Directors Group **October 7th 2019**

Information Asset Owners (IAOs): strengthening accountability for data protection and information management.

1. The Council's Information Governance Framework (2019) assigns the role of Information Asset Owner (IAO) to Directors.

2. The role of the IAO is to understand what information is held within their services and how it is managed – access and disclosure, security and risk, opportunities.

3. An information asset is a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited effectively. Information assets have recognisable and manageable value, risk, content and lifecycles.

4. The Framework relies on key roles like the IAOs, Senior Information Risk Owner (SIRO) to help assure governance is in place – Annual Governance Statement.

5. IAOs will appoint information asset administrators (IAAs) to assist them such as the system administrator for a case management system, as well as managers who might take a lead for data quality, information management and information rights.

6. IAOs and IAAs will be supported by the Information Governance Working Group of portfolio representatives and the Information Management Team. The Information Governance Board provides the strategic lead for information governance to the council.

7. IAOs will work closely together to ensure there is comprehensive information asset ownership and clear understanding of individual responsibilities and accountabilities. This is particularly true when Information Assets are shared by different parts of the organisation.

8. IAOs will undertake training to understand their accountability so they can exercise the necessary check and control whilst delegating tasks to their management teams and staff.

9. IAOs will promote their role in the service for the assurance of colleagues and customers.

Table of accountabilities

Promote data protection by design and by default There is culture of considering data protection and privacy issues upfront in everything to help ensure compliance with the GDPR's fundamental principles and requirements, and forms part of the focus on accountability. Sign off Data Protection Impact Assessments to Iidentify and minimise the data protection risks of a project. Agree the technical controls to uphold the confidentiality, integrity and availability of information assets. Implement de-identification procedures (including pseudonymisation and anonymization) to protect data.
Disseminate Information Governance policies and ensure mandatory training Make every member of staff aware of corporate policies and procedures, supplemented by necessary local policies and procedures. Ensure mandatory training is undertaken, including any refreshers and specialist training is identified and resourced.
Maintain Records of Processing Activities Ensure that registers of personal data held are compiled and maintained, mandated under Article 30 of GDPR. Know the purpose for collection and sharing, as well as methods used for transferring and handling the data. Non-personal corporate data, software applications, contracts and information sharing agreements and relevant business continuity arrangements constitute the Information Asset Register, which is kept under review.
Comply with regulatory standards Mobilise support (as applicable) for annual compliance with: NHS Data Security and Protection Toolkit; CQC key lines of enquiry; Public Service Network (PSN); Cyber Essentials scheme; Payment Card Industry-Data Security Standard (PCI-DSS); Lexcel Standard for legal practices.
Direct information security investigations Promote a culture of honesty about incidents so that they are reported as quickly as possible to contain them, and notify the Information Commissioner if necessary. Sign-off and monitor improvements to processes to reduce human error.
Own Information Risk Register Identify, prioritise and manage risks involved in all business activities, i.e., personal and non-personal information as it is moved in, out or between services. Give attention to contractors so they can meet and maintain the council's standards if data protection.
Lead information management practice Information is seen as a key corporate asset and staff consider themselves 'trusted stewards' of sensitive data. Data are valued throughout its lifecycle to ensure the maintenance of accurate and current records, with a clear review, retention and disposal policies in line with legal and regulatory frameworks.
Publish Open Data Identify, collect and systematise the flow of datasets to meet the Freedom of Information model publication scheme; Local Government Transparency Code 2015; INSPIRE regulations 2009 (geospatial datasets) and the council commitment to transparency.
Authorise responses to information rights requests Provide resources to respond to Freedom of Information, Environmental Information and Subject Access Requests, as well as other data subject rights under GDPR, and requests for the Re-Use of Public Sector Information Regulations 2015 (ROPSI). Maintain clear lines of authorisation for the disclosure or withholding of information. Keep to deadlines for responses.
Sign Information Sharing Agreements Negotiate, manage and approve agreements on the sharing of personal information between organisations in memoranda of understanding or enforceable contracts. Document data flows to minimise risk and provide transparency to data subjects.
Approve Privacy Notices Provide clear information about the use of personal data when it is collected in 'layers', from the minimum to more or detailed information. Online forms and telephone numbers used by customers have appropriate privacy notices. All privacy notices are reviewed at least annually.
Monitor Data Quality Develop policy and guidance on data quality, with training for staff to understand and apply. Log and investigate incidents of inaccuracy and make provision for spot checks and self-audit.