Derby City Council

Personnel Committee
18 March 2015

ITEM 5

Report of the Assistant Director of Public Health

Information Governance Toolkit – Local Authority Requirements

SUMMARY

1.1 All bodies, including local authorities, processing the personal confidential data of citizens accessing health and adult social care services must complete and publish Information Governance (IG) Toolkit assessments.

1.2 To achieve the required 'Level 2' status, Derby City Council must meet and provide evidence across range of requirements.

1.3 Requirement number 12-147 requires that 'Employment contracts which include compliance with information governance standards are in place for all individuals carrying out work on behalf of the organisation'. To meet this all new and existing employment contracts must contain 'comprehensive information governance compliance requirements'.

1.4 Additionally, it is also required that all staff are informed of their responsibilities and the consequences of misconduct and that new staff 'are appropriately vetted and informed of their responsibilities regarding compliance with information governance standards'.

1.5 To achieve these requirements of the Council it is proposed that:

- a generic IG clause is added to the Council Employment Contract
- the organisational expectations of staff in relation to IG are incorporated within the staff induction programme
- completion of the induction programme and subsequent IG training are monitored and recorded at individual staff level.

1.6 It is proposed that the following is accepted as the IG clause for inclusion in the Council employment contract:

*"**Data Protection and confidentiality***

As an employee of Derby City Council you must be familiar and compliant with the principles of the Data Protection Act ensuring that personal information is collected, stored, processed and transferred in accordance with the Act; and with other obligations the Council has in respect of information security.

All Council staff are required to keep confidential all information and documentation relating to a client, a member of staff or the Council's business, which he/she comes

into contact with.

Failure to act in accordance with the Data Protection Act or disclosure of confidential information to any unauthorised person or persons will be considered as gross misconduct and may lead to disciplinary action.

1.7 The proposed clause was presented and approved at the Conditions of Service Working Party on the 9th January 2015.

1.8 A letter to all existing staff will be drafted outlining proposed amendment to employment contracts to include the suggested clause.

RECOMMENDATION

2.1 To approve the proposals set out in 1.5.

2.2 To approve the inclusion of the data protection and confidentiality clause (as set out in 1.6) in all Derby City Council employment contracts.

REASONS FOR RECOMMENDATION

3.1 To support Derby City Council in achieving its requirement to meet Level 2 of the Information Governance Toolkit.

SUPPORTING INFORMATION

4.1 Further information on the IG Toolkit can be found in Appendix 2.

OTHER OPTIONS CONSIDERED

5.1 No further options considered as compliance with the IG Toolkit is a requirement of the Council.

This report has been approved by the following officers:

Legal officer	Olu Idowu, Head of Legal Services
Financial officer	
Human Resources officer	Diane Sturdy, Acting Head of Service – Organisational Development, Employee Relations and Pay & Reward Strategy
Estates/Property officer	
Service Director(s)	Nick O'Reilly, Director of Information Systems
Other(s)	Richard Boneham, Head of Governance & Assurance Amanda Verran, Head of Business Support

For more information contact:	Alison Wynn, 01332 643106 alison.wynn@derby.gov.uk

Background papers: **List of appendices:**	None Appendix 1 – Implications Appendix 2 – About the IG Toolkit

Appendix 1

IMPLICATIONS

Financial and Value for Money

1.1 Serious information security breaches could result in financial penalty.

Legal

2.1 Local Authorities processing the personal confidential data of citizens accessing health and adult social care services must complete and publish Information Governance (IG) Toolkit assessments.

Personnel

3.1 All Council staff have a responsibility to collate, process and transfer personal information in line with the principles set out in the Data Protection Act and to keep confidential all information and documentation relating to a client, a member of staff or the Council's business. Failure to do so could result in disciplinary action.

IT

4.1 Appropriate IT security arrangements need to be in place to ensure compliance with the IG Toolkit.

Equalities Impact

5.1 None.

Health and Safety

6.1 None.

Environmental Sustainability

7.1 None.

Property and Asset Management

8.1 Information assets must have an assigned asset owner and must be appropriately managed and monitored throughout the organisation.

Risk Management

9.1 Compliance with the IG Toolkit will reduce organisational risk associated with information management and security.

Corporate objectives and priorities for change

10.1 Appropriate information management and security will support the effective delivery of corporate objectives and priorities.

Appendix 2

About the IG Toolkit

What is Information Governance?

Information Governance is to do with the way organisations 'process' or handle information. It covers personal information, i.e. that relating to patients/service users and employees, and corporate information, e.g. financial and accounting records.
Information Governance provides a way for employees to deal consistently with the many different rules about how information is handled, including those set out in:

- The Data Protection Act 1998.
- The common law duty of confidentiality.
- The Confidentiality NHS Code of Practice
- The NHS Care Record Guarantee for England.
- The Social Care Record Guarantee for England.
- The international information security standard: ISO/IEC 27002: 2013 and ISO/IEC 27001: 2013.
- The Information Security NHS Code of Practice.
- The Records Management NHS Code of Practice.
- The Freedom of Information Act 2000.
- The Human Rights Act article 8.
- The 'Report on the review of patient-identifiable information' (alternative title 'The Caldicott Report') and the 'Information: To Share Or Not To Share? The Information Governance Review (also known as Caldicott 2 Recommendations)

What is the IG Toolkit?

The Information Governance Toolkit is a Department of Health (DH) Policy delivery vehicle that the Health and Social Care Information Centre (HSCIC) is commissioned to develop and maintain. It draws together the legal rules and central guidance set out by DH policy and presents them in in a single standard as a set of information governance requirements. The organisations in scope of this are required to carry out self-assessments of their compliance against the IG requirements.

What are the information governance requirements?

There are different sets of information governance requirements for different organisational types. However all organisations have to assess themselves against requirements for:

- Management structures and responsibilities (e.g. assigning responsibility for carrying out the IG assessment, providing staff training, etc.).
- Confidentiality and data protection.
- Information security.

What is the purpose of the information governance assessment?

The purpose of the assessment is to enable organisations to measure their compliance against the law and central guidance and to see whether information is handled correctly and protected from unauthorised access, loss, damage and destruction.

Where partial or non-compliance is revealed, organisations must take appropriate measures, (e.g. assign responsibility, put in place policies, procedures, processes and guidance for staff), with the aim of making cultural changes and raising information governance standards through year on year improvements.

The ultimate aim is to demonstrate that the organisation can be trusted to maintain the confidentiality and security of personal information. This in-turn public confidence that 'the NHS' and its partners can be trusted with personal data.

Source: https://www.igt.hscic.gov.uk/resources/About%20the%20IG%20Toolkit.pdf