

Peterborough City Council
Strategic Governance Board



Information Governance

Document Properties	
Title	Corporate Information Governance : Progress update to SGB 02-Jun-10
Identifier	n/a
Author	C Taylor
Owner	D Baker
Subject	
Audience	SGB
Coverage	PCC
Protective Marking	Unclassified
Document Format	MS Word
Document Type	Progress Update Report

Approval			
Role	Name	Approved	Date
Author	C Taylor		
Assurance	D Baker/S Crabtree	Diane Baker	27 th May 2010
Sign-off	D Baker	Diane Baker	27 th May 2010

Version Control		
Version No.	Date Issued	Draft/Final
0.2		

Document History and Change Control	
Version No.	Summary of change(s)
0.2	Minor amendments to first draft

Information Governance

Corporate Information Governance Group (CIGG)

Update to Strategic Governance Board - 02/06/10

TERMS OF REFERENCE

The draft Terms of Reference for the Corporate Information Governance Group are submitted to the Strategic Governance Board for approval as set out below:

- To ensure that the Council has effective policies and management arrangements covering all aspects of Information Governance in line with the Council's overarching Information Governance Policy, i.e.
 - Openness
 - Legal Compliance
 - Information Risk
 - Information Quality Assurance
- To ensure that the Council undertakes or commissions annual assessments and audits of its Information Governance policies and arrangements.
- To establish an annual Information Governance Improvement Plan, secure the necessary implementation resources, and monitor the implementation of that plan.
- To ensure that the necessary mechanisms are put in place to handle reports into breaches of confidentiality and security and where appropriate undertake or recommend remedial action.
- To report to the Strategic Governance Board on Information Governance issues.
- To liaise with other Council committees, working groups and programme boards in order to promote Information Governance issues.
- The Group will meet a minimum of four times a year.

PROGRESS UPDATE

1. Where we are now

Policy work

An initial review of the existing policies relating to Information Governance has been conducted and, whilst we have found some excellent policies, we have also found some policies that:

- are out of date (e.g. email policy dated 1999);
- exist only in draft (ICT policy);
- contain factual inaccuracies (Records Management);
- have never been fully implemented (Data Quality).

This policy work is continuing and is a priority area for the group and in this context links have been made by the group to the:

- Strategy to Policy Project (Concept to Publish);
- Green Shoots Programme.

New policies have been drafted in relation to:

- Corporate Information Governance;
- Protective Marking;
- Email - use, retention and disposal;

Peer review of these policies is underway at the moment and these will be submitted to the full CIGG for review and sign-off prior to presentation to the relevant committees.

Committees and Standing Invitations

The group will be putting the new policies to the Audit Committee for approval and will also be extending a standing invitation to Councillor Seaton, as the Cabinet Member for Resources.

2. Where we want to be

In line with the recommendations originally made to the Strategic Governance Board:

- the Group is working towards the publication of a Peterborough Information Charter
- the decision made by Internal Audit to use the Information Assurance Maturity Model Framework has guided the group to use that Model and to:
 - achieve Level 1 of the Model by Apr 2011
 - aspire to achieve Level 2 of the Model by Apr 2012

Information Assurance Maturity Model Level 1

- **Description** : Initial awareness of the criticality of Information Assurance to the Business and its Legal Requirements
- **Requirement** : Main Board recognition that information is a vital business asset and that Information Assurance is an integral part of corporate governance. Board commitment to effective Information Assurance is promulgated in a top level policy statement. Appointment of a Senior Risk Owner on the Main Board and Information Asset Managers throughout the organisation, taking responsibility for their assets. Publication of an Information Charter

3. How we are going to get there

An outline timetable of activities and the initial approach to be taken has been developed and is attached at Annex 1.

4. What the benefits are

The introduction of Corporate Information Governance will contribute to the Council's performance in the following areas:

- **Governing the business**
 - i. Does the organisation produce relevant and reliable data and information to support decision making and manage performance
 - ii. Does the organisation promote and demonstrate the principles and values of good governance
 - iii. Does the organisation manage its risks and maintain a sound system of internal control
- **Managing resources**
 - i. Does the organisation manage its assets effectively to help deliver its strategic priorities and service needs

5. How we will know we have got there

Internal Audit has adopted the Information Assurance Assessment framework as the tool to measure the Council's progress.

Information Assurance Maturity Model

Level 1 – Initial Awareness of the Criticality of IA to the Business and Legal Requirements			
<i>Embedding Information Risk Management (IRM) Culture Within organisation</i>			
1. Process : Leadership & Governance	Due date	Progress	Status
1.1 Main Board recognition that information is a vital business asset and that IA is an integral requirement of corporate governance	Jul-10	g	Strategic Governance Board have set-up a sub-group to progress Corporate Information Governance
1.2 Board commitment to effective IA is promulgated in a top-level policy statement	Jul-10	a	Information Governance Policy now in draft form and currently out for peer review before wider consultation
1.3 Appointment of a Senior Information Risk Owner at CMT level	Aug-10	r	Likely to be part of an existing post - recommendation to be made by CIGG and approval to be given by CMT
1.4 Appointment of Information Asset Owners throughout the organisation taking responsibility for their assets.	Jul-10	r	Likely to be a new network appointed by CMT
1.5 Publication of an Information Charter	Aug-10	g	Work on this has started and is progressing
2. Process : Training, Education & Awareness			
2.1 A programme of annual information risk awareness training is instituted for all who have access to personal data within the organisation its delivery partners and 3rd party suppliers.	Sep-10	r	Corporate policies will be reviewed to ensure that they cover Information Risk. Necessary changes will be made and the new policies will be published on In-Site. Information Risk is likely to become a specific item within the Council's overall approach to corporate Risk Management. The CIGG will work with HR, Comms, the Risk Manager and individual Service areas to ensure that policies are aligned and induction and ongoing training is available in relation to Information Risk.
2.2 A organisational cultural change plan is implemented	TBA	r	Requirement to be assessed. This could be approached through Business Transformation and the roll-out of projects such as EDRM and the Digital mailroom

3. Process : Information Risk Management				
3.1	A comprehensive information risk policy is in place. The organisation's information risk appetite is clearly articulated	Jan-11	r	Not yet started
3.2	Information risks with appropriate owners and managers are identified within risk registers at the strategic level.	Jan-11	a	Existing Risk Register needs to be considered as a potential mechanism for this.
3.3	All new IS are subject to an effective accreditation process, where appropriate Privacy Impact Assessments are used and effective contract mechanisms are used to apply IA through life.	Apr-11	a	This is partial at the moment but a policy is planned
3.4	The organisation's approach to addressing information risks is agreed with the organisation's external stakeholders, where applicable	Apr-11	r	Yes in principal once the Council has formed an initial position then this will be shared and agreed with partners and stakeholders. Information Sharing Protocols are to be developed - Green Shoots is an example of where this requirement is pressing.
Implementing Best Practice IA Measures				
4. Process : Through-Life IA Measures				
4.1	The requirement for taking a coordinated and systematic approach to through-life IA measures is understood and plans exist to determine the status of existing IS.	Apr-11	r	IS Information Risk policy to be developed
4.2	All new IS are subject to through-life IA measures to deal with the full range of vulnerabilities and threats to information, including those arising from	Apr-11	g	IS Information Risk policy to be developed
☐	personnel behaviour,	Sep-10	a	Policy to be developed
☐	business process,	Sep-10	a	Policy to be developed
☐	natural disaster,	Nov-10	a	Policy to be developed
☐	malicious intent and	Nov-10	a	Policy to be developed
☐	obsolescence.	Nov-10	a	Policy to be developed

4.3	The organisation has a Forensic Readiness Policy.	TBA	r	Requirement to be assessed
4.4	Implementing Best Practice IA Measures	Dec-10	r	To be defined
5. Process : Assured Information Sharing				
5.1	The requirements for sharing information across the organisation's boundaries are identified and arrangements are in place to work with external stakeholders to achieve shared IA objectives.	Aug-10	g	This work has commenced
5.2	The need to understand and control how IS interact with one another both internally and externally is acknowledged and work to implement IA control mechanisms is implemented.	Aug-10	g	This work has commenced
Effective Compliance				
6. Process : Compliance				
6.1	A compliance regime is established to confirm the effectiveness of IRM against mandated minimum standards.	Sep-10	g	Currently being developed by Internal Audit
6.2	The Board's Audit Committee ensures that it receives comprehensive assurance on IRM and challenges assurance, where required.	Sep-10	g	Currently being developed by Internal Audit
6.3	The organisation reports annually on IA issues.	Apr-11	r	To be achieved as a part of the Council's overall approach to Risk Management