ITEM 9

NORTH YORKSHIRE COUNTY COUNCIL

AUDIT COMMITTEE

19 APRIL 2012

INFORMATION GOVERNANCE

Report of the Corporate Director – Finance and Central Services

1.0 PURPOSE OF THE REPORT

1.1 To update Members on the progress made to date in respect of improving the effectiveness of the Information Governance arrangements in the County Council.

2.0 BACKGROUND

2.1 The County Council is committed to developing a comprehensive and effective policy framework covering all aspects of Information Governance (IG). A Framework has been developed within which new or emerging issues can be identified and then addressed systematically. This Framework reflects Government requirements as set out in various policy and guidance documents. Work is also continuing to address a number of interlinked issues, as set out in this report.

2.2 For practical purposes, IG reporting to this Committee is categorised into five principal strands as follows:

(a) **Information Governance Framework**

This addresses the overall management and development of IG arrangements at a corporate, managerial and operational level across the County Council. Updates are provided on how the County Council is progressing with the implementation of the overarching IG Policy and Strategy.

(b) **Information Security**

This considers the adequacy of the County Council's arrangements for protecting personal and sensitive data in accordance with the principles of the Data Protection Act 1998 and guidance issued by the Information Commissioner's Office (ICO). Information Security also encompasses the ISO 27000 series of international quality standards which detail the key requirements that the County Council must fulfil in order to provide assurance that the necessary process controls are both in place and effective.

(c) **Compliance**

This considers the legal framework and the standards that need to be established to ensure that data and information management throughout the County Council is conducted within the relevant legislative parameters (e.g. Data Protection, FOI). This section will also provide feedback from compliance audits, undertaken by Veritau auditors, to assess the degree to which the directorates and service areas are complying with the principles detailed within the IG Framework.

(d) **Information Quality**

This set of requirements covers the need to ensure the quality, accuracy, currency and other characteristics of information, which is held, used or issued.

(e) **Records Management**

This is the process of creating, describing, using, storing, archiving and disposing of records according to a pre-defined set of standards.

2.3 The following paragraphs provide an update of progress within the County Council in relation to each of the above areas, since the last report to this Committee on 8 December 2011.

3.0 INFORMATION GOVERNANCE FRAMEWORK

3.1 The IG Framework has been developed to incorporate the core measures identified in the Government's Data Handling review, the HMG Security Framework and ISO 27001. It is intended that, within this Framework, all the County Council's policies, protocols and guidance notes relating to IG can be developed in a way that is both comprehensive and complementary to each other. The objective of the Framework is to set out how the County Council will improve its information management by establishing:

- core measures to protect personal data and other information across the County Council
- a culture that properly values, protects and uses information
- stronger accountability mechanisms within the County Council
- stronger scrutiny of performance in relation to the above

3.2 Management Board approved the overarching Information Governance Policy and Strategy in March 2010 and nominated the Corporate Director – Finance and Central Services as the County Council's Senior Information Risk Owner (SIRO). A copy of the Information Governance Strategy was presented to Members of this Committee at its meeting in April 2010.

3.3 A feature of the Strategy was a 'world map' of the various IG policies that would be required and how they interrelate. The latest version of this 'world map' is attached as **Appendix 1** for information.

Corporate Information Governance Group

3.4 As the County Council's SIRO, the Corporate Director – Finance and Central Services, chairs the Corporate Information Governance Group (CIGG2), which addresses new and emerging issues as well as coordinating the development of the IG Framework.

3.5 The role of CIGG2 is to:

- develop the necessary corporate IG policies
- coordinate and approve corporate IG standards for the mitigation of risk
- monitor compliance with the Information Assurance Assessment Framework
- establish a policy for reporting, managing and recovering from information risk incidents
- provide and maintain mechanisms that command the confidence of individuals through which they may raise concerns about information risk to senior management or the Audit Committee

3.6 CIGG2 includes representatives from all Directorates as well as 'advisers' from areas such as IT, HR and Legal. It has met regularly in order to establish momentum to the IG process.

3.7 Notes of the two most recent meetings are attached at **Appendices 2** and **3** respectively. Attachments to these reports have not been provided. If Members require more detail on any particular topics, then this can be provided on request.

3.8 The main actions since the last report to this Committee on Information Governance are as follows:

- Directorate Information Governance Champions (DIGCs) are continuing to proactively promote the IG agenda within their directorates. Further detail of the progress made by the individual DIGCs was provided in their annual reports submitted to the Audit Committee in December 2011
- approval of a security classification system for records, documents and information assets
- further refinement of the information asset registers within directorates including the application of the security classification system (see above) so that records can be prioritised for IG purposes
- continuation of the programme of unannounced audit visits to County Council premises to assess information security arrangements
- ongoing development of policies and documentation to enable implementation of the IG Framework and ISO 27000
- review of the NYCC training needs for IG to target training more closely on the needs of various staff groups, and
- ongoing development of a revised process for reporting and reviewing information security breaches within NYCC.

The Role of Veritau

3.9 Staff from Veritau support the development and implementation of the IG Framework by:

- preparing and/or advising on corporate IG policies prior to their submission to CIGG2
- supporting and coordinating the roll out of the policy framework across the County Council, and
- raising awareness and promoting compliance via training, guidance and advice.

3.10 Earlier in the year, Veritau's auditors carried out a review of arrangements within the County Council against the Information Governance Maturity Model and reported the results to the SIRO. The results of this review have provided a "road map" to help the County Council achieve Level 2 maturity. The Internal Audit Plan for 2012/13 (see **Agenda Item 4**) also includes a programme of unannounced visits by Veritau auditors to premises to confirm compliance with information governance policies.

4.0 INFORMATION SECURITY

External Factors

4.1 The Information Commissioner's Office (ICO) has the power to fine organisations up to £500,000 for serious data breaches or losses. Since the last report to the Committee in December 2011, the ICO has imposed the following fines:

- £140,000 against Midlothian Council for disclosing sensitive personal data relating to children and their carers to the wrong recipients on five separate occasions
- £80,000 against Cheshire East Council for failing to take appropriate measures to ensure the security and appropriateness of disclosure when emailing personal information
- £80,000 against Norfolk County Council for disclosing information about allegations against a parent and the welfare of their child to the wrong recipient, and
- £100,000 against Croydon after a bag containing papers relating to the care of a child sex abuse victim was stolen from a public house.

4.2 Other breaches by local government bodies reported by the ICO have included:

- Basingstoke and Deane Borough Council - breaches on four separate occasions during a two month period in 2011 including an incident in which an individual was mistakenly sent information relating to 29 people who were living in supported housing

- Brighton and Hove Council - an employee emailed the details of another member of staff's personal data to 2,821 council employees. A third party also informed the ICO of a historic breach which occurred in May 2009 when an unencrypted laptop was stolen from the home of a temporary employee.
- Craven District Council - the theft of an unencrypted laptop containing a database with child swimming lesson details for 2,300 individuals. The laptop was stolen from a ground level office at the Aireville Swimming Pool, Skipton. This office is protected by several security devices and the police attended the scene within minutes of the office being entered. However the intruder was able to immediately remove the laptop and escape just as the police arrived. This was because the laptop had been left unsecured on a desk in a position where it could be seen from outside the office.

4.3 Within NYCC there have been seven reported incidents over the last two months, including three cases of failure to "blind copy" customers' email addresses, thus disclosing the recipients to everyone else; one client file lost; and three inappropriate disclosures, one involving confidential information and perhaps requiring notification to the Information Commissioner. Given the "sensitive" content of some of these breaches, further details will be reported at the meeting.

What the County Council is doing to protect its information

4.4 The Information Governance Officer (IGO) (Veritau) and the Council's Information Security Officer (ITSO) continue to work together to ensure that the County Council's systems for reporting and investigating data security breaches are consistent and operate effectively. This includes the approval by CIGG2 of a procedure for investigating and reporting incidents, including escalation to the SIRO, possible external reporting (ie to the ICO) of the most serious incidents (none has been reported yet) and the development of an electronic system for recording and investigating breaches which will be accessible by authorised Council staff.

4.5 NYCC's ICT Services is one of only 10 councils to hold ISO IEC 27001 certification. The County Council have also been certified under section 4.2 of the Government Connect Code of Connection (Government Secure Internet).

4.6 The ITSO has primary responsibility for ensuring that the County Council has adequate electronic security arrangements in place. These include:

- 'port blocking' to ensure that only hardware encrypted devices (as issued by ICT) can be connected to the County Council's USB ports
- routine monitoring of the use of IT to ensure that the County Council's data security policies are adhered to
- carrying out investigations where "technical" breaches are detected, and
- acting as an expert witness at disciplinary panels.

4.7 Members should note that, although the above controls address the risk of unauthorised disclosure of electronic data, the risk of disclosure also applies to papers records (see **paragraphs 4.1 and 4.2** above for examples from other authorities).

5.0 COMPLIANCE

5.1 Veritau's auditors have not carried out any further unannounced visits to County Council premises since the report to the Audit Committee in December 2011. Further data security compliance visits are scheduled for the 2012/13 financial year and have been included in the Internal Audit Plan (see **Agenda Item 4**).

Freedom of Information Act 2000

5.2 Since 1 January 2005, all information held by the County Council must be disclosed to anyone who submits a written request for it, unless an exemption as defined in the Act applies. The Act applies only to written requests for information (but includes e-mail). Requests must be answered within the statutory 20 working day time frame.

5.3 Between 1 April 2011 and 31 March 2012, the County Council received a total of **1103** FOI requests. This compares with **1096** received between the same period in 2010/11 and **826** received in 2009/10 (an increase in workload of almost **34**% since 2009/10). The County Council has responded to 98% of these requests within the 20 working days time frame defined by the legislation (compared to a performance target of 95%).

5.4 Two important changes to the FoI are included in the Protection of Freedoms Bill (PoF) currently at committee stage in the House of Lords. These proposed changes are as follows:

- the extension of FoI to companies owned by local authorities- this would include Veritau and Veritau NY, Yorwaste, and NYnet
- an obligation to make available "datasets" of unprocessed ("raw") data, created in the course of County Council activity and which would not be exempt under FoI. The intention is to stimulate innovation and economic activity by removing barriers to commercial exploitation

The first proposal does not mean any significant change for the County Council since a lot of the information held by the County Council's owned companies was already subject to disclosure. The change relates instead to the 'internal' information which might be held by these companies. The second proposal will require some additional work to identify, prepare and publish the required datasets. However, it is not yet clear how much private sector interest might be generated should this proposal be implemented.

6.0 RECORDS MANAGEMENT

6.1 Records management is concerned with the application of systems and processes to control access, retention and disposal of records in accordance with ISO 15489 and Lord Chancellor's Code of Practice on the Management of Records under Section 46 of the Freedom of Information Act 2000.

6.2 The Records Management Service manages in excess of 20,000 boxes of semi active and inactive paper based records, controlling access and applying the County Council's retention policy to these records. It also hosts the central scanning bureau which transfers paper records to digital format. The County Record Office has been approved as a 4 star record office by The National Archives, placing it in the top 6, nationally for the provision of archival services.

6.3 Efficient utilisation of the storage capacity at the Record Office relies on a balance between the respective volume of incoming files and those that pass their retention date. At present, a backlog of disposals has developed which is being actively addressed. Until this is resolved, the Record Office has only a limited ability to receive incoming files for storage. The Record Office is therefore looking at the possibility of securing off-site "deep storage" because the forecast is that the current storage will be insufficient within the next 6 to 12 months.

6.4 To assist the County Council achieve efficient records management, the Records Management Service is positioned within the existing Information Governance corporate structure. The RM attends CIGG2 and works closely with the EDRMS (HR) Project and the Veritau IGT in order to:

- develop records management strategy and policy;
- agree the format and content of information audits;
- develop file plans;
- support the implementation of the HR EDRMS project; and
- review and update the corporate records retention and disposal schedule.

7.0 PRIORITIES FOR THE NEXT SIX MONTHS

7.1 The following have been identified as priority tasks for the next six months: -

(a) implement the revised e-learning training package for employees

(b) complete the development of a new electronic system for monitoring and recording data security breach investigations

(c) ensure information asset registers have been completed for all Directorates with their accompanying security classifications

(d) address the storage issues at the Record Office.

8.0 RECOMMENDATION

8.1 Members are asked to note the progress made on information governance issues to date.

JOHN MOORE
Corporate Director - Finance and Central Services

County Hall
Northallerton

10 April 2012

Background Documents

Contact Roman Pronyszyn, Client Relationship Manager (extension 2284).

Report prepared by Roman Pronyszyn, Client Relationship Manager and presented by John Moore, Corporate Director - Finance and Central Services.

Appendices

The following appendices are attached to this report:

Appendix 1 – Information Governance ‘World Map’
Appendix 2 – Minutes of the CIGG2 Meeting 11 January 2012
Appendix 3 – Minutes of the CIGG2 Meeting 14 March 2012

<table>
<tr><td rowspan="2"><b>IG policy map as at
MARCH 2012</b></td><td colspan="5"><b>Information Governance Policy</b></td></tr>
<tr><td colspan="5"><b>Information Governance Strategy</b></td></tr>
<tr><td><b>1a: DP Policy UP</b></td><td><b>1b: FoI Policy UP</b></td><td><b>2: Information Security Policy UP</b></td><td>3: <i>Data Quality Policy</i> U</td><td><b>4: Records Management Policy UP</b></td></tr>
</table>

<table>
<tr><td rowspan="2"><b>1a, 2</b>
Monitoring Policy
Gov Connect Usage Policy P
<b>Internet Usage Policy UP</b>
<b><i>Info Security Incident Policy/Procedure UP</i></b>
<b>Portable Media</b></td><td><b>1a&b, 2</b>
<b><i>Charges for enquiries U</i></b></td><td><b>2,3</b>
Network Access Policy
<b>Use of Social Media Policy UP</b>
<b><i>External cyber bullying & internet harassment policy & guidance</i></b></td><td><b>4</b>
Records and Retention Disposal Schedule P
<b><i>Information Audit Survey</i></b>
<b>Scanning Policy P</b></td></tr>
<tr><td rowspan="2"><b>2</b>
Software Policy P
Information Security Management Standard - ISMS (suite of technical IT policies)
<b>Anti Virus Policy P</b></td><td><b>2, 3, 4</b>
Service Continuity Management Policy</td><td><b>1a/b, 4</b>
<b><i>Email Archiving Policy</i></b></td></tr>
<tr><td><b>1a, 2, 3</b>
<b>Data Processing (by Contractors) Policy UP</b></td><td colspan="2"><b>1a/b, 2, 3, 4</b>
<b>Information Sharing with Partners Policy UP</b></td></tr>
<tr><td><b>1a 2, 4</b>
<b>Privacy Statement (Customer Service Centre) [call recording] U</b></td><td colspan="3"><b>1a/b, 2, 4</b>
<b><i>Computer, Telephone & Desk Use Policy</i></b>
<b><i>Security classification Policy (was “marking”) UP</i></b>
<b><i>Mobile Phones policy</i> (was Blackberry Policy)</b>
<b>Remote Working Policy P</b>
<b>Email Policy UP</b></td></tr>
</table>

Items in bold have been approved by CIGG2
Items in *bold italics* are under discussion within CIGG2
All other items are still to be drafted and presented for discussion

U union consulted
P on Intranet

APPENDIX 1

Changes since November 2011:
Monitoring Policy currently under discussion
External cyber bullying & internet harassment policy & guidance added
Mobile Phones still under discussion (ie re-italicised)

APPENDIX 2

Corporate Information Governance Group 2

Meeting 13

11 January 2012 @ 2pm in Meeting Room 2

Attendees:

John Moore (JSM)	-	Senior Information Risk Owner and Chair	
Fiona Sowerby (FS)	-	Head of Risk Management & Insurance, Secretary to Group	

Champions

Sukhdev Dosanjh (SD)	-	DIGC HAS	
Kevin Tharby (KT)	-	DIGC CYPS	
Shaun Lee (SL)	-	DIGC FCS	
Joel Sanders (JL)	-	DIGC BES	
Helen Edwards (HE)	-	DIGC CEG	

Advisers

Moira Beighton (MB)	-	Legal	***Apologies*** (IE as sub)
Isabel Esteves (IE)		Legal	
Kelly Hanna (KH)	-	HR	***Apologies***
Roman Pronyszyn (RP)	-	Audit & Information Assurance Manager, Veritau	
Robert Beane (RB)	-	Information Governance Officer, Veritau	***Apologies***
Louise Jackson (LJ)		Information Governance Support Officer, Veritau	
Colin Cottrell (CC)	-	Information Security Officer	
Ian Kaye (IK)	-	Records Manager	
Janice Williams (JW)	-	eDRMS Project Manager	***Apologies***
Simon Wright (SW)	-	Senior Emergency Planning Officer	***Apologies***
Phil Jones (PJ)	-	Property	**Not present by agreement with JSM**

cc	Tracy Harrison	-	BES
	Robin Mair		CEG
	Keith Sweetmore	-	CEG
	Maureen Howard	-	HAS
	Dawn Ross		HAS
	Max Thomas	-	Veritau

ACTION NOTES

Item No	***Item***	***Action By***
PART A	**FORMALITIES / STANDING ITEMS**	
1	**Introductions and Apologies** Introductions – Louise Jackson was introduced to the Group. Apologies - see above.	
2	**Future meetings** all Wednesdays **2012 dates** 14 March 2012 @ 2.00pm **23 May 2012 @ 2.00pm**	

Item No	*Item*	*Action By*
PART B	**ACTION PLAN**	
3	**Roll out Plan**	
3.1	**Update on Progress of Plan (including Information Charter)** RP advised that many of the actions on the Plan have been completed and are highlighted in grey. He then took the Group through the outstanding actions to find out their present position. These items included: • Approval of various policies by Management Board – it was agreed that the process involved approval by CIGG2 rather than Management Board. • Access Control/Authentication Physical Policy – this relates to Access Control and is presently on hold. • Review/update Records and Retention Disposal Schedule – IK confirmed that this has been restructured and re-done. A discussion took place around linking this Schedule with the Information Asset Register. It was agreed that DIGCs would take the initiative on this and IK will audit occasionally. • Various training requirements – RP will link these targets with the work being carried out on staff awareness and training and develop a training plan with DIGCs. • Technical and non technical security breach reporting etc. – CC/JSM are preparing a report for Management Board. • Information Charter – RP to provide draft for JSM. • Information Governance Risk Register – first prep meeting between RP/FS on 30 January 2012. • Use of IT Equipment Policy and Remote Working Policy – in progress. • Schedule of penetration testing – CC confirmed that this is done regularly and reports are provided to TWIG. • Issues relating to CCTM – CC to advise RP. • NEGWARP membership – CC to discuss with RB. **Action:** RP to update Action Plan as discussed and as above and provide a revised version to the next meeting.	**RP**
3.2	**Staff Awareness and Training** - **SIRO/DIGCs training – feedback** Training arranged for 20 January 2012. A discussion took place around the expected outcomes including the IT system/shared facility that will be a log of recorded breaches etc. It was suggested that the database should not be complicated but effectively be a recording sheet for the breaches and their position in the process.	

Item No	***Item***	***Action By***
	Action: Training session/workshop to provide the following outcomes: A notification procedure/workflow chart agreed with DIGCs. An agreed specification for an IT system/shared facility that will show a log of recorded breaches and their investigation process, and provide a single record of a breach that can be accessed in a controlled way.	**RP/RB**
	- **training within the Directorates incl e learning** **Directorates** BES – JS presented a paper showing the implementation of information governance training across BES. He confirmed that this has been signed off by BES management team. FCS – SL advised that FCS management team have agreed what mandatory information governance training will be done by which staff groups depending on what is relevant to their job role. CYPS – KT advised that mandatory information governance training will take place across the Directorate and be a mixture of both long and short courses depending on job roles. HAS – SD advised that information governance training is still to be scoped across the Directorate. CEG – HE advised that needs have been partially identified and the exercise will be completed by 20 January 2012. **E learning** RP presented the draft 20 minute e learning module for data protection and information security. DIGCs were asked to provide comments on the module including the content, length and any amendments. It was suggested that DIGCs comments should be provided by end January 2012 to RP/RB. Following this, RP/RB will refer the module to the e learning development unit. HE will assist in this.	
	Action: **Directorates:**	
	SD to scope information governance training requirements across HAS's staff groups.	**SD**
	HE to complete the scoping of information governance training requirements across CEG staff groups.	**HE**
	E learning:	
	DIGCs to provide comments on the 20 minute data protection and information security module to RP/RB by end of January 2012.	**DIGCs to RP/RB**
	RP/RB to liaise with the e learning development unit to transfer the module onto the Learning Zone.	**RP/RB**

Item No	Item	Action By
	- **training log**	
	Carried forward to next meeting.	**JSM**
3.3	**Information Audits – progress to date**	
	DIGCs provided details of progress on Information Audits as per the Action Log. CYPS still has some work to do before information audits are completed. BES has completed information audits but is reviewing Economic Partnership Unit's audit. CEG information audits are complete and are awaiting quality assurance. HAS still has some work to do before information audits are completed. FCS information audits are being reviewed following quality assurance. RP advised that RB has discussed the information audits with all Directorates. Discrepancies have been found and it will be necessary to discuss further and decide upon actions to remedy this.	
	Action: DIGCs to continue to complete and review information audits following quality assurance.	**DIGCs**
	RP/RB to continue quality assurance and find solutions for the discrepancies found during quality assurance.	**RP/RB**
3.4	**External cyber bullying/internet harassment**	
	- **policy and guidance – update on World Map** Noted.	
	- **verbal harassment of staff by staff** The article was published for all staff on the intranet on 1 December 2011 and the Social Media Policy has been updated.	
4	**Communication Issues**	
4.1	**Updated World Map**	
	Noted. IK advised that the Trade Unions have been consulted on the Records Management Policy and this should be noted on the Map.	
	Action: RB to amend the World Map to show that the Trade Unions have been consulted on the Records Management Policy.	**RB**
4.2	**Posters**	
	HE explained the background to this item and mentioned KT's suggested 'dos and don'ts'. HE confirmed that the posters would be issued in installments. The Group suggested the following: • The consequences should be shown on the poster, for example, state that there will be a fine. • The posters should be customised for particular staff groups.	

Item No	*Item*	*Action By*
	• The posters should be available to place on doors, filing cabinets as well as electronically. • The small steps/big difference note when logging in to a computer should be replaced with an information governance promotion. JSM suggested HE talks to FS if a budget is required. HE confirmed that she will circulate amended messages/posters for comment and feedback. HE will then start the publicity/poster campaign.	
	Action: HE to circulate amended messages/posters for comment and feedback.	**HE/ALL**
	HE to start publicity/poster campaign.	**HE**
4.3	**Any other issues to be clarified/raised?** None.	
5	**Information Security**	
5.1	**Internet Issues – update** CC advised that detailed information on internet issues continue to be provided to Assistant Directors with anonymous notifications being provided to DIGCs.	
5.2	**Details of latest Breaches - internal and external** **Internal** Noted. CC advised that these include identity issues and use of non NYCC USB sticks. **External** Noted. CC advised that the NHS have blocked all access other than through NHS encrypted equipment. SD advised that requirements will need to be scoped within HAS in view of the forthcoming developments for HAS with the NHS.	
5.3	**SIRO breaches** ➢ **SIRO/DIGC workshop on 20 January 2012** see item 3.2 above. ➢ **Notification procedure** see item 3.2 above. ➢ **shared facility showing a log of recorded breaches and their investigation process** see item 3.2 above. ➢ **handling of Subject Access Requests** Carried forward to next meeting.	
	Action: Put on next meeting's agenda.	**JSM/FS**

Item No	Item	Action By
6	**Records Management**	
6.1	**Records and retention issues in Customer Services - update**	
	IK advised that meetings have taken place with the Customer Services team to look at the 'journey of data' held. IK will continue to progress this and report again to the next meeting.	
	Action: IK to continue to work with the Customer Services team and report progress to the next meeting.	**IK**
6.2	**Records and retention schedule - update**	
	See also item 3.1. A discussion took place around linking this Schedule with the Information Asset Register. It was agreed that DIGCs would take the initiative on this and IK will audit occasionally.	
	IK also advised that further work is required on the Schedule to co-ordinate the corporate advice with existing advice given on retention by CYPS and HAS. Also, CYPS and HAS Directorate retention schedules need to be included into the corporate Schedule.	
	Action: DIGCs will take the initiative in linking the Records and Retention Schedule to the Information Asset Register and IK will audit occasionally.	**DIGCs and IK**
	IK to carry out further work with CYPS and HAS to align advice and schedules within Directorates with the corporate advice and Schedule.	**IK**
6.3	**Publication Scheme - update**	
	RP advised that the update of the Scheme is in progress and will include issues arising out of the Data Transparency Code.	
	Action: RP will continue to advise progress on the update of the Publication Scheme.	**RP**
PART C	**POLICY DEVELOPMENT**	
7	**Set 5**	
7.1	**Security Classification Policy – deferred until March 2012**	
	Deferred until March 2012 meeting.	
7.2	**Information Enquiry Charges Policy**	
	Deferred.	
8	**Set 6**	
8.1	**Computer, Telephone and Desk Use Policy on World Map?**	
	Complete.	

Item No	*Item*	*Action By*
9	**Set 7**	
9.1	**E Mail Archiving and File Management Policy**	
	➢ **progress report on electronic document storage including emails**	
	CC advised that Quest is being used effectively. However some comments suggested that the Search facility is not as good as previously on Groupwise. This could be a potential training issue and CC will look into this and put on the next TWIG agenda for discussion.	
	JSM advised that Dave Sadler is to develop an E Mail/File Management Policy; CC will advise him.	
	Action: CC to put training on Quest on the next TWIG agenda for discussion.	**CC**
	CC to advise Dave Sadler that an E Mail/File Management Policy needs to be developed.	**CC/Dave Sadler**
	➢ **Named (P) drive analysis**	
	CC advised that the Named drive analysis has not been produced due to the current migration. This will be forwarded to relevant DIGCs when migration is complete and a review has been done to ensure the information is accurate.	
	Action: CC will forward the Named drive analysis to DIGCs as soon as the migration has been completed and he is sure the information is accurate.	**CC**
10	**Other Policies to be Considered?**	
10.2	**Any Others?**	
	None.	
PART D	**OTHER MATTERS**	
11	**Remote/Flexible Working – sensitive/non sensitive data**	
11.1	**Guidance Note on Remote/Flexible Working relating to Sensitive/Non Sensitive Data – update**	
	Awaiting the outcome from the Property One Council work stream.	
	Action: JSM to advise the outcome from the Property One Council work stream.	**JSM**
11.2	**Domestic PCs, web access and related issues – technical constraints versus policy adherence versus legal position**	
	JSM/RP/CC advised that there has been a raft of breaches to the Information Governance policies that are in force. JSM further explained that it is possible to detect who is logged in via a home computer and stop files (sensitive or otherwise) being transferred to home PCs via Outlook Web Access.	

Item No	*Item*	*Action By*
	SD/IE advised that when logging on to a home computer you are given the option to confirm that your manager has authorised unrestricted work. However it is thought that some employees are taking this option but they have not been authorised by their managers. JSM advised that he would like to take a report to Management Board explaining the position and provide a sample of the extent of the breaches. Management Board can then either decide whether the practice should be stopped and necessary staff provided with NYCC equipment or whether Management Board is prepared to accept the risk. JSM will copy the report to DIGCs when it is ready. **Action:** CC/RB to continue to collect data relating to breaches and provide information to JSM. JSM to produce a report for Management Board's consideration to determine whether the practice of working on home PCs should be stopped and necessary staff provided with NYCC equipment or whether Management Board is prepared to accept the risk of breaches. JSM will provide a copy of the report to DIGCs.	**CC/RB** **JSM**
12	**Local scanning arrangements**	
12.1	Local scanning update Carried forward to next meeting.	**JW**
12.2	Ad hoc local scanning IK advised that there have been various queries relating to the scanning of documents. He further advised that the Scanning Policy needs to be amended to define and allow 'ad hoc' scanning of low volumes of documents to enable teams to share information more easily. He asked for confirmation that these amendments are in order. It was confirmed that the amendments should stand. IK also advised that the Central Scanning Bureau is being used to scan historic environment records to a shared drive (rather than Wisdom). It was confirmed that this use of the CSB is in order. **Action:** IK to amend the Scanning Policy and ensure the updated version is placed on the intranet.	**IK**
13	**Violent Warning Marker System** - update SD advised that he has had discussions with Judith Hay, AD for Children's Social Care and RB about what should be included in such a System. The discussion was around what is 'violent' and what is 'a hazard'. JS advised that a meeting has been arranged for 26 January 2012 to further discuss what should be included on a System and will include RB and Legal Services. SD confirmed that a corporate Policy would be available by 1 April 2012. **Action:** As per previous meeting notes and Actions Log.	**SD**

Item No	*Item*	*Action By*
14 14.1	**DPA / FOIA Issues** **Revised FOI Process Map – update** RP advised that he has discussed this with Carole Dunn and changes will be made to the Process Map. JSM advised that it needs to take into account the expectation of FOI staff and Directorate staff. LJ advised that it needs to be a corporate filter that enables efficient handling. JSM suggested that people dealing with FOIs should differentiate between factual questions and genuine FOIs rather than treating all requests as an FOI. It was suggested that the flowchart will assist in this differentiation. It was requested that issues be resolved and a flowchart be agreed for referral to this Group for the 14 March 2012 meeting. **Action:** RP to carry out changes following discussions with Carole Dunn and refer an agreed version back to this Group at the 14 March 2012 meeting.	**RP**
14.2	**Data requests/complaints – multiple officer inputs** Carried forward to next meeting.	**RB**
15	**Multi-Agency Group –** update Carried forward to next meeting.	**RB**
16 16.1	**Internal Audit Reports** **Current Audit Reports that refer to Information Governance** RP advised that there are no internal audit reports presently in progress.	
16.2	**Unannounced information security checks – update (*linked to 5*)** It was suggested that RP liaises with DIGCs before deciding which areas to cover for further unannounced information security checks. **Action:** RP to liaise with DIGCs before deciding which areas to cover for further unannounced information security checks.	**RP**
17 17.1	**Coalition Government Latest Proposals** **Transparency Agenda – update** JSM referred to the recent update around publishing senior officer details. SL will keep the Group informed of any updates.	**SL**
17.2	**Draft NYCC self assessment of compliance with Code of Recommended Practice for Local Authorities on Data Transparency - update** JSM/SL went through the updated self assessment following comments from CYPS and BES. Comments are still awaited from HAS and CEG. Comments would particularly be welcome from Kim Trenholme on the 'pay multiple' and Neil Irving on issues relating to the voluntary community and social enterprise and the community asset register.	

Item No	*Item*	*Action By*
	Action: SL to keep the Group informed of any updates. SL to obtain comments from Kim Trenholme and Neil Irving on updates including issues around the 'pay multiple', the voluntary community and social enterprise and the community asset register.	**SL** **SL/HE**
18	**Employee Policy Acceptance Tracking System - update** Following consultation, HE advised that whilst such a tracking system would be helpful in disciplinaries etc., knowing who has been advised doesn't necessarily provide extra evidence. It was agreed that this initiative will not be taken forward.	
19	**Actions Log** Noted. FS will update the Log as at 11 January 2012 following this meeting, show completed actions as highlighted and add new actions as necessary.	**FS**
20	**Any Other Business** RP advised that a notification has been received that the European Union is intending to make changes to the Data Protection Policy. One change involves a breach being notified to the ICO within 24 hours. RP will keep the Group informed of developments. SD advised that he has received phone calls from 'unknown' people. CC advised that his contact details must have been picked up and are being used in an illegitimate way. CC advised that this cannot be stopped but he will be placing a message on the intranet on this matter. HE advised that there is an EU Directive which comes into force in May 2012 relating to the ICO being able to investigate issues relating to cookies. HE will keep the Group advised of developments. **Action:** RP to advise further on the possible changes to the Data Protection Policy by the EU. CC to issue a message relating to phone calls from illegitimate sources. HE to advise further on the EU Directive relating to cookies.	**RP** **CC** **HE**

APPENDIX 3

Corporate Information Governance Group 2
Meeting 14
14 March 2012 @ 2pm in Meeting Room 2

Attendees:

John Moore (JSM)	-	Senior Information Risk Owner and Chair	
Fiona Sowerby (FS)	-	Head of Risk Management & Insurance, Secretary to Group	
Champions			
Sukhdev Dosanjh (SD)	-	DIGC HAS	
Kevin Tharby (KT)	-	DIGC CYPS	
Shaun Lee (SL)	-	DIGC FCS	
Joel Sanders (JL)	-	DIGC BES	
Helen Edwards (HE)	-	DIGC CEG	
Advisers			
Moira Beighton (MB)	-	Legal	
Kelly Hanna (KH)	-	HR	***Apologies***
Roman Pronyszyn (RP)	-	Audit & Information Assurance Manager, Veritau	
Robert Beane (RB)	-	Information Governance Officer, Veritau	
Colin Cottrell (CC)	-	Information Security Officer	
Ian Kaye (IK)	-	Records Manager	
Janice Williams (JW)	-	eDRMS Project Manager	
Simon Wright (SW)	-	Senior Emergency Planning Officer	***Apologies***
Phil Jones (PJ)	-	Property	**Not present by agreement with JSM**

cc	Tracy Harrison	-	BES
	Robin Mair		CEG
	Keith Sweetmore	-	CEG
	Maureen Howard	-	HAS
	Dawn Ross		HAS
	Max Thomas	-	Veritau

ACTION NOTES

Item No	*Item*	*Action By*
PART A	**FORMALITIES / STANDING ITEMS**	
1	**Introductions and Apologies** Apologies - see above.	
2	**Future meetings** all Wednesdays **2012 dates** 30 May 2012 @ 2.00pm 18 July 2012 @ 2.00pm	

Item No	*Item*	*Action By*
PART B	**ACTION PLAN**	
3	**Roll out Plan**	
3.1	**Update on Progress of Plan (including Information Charter)**	
	RP advised that he will be carrying out a full review of the Roll Out Plan. This will involve taking a high level view but with a granular approach and it will be refocussed around Directorates.	
	Action: RP to carry out a full review of the Roll out Plan and present the revised version to the next meeting.	**RP**
3.2	**Staff Awareness and Training**	
	- **training within the Directorates**	
	Directorates	
	All Directorates have identified their needs for training. RB will review the requirements provided by the DIGCs (as well as the information provided as part of the Actions Log) and formulate a training plan for all Directorates.	
	Action: RB to formulate a training plan for all Directorates.	**RB**
	- **E learning facility - update**	
	RB advised that he had received some DIGCs comments on the draft 20 minute e learning module for data protection and information security. RB had also referred the module to the e learning development unit to discuss transfer/conversion into a presentation format. RB advised that KH had advised that she requires confirmation that DIGCs agree to the content before it can be converted into an e learning module.	
	Action: RB to obtain all DIGCs' agreement to the content of the draft 20 minute e learning module before it can be converted into the required format. RB to then take forward the agreed module for conversion and transfer onto the Learning Zone.	**RB/DIGCs**
	- **Info Gov as competency**	
	KH advised that she had looked into the possibility of including information governance as a competency for appropriate staff groups. She confirmed that this has been agreed and that JDs and PSs could be updated.	
	Action: HE to talk to HR to get guidance on how this should be taken forward.	**HE**
	- **training log**	
	A discussion took place around how training will be recorded. E learning (both short and long versions) should be recorded through the Learning Zone. However it is not clear how any group training will be recorded. HE confirmed that she will ask HR how this could be done.	
	Action: HE to ask HR how group training can be recorded as this will not be done through the Learning Zone.	**HE**

Item No	***Item***	***Action By***
3.3	**Information Audits – progress to date**	
	RB advised that there is a wide variation amongst the information audits but the variation is legitimate because of the different services provided. He confirmed that he will establish a standard which will include certain issues eg appraisals, in order to provide some consistency.	
	It was decided that this item is no longer needed on the agenda and will be brought up when necessary in the future.	
	Action: RB to establish a standard for information audits in order to provide some consistency.	**RB**
	FS to take this item off the agenda in future.	**FS**
4	**Communication Issues**	
4.1	**Updated World Map**	
	Noted.	
	Action: RB to continue to keep the World Map up to date.	**RB**
4.2	**Posters**	
	HE confirmed that the posters were currently being printed following feedback and discussions with DIGCs. It was agreed that HE should continue to liaise with DIGCs and arrange distribution of the posters.	
	HE advised that she is discussing changing the default screen on computers to a message around information governance from 'Small Steps Big Difference'.	
	HE will also arrange a key message and intranet news item on information governance to coincide with when the posters are being distributed.	
	She confirmed that this will all take place within the next month.	
	Action: HE to complete the task of printing the posters and arrange distribution with DIGCs.	**HE/DIGCs**
	HE to continue discussions with Dave Sadler on changing the default screen on computers to a message around information governance.	**HE**
	HE will arrange a key message on information governance.	**HE**
4.3	**Any other issues to be clarified/raised?**	
	None	
5	**Information Security**	
5.1	**Internet Issues – update**	
	A paper was provided relating to potential excessive personal browsing of the internet during paid hours. JSM explained that this issue has arisen due to a disciplinary outcome being overturned on appeal. JSM asked whether these reports to Directorates were followed up and CC confirmed that they are. It was agreed that the responsibility for dealing with these matters sits with managers. However a definite link needs to be created between DIGCs and Directorate HR reps to ensure correct and consistent advice is provided.	

Item No	*Item*	*Action By*
	Action: JSM is reviewing the role of ICT in this process - need to ensure that a definite link is created between DIGCs and Directorate HR reps to ensure correct and consistent advice is provided.	**JSM**
5.2	**Details of latest Breaches - internal and external** **Internal** Noted. CC advised that he had recently attended training delivered by the ICO and had established that if the risk of breach has been mitigated to the best ability of the Council then a fine will not necessarily apply. He also advised that the key message relating to e mails being sent to addressees through the 'BCC' box had received favourable feedback. CC further advised that PGP Encrypt is now extensively being used to send encrypted e mails. Presently it is necessary to put 'encrypt' in the subject field of the e mail whereas in future this will be amended to pressing a button marked encrypt. **External** Noted. JSM asked DIGCs if they use the details of the breaches within their Directorates in order to raise awareness. ML advised that CYPS distribute the information through their Directorate Information Governance Group. A discussion took place around the security of laptops and the use of a Kensington lock to deter opportunist thieves. CC/FS confirmed that losses had improved recently. CC confirmed that an asset register for all hardware will soon be available.	
5.3	**SIRO breaches** ➢ **SIRO/DIGC workshop on 20 January 2012** It was agreed that the workshop that was organised was a success. It was suggested that the people that attended the training may wish to meet every 6 months to discuss breaches and do some benchmarking among Directorates. **Action** RP to take forward suggestion of training every 6 months. ➢ **Notification procedure** A discussion took place around the revised Information Security Incident Investigation Procedure and associated documents that have been produced following the workshop on the 20 January 2012. It was agreed that ALL but particularly DIGCs should read the Procedure document and ensure that they are comfortable with their roles and responsibilities. Plus that the narrative in the document reflects the workshop outcome regarding sequential workflow. All comments to RB. SD advised that he is concerned that there are adequate definitions around breach information that should be fast-tracked to the SIRO. RB confirmed that there is adequate reference to this in the flowchart.	 **RP**

Item No	*Item*	*Action By*
	ML suggested that deputies should be named in case DIGCs are on holiday or on sick leave. This was agreed and suggestions were made for possible deputies. All DIGCs to arrange this and provide names to RB/RP so that appropriate training can be given.	
	Action ALL but particularly DIGCs to read the Procedure and ensure that they are comfortable with their roles and responsibilities.	**DIGCs**
	Plus that the narrative in the document reflects the workshop outcome regarding sequential workflow. All comments to RB.	**ALL to RB**
	JSM to arrange submission of document to Management Board – will advise DIGCs of details so that they can 'brief' their respective Directors.	**JSM**
	All DIGCs to arrange deputies and provide names to RB/RP so that appropriate training can be given.	**DIGCs**
	➢ **shared facility showing a log of recorded breaches and their investigation process**	
	RB confirmed that the specification for a shared incident log has been completed and has been submitted to ICT. JSM confirmed that he will be following this up with ICT.	
	Action JSM to follow up the specification for a shared incident log that has been submitted to ICT	**JSM**
	➢ **handling of Subject Access Requests**	
	SD advised that this issue originally evolved as a result of some information not being redacted when responding to a request. Following this there was an audit of practices within Directorates and it was agreed that there needs to be a consistent approach across Directorates. It was suggested that primarily SD/KT should meet to discuss a way forward.	
	It was also agreed that RB/RP will test whether the breach system specification (see above) would be suitable to track subject access requests too. RB/RP/SD/KT should then liaise to agree if this works.	
	Action: SD/KT to meet to discuss and agree a consistent approach to handling subject access requests across Directorates.	**SD/KT**
	RB/RP to test whether the breach system specification would be suitable to track subject access requests too. And then liaise with SD/KT to agree if this works.	**RB/RP/ SD/KT**
5.4	**Unannounced information security checks – update**	
	Nothing to report until next checks undertaken.	

Item No	*Item*	*Action By*
6	**Records Management**	
6.1	**Records and retention issues in Customer Services - update**	
	IK advised that he is continuing to work with Katherine Kelly on Lagan. He also confirmed that no records are now retained in the test environment.	
6.2	**Records and retention schedule - update**	
	IK advised that the records and retention schedule will be reviewed following completion of the information audits. IK/RB will continue to liaise on this matter.	
	Action: IK to continue to work on records and retention issues with RB and DIGCs	
6.3	**Publication Scheme - update**	
	RP confirmed that the Publication Scheme will continue to be reviewed. It was agreed that this item can be removed from the agenda.	**RP and FS**
PART C	**POLICY DEVELOPMENT**	
7	**Set 5**	
7.1	**Security Classification Policy**	
	JSM began a discussion around how it is possible to find a way of consistently classifying documents. He asked whether it would be possible to condense the policy to a one sided summary which would be understood by all employees.	
	SL suggested that DIGCs initially look at information asset registers and attempt to classify the documents listed in the register.	
	It was decided that BES, FCS and CEG will do the following: • pilot the use of the security classifications and advise whether the system is practical at the next meeting. • having tested and agreed that the classifications will work, advise how it is possible to get all employees to understand what should be done.	
	SD advised that HAS still need to understand the basics of information governance before applying a further layer of security.	
	Action BES, FCS and CEG will do the following: • pilot the use of the security classifications and advise whether the system is practical at the next meeting. • having tested and agreed that the classifications will work, advise how it is possible to get all employees to understand what should be done.	
7.2	**Information Enquiry Charges Policy**	
	Deferred.	

Item No	*Item*	*Action By*
8 8.1	**Set 6** **Computer, Telephone and Desk Use Policy** ➢ **'Clear desk' part into Security Classification Policy** Linked into Item 7.1 above.	
9 9.1	**Set 7** **E Mail Archiving and File Management Policy** ➢ **progress report on electronic document storage including emails** JSM advised that this issue is now being progressed under the One Council ICT Systems and Data workstream. The technology platform relating to storage is now fully tested by ICT. JSM then suggested arranging a special one off meeting of this Group to discuss a proposal for the storage of past and future data. He expressed concern about the high cost of storage of e mails and other data and the fact that many e mails do not need to be created. He went on to say that if anyone would like others to attend the one off meeting they will be welcome. **Action:** JSM to arrange a one off meeting of this Group (plus other interested parties) to discuss a proposal for the storage of past and future data. ➢ **Named (P) drive analysis** Noted.	**JSM**
10 10.2	**Other Policies to be Considered?** **Any Others?** None.	
PART D	**OTHER MATTERS**	
11 11.1	**Remote/Flexible Working – sensitive/non sensitive data** **Guidance Note on Remote/Flexible Working relating to Sensitive/Non Sensitive Data – update** JSM advised that there is a mixture of One Council workstreams including HR, ICT Systems and Data and Property that are all working on this matter. Once their collective work is complete it will be necessary to have a set of 'rigorous and imaginative thinking' volunteers to test the template. **Action:** JSM will continue to update the Group on the outcome of the work being carried out.	**JSM**

Item No	*Item*	*Action By*
11.2	**Domestic PCs, web access and related issues – technical constraints versus policy adherence versus legal position** See item 11.1 above. This issue will also be picked up by the One Council workstreams mentioned above. CC advised that he has asked the ICO whether an employer would be responsible if a domestic PC was lost/sold with employer related personal data on it. He will advise the answer when received. MB suggested that if policies are produced and circulated together with the provision of awareness raising and training, then this should assist in an organisation not being held responsible. JSM advised that once all these issues have been suitably addressed and responses agreed, then he will report to Management Board. **Action:** CC to advise outcome of discussions with the ICO relating to an employer's responsibility for an employee placing employer related personal data onto a domestic PC. JSM to keep the Group appraised of developments relating to use of domestic PCs.	
12	**Local scanning arrangements**	
12.1	**Permitted local scanning – update and corporate list** JW began the discussion on this matter by advising that the previously agreed Local Scanner and Permitted Scanning Request form and flowchart does not appear to be working. After the initial rationalisation exercise it was agreed what local scanning was permitted within Directorates. Following on from this, any new request was supposed to go to the DIGC/ICT client officer and go through the justification process. However this does not seem to have been followed and the Directorate lists have not been updated. JW advised that the STIC Advisory Board has requested an up to date list of permitted scanning in the Directorates. HE advised that there is no liaison between the ICT client officer and the DIGC. It was agreed that JW would provide a draft of the required process/revised request form and discuss and agree this with JSM. It was also agreed that JSM would ensure that a link is created between the ICT client officer and the DIGC to build on the existing list and bring each Directorate list up to date. ML suggested that once all local scanners have been identified then a challenge should be made relating to the use of these scanners. JW would then like to do a cross Directorate analysis to ensure there is the most effective and efficient use of scanners.	
	Action JW to provide a draft of the required process/revised request form for local scanning and discuss and agree this with JSM.	**JW/JSM**
	JSM to ensure that a link is created between the ICT client officer and the DIGC to build on the existing list of local scanners and bring each Directorate list up to date.	**JSM plus DIGCs and ICT client officers**

Item No	*Item*	*Action By*
12.2	**Scanning Policy – updated version on intranet?** Confirmed on World Map.	
13	**Violent Warning Marker System** - update SD advised that a draft corporate Policy has been written and is presently being considered by JS/KT and Legal Services. SD advised that this draft Policy will be taken to the Corporate Risk Management Group for approval on 22 March 2012. JSM suggested that assuming the Policy is approved, SD should then talk to JSM about the specification for a corporate access controlled system which will record and log all violent warning markers. He will then refer this to Dave Sadler, ICT Services. **Action:** SD to take a draft Policy to the Corporate Risk Management Group for approval on 22 March 2012.	**SD**
	Following approval, SD to discuss the specification for a corporate access controlled system which will record and log all violent warning markers with JSM. JSM to then refer to ICT Services.	**SD/JSM**
14	**DPA / FOIA Issues**	
14.1	**Revised FOI Process Map – update** RP tabled the revised FOI Procedure. He advised that this has been agreed by the Corporate Governance Officer Group and the Chief Executive. HE advised that various corporate functions are involved in the process such as Comms but there is no mention of these functions in the procedure. JSM suggested arranging a meeting of the FOI contacts in each Directorate to familiarise them with the revised Procedure and ensure they leave with a full understanding of the process. It was suggested that CIGG2 members are cc'd into the invitation to the meeting so that they are aware of it and can attend if they so wish. SD asked what problems have been encountered when dealing with FOIs. RP advised that issues included the speed at which FOIs are dealt with, misinterpretation of the FOI request and where the FOI team fit into the process. **Action:** RB/RP to arrange a meeting of FOI contacts in each Directorate and ensure they have a full understanding of the process. CIGG2 members to be cc'd into the invitation to the meeting.	**RB/RP**
14.2	**Data requests/complaints – multiple officer inputs** See item 14.1.	
14.3	**Possible changes to the Data Protection Policy by the EU – update** Deferred.	

Item No	***Item***	***Action By***
15	**Multi-Agency Group (Protocol) – update** RB advised that this should be called the Multi Agency Protocol rather than Group. In relation to the Protocol, RB has been advised that a decision needs to be taken by the NY&Y Chief Executives Group to formally abandon the Protocol and then whether any constitutional issues need to be addressed. The Code of Practice can then be applied directly. JSM suggested that the principles in the Code of Practice could be used as a checklist for each partnership to then produce their own protocol. There is also perhaps a need for the data sharing protocol to be inserted into the Partnership Governance toolkit. SD advised that in HAS, the independent sector providers adhere to a data protection policy but he is unsure of what protocol is applying in multiple partnerships where data is exchanged. It was agreed that SD would arrange a meeting with other Directorates and involve Legal Services, and decide what the Council position should be on sharing data with various organisations including Commissioning Groups. RP will provide a list of known partnerships to SD for the discussion. DIGCs then need to decide whether each partnership needs a data sharing protocol. The outcome will then be reported back to the next meeting. JSM will separately discuss an update of the Partnership Governance toolkit to reference this issue with Geoff Wall and Neil Irving. **Action** SD plus DIGCs and Legal Services to decide what the Council position should be on sharing data with various organisations including Commissioning Groups. SD plus DIGCs to consider the latest list of partnerships and decide whether each partnership needs a data sharing protocol. SD on behalf of DIGCs will report the outcome to the next meeting. JSM will discuss an update of the Partnership Governance toolkit to reference the need for a data sharing protocol with Geoff Wall and Neil Irving.	**SD plus DIGCs and Legal Services** **JSM**
16 16.1	**Internal Audit Reports** **Current Audit Reports that refer to Information Governance** None.	
17 17.1	**Coalition Government Latest Proposals** **Transparency Agenda – update** SL advised that the Agenda is constantly evolving but requirements are becoming embedded in Council activities. He will continue to advise of any developments.	

Item No	*Item*	*Action By*
17.2	**Draft NYCC self assessment of compliance with Code of Recommended Practice for Local Authorities on Data Transparency** SL advised that NYCC is already doing many of the issues raised on the self assessment. He pointed out that links to various points to demonstrate compliance are available in the self assessment. The areas where NYCC are possibly weak are in the following areas: • Property register – we are presently looking at how we can comply. • Information relating to the provision of grants to the voluntary community and social enterprise sector – this information is not available in one central point. JS also mentioned the LEP at this point. • Contracts and tenders to businesses and to the voluntary community and social enterprise sector – this issue will be looked at by the One Council Procurement workstream. **Action:** SL to continue to update the self assessment and keep the Group appraised of developments. **Post meeting** RB advised that a Protection of Freedoms Bill is currently going through the House of Lords. This Bill contains proposals to require all public authorities to release datasets in a re usable electronic format (see paper re post meeting Item 17 FOI Datasets for more details).	**SL**
18	**Message on intranet regarding phone calls from 'unknown' people** CC confirmed that this was a much wider issue that was happening across the County Council. It has been brought under control but will continue to be monitored.	
19	**EU Directive relating to cookies** HE confirmed that there were no further updates on this matter and will advise when it needs to be discussed again in the future.	
20	**Actions Log** Noted and agreed.	
21	**Any Other Business** JW advised that there is an issue on Wisdom where the Word docs template appears to retain the first author and therefore requires advice on what implications this has. RP/RB will reflect on this matter after further discussion with JW/JS and advise accordingly. **Action:** RP/RB to discuss and understand the Word docs template on Wisdom issue relating to the retention of the first author and resolve with JW/JS.	**RP/RB and JW/JS**