Data Protection

Overview & Scrutiny Committee
24 June 2014

Matt Scott
Chief Information Officer

Why Data Protection is Important

- Council manages information relating to residents, employees, businesses, visitors, suppliers, partners etc.
- Obligation to:
    - Protect personal information from being misused
    - Share personal information where appropriate to support functions
- Improved accuracy and relevance leads to improved decision making
- Poor management of personal information has serious reputational consequences
- Breaches can lead to enforcement action

Data Protection & Governance Structure

- Registered Data Controller - Z169787X
- Data Protection governed through the following
    1) Senior Information Risk Owner (SIRO) role
    2) Supported by Information Governance Manager
        - Provides advice/guidance on compliance with legislation
        - Manage DP complaints
        - Investigate breaches of Data Protection
    3) Caldicott Guardian
        - Responsible for all healthcare information managed by Council
    4) Information Assurance Group
        - Establish and maintain a strategy for Information Governance
        - Provide oversight of information management policies

Incident Management – Data Protection

- Formal breach notification procedures followed
- Mandatory online reporting of Adult Social Care and Public Health DP breaches
- Regular SIRO & Caldicott Guardian meetings to review open incidents
- Quarterly report to CMT of DP Incidents
- Serious breaches reported to Information Commissioner's Office (ICO)
- 2013/14 – 4 incidents reported to ICO

Data Protection Training

- Current provision reviewed and being relaunched
- Key areas for improvement identified:
    - Introduction of testing to monitor understanding of legislation
    - Targeted training for teams managing highly sensitive information
    - Communication of DP training material
    - Individual team briefings
- Raise awareness of DP responsibilities in managing data in key systems
    - CCMS (Framworki)
    - SWIFT
    - SAP

Data Protection and Members

- Members are Data Controllers for constituents' data
- All members should register with ICO
- Members have a legal obligation to manage personal information under their control
- Must ensure that all personal information – electronic or hard copy – is protected against loss or damage
- Best Practice advocated by ICO information security includes:
    - Encrypt all personal information
    - Do not share logins
    - Use strong passwords
- Data shared with Council becomes responsibility of Council as well.
- Changes to email protocol and supporting technology assist members to achieve these requirements

Information Governance Roadmap

Data Sharing

•Closer working relationships with external bodies leading to increased information sharing

•Register of data sharing agreements being developed

Compliance Framework

•CBC committed to improving Information Governance to meet compliance with NHS Information Governance Tool Kit to enable sharing with health partners

•CBC submitted March 2014

- Overall submission “positive” with IAG seen as “…appropriate structure to agree…Improvement Planning actions.”
- Improvement Programme being scoped to address key areas