

KEY ROLES INVOLVED IN INFORMATION GOVERNANCE

- The **Corporate Risk Manager** is responsible for maintaining the Corporate Risk Register and managing the council's strategic risks. This includes strategic information risks identified by the Senior Information Risk Owner.
- **Information Asset Owners (IAOs)** (the Corporate Directors) are responsible for ensuring information assets within their services are properly recorded, documented and associated risks effectively managed. IAOs are supported by the Corporate Information Security Officer and Information Asset Administrators who manage individual information assets.
- The **Caldicott Guardian** (the Corporate Director for Social Care, Health & Wellbeing) as a champion and advocate for the privacy rights of individuals and is the senior responsible officer for protecting confidential information relating to an individual's health and social care. The CG is responsible for ensuring that the Caldicott Principles^[1] are applied to any handling, sharing or use of confidential information.
- The **Chief Information Officer (CIO)** (the Director of Infrastructure) provides vision and leadership in the development and implementation of the council's technology and commissioning strategy. The CIO understands how the strategic aims of the council may be impacted by technology and information system risks and ensures these are managed effectively.
- The **Corporate Information Security Officer** is responsible for the council's Information Risk Management Strategy and is accountable to the SIRO and CIO. The role provides expert advice on information risk and its management, including developing and implementing policies and procedures for legislative and regulatory compliance.
- The **Infrastructure Risk and Compliance Team's** responsibilities include performing Information Risk Assessments for new information systems and when changes are made to existing systems. The team also implement and maintain technical controls identified in risk assessments, internal audits or following incident investigations. The team maintain the council's Public Service Network (PSN) and Payment Card Industry (PCI) compliance, reviewing and monitoring technical controls and ensuring compliance with technical security standards, including CESG.
- The **Information Resilience and Transparency Team** reports to the Director of Governance and Law (SIRO) and is responsible for: Compliance with Data Protection, Freedom of Information and transparency legislation and statutory codes of practice; training, guidance and support to managers and employees; responding to requests for information; responding to Data Subject Access Requests; incident and breach management; safeguarding checks; Privacy Impact Assessments and Records Management.
- The **Records Manager** reporting to the IR&T Team Leader, is responsible for developing the council's information life-cycle and records management

^[1] <http://systems.hscic.gov.uk/infogov/caldicott>

policies, standards and practice. Providing expert advice and training to business managers, the Records Manager maintains the Corporate Information Asset Register for the SIRO and the council's Information Asset Owners together with maintaining records inventories and retention.

- **KCC Managers**, team leaders and supervisors are responsible for ensuring that staff are appropriately trained and adhere to the council's information governance policies. Contract managers (or managers with contract management responsibilities) are responsible for ensuring that contractors and commissioned service providers handle and protect our data and respect the privacy and confidentiality of our employees, residents and service users. Managers are responsible for ensuring that information is only disclosed or shared outside the organisation in a fair and lawful way and documented in accordance with relevant policies and procedures. (See [Management Guide No. 5 – Information Governance](#))