in use.

5. **Real-Time Data: what sort of data will be shown, how will alerts and thresholds be set up?**
There are none at present, streaming analytics which use real time data have not been required in any of the work to date.

   When a business need is established to use real time data in analytics, Azure streaming analytics will be turned on within the Data and Analytics platform for that purpose only and in order to ensure cost feasibility. Where we are able to implement real-time reporting, we can also implement 'point in time' reporting so that we can review trends where necessary. Alerts can be automated based on dates or data, so that a pre-defined report can sent to an email address or an alert set. The thresholds for this will be defined on a case-by-case basis based on business need and appropriate Privacy Impact and/or risk assessments.

6. **Video Data - Anonymisation and what is the AI-Integration policy? - all sorts of privacy issues here.**
Privacy issues are indeed standard with any sensitive data. Image data that makes somebody personally identifiable is treated no differently in breach or misuse than an address or name. There is a robust PIA process underpinned by technical platform controls.

   Currently this is a developing area and any personalised data is anonymised within data sets. As our approach develops, so too will policy and protections which will be completed and applied before usage begins.

   In terms of deploying AI on video data, this is only being explored at a technical proof-of-concept level, and this exploration does not use facial recognition or personal data.

7. **The proposed programme includes Ivanti Replacement. Ivanti is an IT orientated customer relationship management product; it's being replaced by what tool?**
The council is upgrading its legacy IT Service Management platform with a much later version from the same supplier.

8. **The Ethics Board - who is on it, and what's the process for membership?**
This is being developed and options will be considered by Data, Insights and Analytics Board. We will require all those requesting data driven projects or insight to set out how they have identified and taken any ethical considerations into account. This may prove sufficient, although for more complex and sensitive matters an ethics board may prove more beneficial.

9. **Regarding the monetisation of the data, is the council planning to sell information gathered by this system to third parties?**
We have no plans to do this and have committed to an Open Data approach.

10. **Third-party contributions to the data set: examples like Fix My Street and Bristol Waste, will they be accessible in dashboards, and the data sharing principles?**

Fix My Street already has an integration with the Citizen Services team, and therefore we can merge this data within the available dashboards. We will be taking data feeds from partner organisations. The basis here is that the data will be available to a user as long as a Privacy Impact Assessment has been completed and the user has a valid legal justification for doing so, including a requirement to comply with GDPR regulations at all times.

11. **What is the process for sharing information that is not in the scope of the Open Data Standards? Other government agencies like the Police, DVLA, and UK Border Force will ask for data access.**

There are number of ways to improve compliance assurance in the way we share data. We are piloting Azure Secure Data Share later this year for example. We have existing Information Sharing Agreements with several organisations including Police, NHS and the Department of Work and Pensions where there is a legal and appropriate reason to share the data. Data can be shared via exchanged data sets, or by carefully controlled, secure federated access to our data lake.

Guy Collings
Head of Insight, Performance and Intelligence
08/09/2021