Agenda Item No: **10**

Cabinet (Performance Management) Panel

23 February 2015

Report title	Information Governance Board – changes to membership and roles	
Decision designation	AMBER	
Cabinet member with lead responsibility	Councillor Paul Sweet Governance and Performance	
Key decision	No	
In forward plan	No	
Wards affected	All	
Accountable director	Kevin O'Keefe, Governance	
Originating service	Democracy	
Accountable employee(s)	Adam Hadley Tel Email	Group Manager - Democracy 01902 554026 adam.hadley@wolverhampton.gov.uk
Report to be/has been considered by	N/A	

Recommendation(s) for action or decision:

The Cabinet (Performance Management) Panel is recommended to:

1. Agree the revised membership for the Information Governance Board (appendix A) and the additional role description for the Chief Cyber Officer (appendix B).
2. Amend accordingly the terms of reference for the Information Governance Board and the associated definitions, roles and responsibilities as agreed by the Cabinet (Performance Management) Panel on 15 September 2015.

1.0 Purpose

1.1 This report is presenting revised membership of the Information Governance Board and the role description for the Chief Cyber Officer.

2.0 Background

2.1 On 15 September 2014 the Cabinet (Performance Management) Panel agreed the new terms of reference and definitions, roles and responsibilities for the Information Governance Board.

2.2 Given the recent senior management restructure the Council has agreed there is a need to revise the membership of the Information Governance Board.

2.3 With cyber security becoming a more prevalent issue within Information Governance there is a need to outline the definition and role for the Chief Cyber Officer.

2.4 The West Midland Pension Fund will become its own Data Controller from 1 April 2015 and as such will no longer be required to sit on the Council's Information Governance Board. The proposed membership reflects this.

3.0 Options

3.1 The proposals are attached as appendix A and B. In summary the proposals are to update the membership of the Information Governance Board in light of the senior management restructure and introduce a role description for the Chief Cyber Officer.

4.0 Financial implications

4.1 There are no financial implications arising from the recommendations in this report.

[GE/06022015/K]

5.0 Legal implications

5.1 The Council has a legal duty under the Data Protection Act 1998, Freedom of Information Act 2000 and Environmental Information Regulations 2004 to appropriately manage and protect information assets.

5.2 The integration of Public Health into the Council in April 2012 required the Council to provide assurance to the NHS that it had in place suitable Information Governance policies, procedures and processes.

5.3 Failure to effectively manage information governance could increase risk of exposure to fraud and malicious acts, reputational damage, an inability to recover from major incidents and potential harm to individuals or groups due to inappropriate disclosure of information.

5.4 The Information Commissioner has the legal authority to:

- Fine organisations up to £500,000 per breach of the Data Protection Act or Privacy & Electronic Communication Regulations
- Conduct assessments to check organisations are complying with the Act
- Serve Enforcement Notices and 'stop now' orders where there has been a breach of the Act, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law
- Prosecute those who commit criminal offences under section 55 of the Act
- Conduct audits to assess whether organisations processing of personal data follows good practice
- Report issues of concern to Parliament.

[RB/06022015/U]

6.0 Equalities implications

6.1 This report seeks to amend existing terms of reference. Therefore, there are no equalities implications.

7.0 Environmental implications

7.1 There are no environmental implications arising from this report.

8.0 Human resources implications

8.1 Within Information Governance there are key roles which have to be filled. These roles are identified within Appendix B along with the posts which fill them. These are:

Role	**Responsible Post**
Data Controller	Head of Paid Service
Senior Information Risk Owner (SIRO)	Director of Governance & Solicitor to the Council
Caldicott Guardian (Children's)	Service Director Children and Young People
Caldicott Guardian (Adults)	Service Director Older People
Qualified Person	Head of Paid Service
Public Interest Test	Director of Governance & Solicitor to the Council
Data Protection Officer / Deputy SIRO	Group Manager – Democracy
Chief Cyber Officer	Head of ICT
RIPA Senior Responsible Officer	Director of Governance & Solicitor to the Council
CCTV Senior Responsible Officer	Director of Governance & Solicitor to the Council

8.2 Where a post is vacant or the incumbent is unable to act the person undertaking that role shall be responsible.

9.0 Corporate landlord implications

9.1 There are no corporate landlord implications arising from this report.

10.0 Schedule of background papers

10.1 Cabinet (Performance Management) Panel – 15 September 2014

Appendix A

Information Governance Board Membership

Senior Information Risk Officer (also RIPA and CCTV Senior Responsible Officer) – Chair
Data Protection Officer / Deputy SIRO – Vice-Chair
Caldicott Guardian (Children's)
Caldicott Guardian (Adults)
Chief Cyber Officer
Service Director for City Environment
Head of Transformation
Head of Audit

Appendix B

Chief Cyber Officer

The Chief Cyber Officer works within an environment as defined by The Cyber Security Strategy of the United Kingdom, dated June 2009, that describes cyber space as that encompassing 'all forms of networked, digital activities; this includes the content of and actions conducted through digital networks.' It also states that 'the physical building blocks of cyber space are individual computers and communication systems … [which] fundamentally support much of our national infrastructure and information.'

Cyber space is a key enabler and therefore a critical asset. In The UK Cyber Security Strategy, dated November 2011, this is picked up as a Tier 1 threat: namely, hostile attacks upon UK cyberspace by other states and large scale crime. These strategies effectively say that we need to put in place measures to reduce the risk and impact of such attacks, i.e. we need to defend ourselves in cyber space.

The Chief Cyber Officer will:

- Provide subject matter expertise and advice to the Information Governance Board on a broad range of cyber risk and security activities including:
  - The collection of ICT tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and the information assets of the Council and users.
- Ensure that information from Government and across the IT industry regarding the identification of new threats and vulnerabilities is reliable, kept up to date and responded to appropriately;
- Oversee arrangements to ensure that IT network security risks in both on-going and planned operations, system developments and projects are properly considered;
- Provide expertise in support of the execution of actions designed to mitigate risks, strengthen defence and reduce vulnerabilities in the following key areas:
  - Home and Mobile Working
  - User Education and Awareness
  - Incident Management
  - Information Risk Management
  - Managing User Privileges
  - Removable Media Controls
  - Monitoring
  - Secure Configuration
  - Malware Protection
  - Network Security