

## NORTH YORKSHIRE COUNTY COUNCIL

## CORPORATE AND PARTNERSHIPS OVERVIEW &amp; SCRUTINY COMMITTEE

31 January 2011

## INFORMATION GOVERNANCE

## Report of the Corporate Director – Finance and Central Services

**1.0 PURPOSE OF REPORT**

- 1.1 To consider the progress made to date in respect of improving the Information Governance arrangements in the County Council.

**2.0 BACKGROUND**

- 2.1 The Committee will be aware, from previous reports, that an Information Governance Framework is being developed within the County Council to reflect the core measures identified in the Government's Data Handling review, the HMG Security Framework and ISO 27001. The objective of the Framework is to establish how the County Council will protect and develop the security, quality and management of its information. The increased importance of Information Governance within the County Council reflects the continuing prominence given by the media to this subject as a result of a number of high profile losses of personal and sensitive data within the public sector. The importance of effective information handling has been reflected in the increased powers awarded to the Information Commissioner's Office (ICO). Since 6 April 2010, the ICO has had the power to issue fines of up to £500,000 to those organisations found to have incurred significant breaches of the Data Protection Act. To date, two organisations have been fined under this new regime: Hertfordshire County Council (£100,000) and Sheffield based A4e (£60,000).

**3.0 PROGRESS TO DATE**

- 3.1 The report attached at **Appendix 1** was presented to Audit Committee at its meeting in December 2010. This report provided Members with an update on the considerable progress made to improve Information Governance arrangements in the County Council. The report details the various actions that have been taken and are ongoing in order to improve the County Council's information security arrangements and to ensure compliance with relevant legislation and best practice.
- 3.2 Since the report was submitted to Audit Committee in December 2010, the British Standards Institute's assessment of ICT Services' Information Security Management System for the County Council has been successfully completed and ICT Services have therefore achieved the ISO 27001 certification. This is a

considerable achievement as only ten other local authorities in the UK are certified to this Standard (out of a total of 433 councils).

#### 4.0 **RECOMMENDATIONS**

4.1 Members to note the progress made on information governance issues as detailed in **Appendix 1**.

JOHN MOORE  
Corporate Director – Finance and Central Services

County Hall  
Northallerton

21 January 2011

**Background documents** – None

## NORTH YORKSHIRE COUNTY COUNCIL

## AUDIT COMMITTEE

9 DECEMBER 2010

## 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 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 has been 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 standards which detail the key requirements that the County Council must fulfill 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 where the County Council is in relation to each of the above areas.

### 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. Attached as **Appendix 1** is the latest version of this 'world map'.

### **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 meetings held on 26 May, 30 June, 4 August, 8 September and 27 October are attached at **Appendices 2 to 6** 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:
- formation of CIGG2 with revised terms of reference and membership. The Group now meets approximately every six weeks
  - nomination of Information Governance Champions for each directorate (DIGCs). These DIGCs are now proactively promoting the IG agenda within their directorate and are members of CIGG2
  - the approval of a number of key IG policies e.g. Email, Internet Usage, Portable Media & Encryption, Use of Social Media, Records Management. Further policies are under discussion including Disclosure of Personal data, Information Security Incident Reporting and Information Sharing with External Partners. As explained in **paragraph 3.3** above, **Appendix 1** shows the current 'world map' of the County Council's IG related policies,

highlighting those that are or have already been considered by CIGG2. Other policies will be added to this map as required

- preliminary identification of key information assets and information asset owners within directorates
- completion of the IG risk register
- port blocking has been applied to County Council IT equipment to ensure that unauthorised devices cannot be installed
- a security labeling mechanism has been devised and will be considered by CIGG2 and communicated to staff as appropriate

### **The Role of Veritau**

3.9 Staff from Veritau support the development and implementation of the Information Governance Framework. This work includes:

- 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
- raising awareness and promoting compliance via training, guidance and advice

In addition, Veritau's auditors have commenced a programme of work designed to test understanding and compliance with the new policy framework. The audit work will aim to identify potential IG risks so as to support the effective roll out of the policy framework. Where risks are identified these will inform the future development of IG policies and help to target other corrective actions.

## **4.0 INFORMATION SECURITY**

### **External Factors**

4.1 Since 6 April 2010, the ICO has had the power to fine organisations up to £500,000 for serious data breaches or losses (the previous maximum fine that could be imposed was £5,000). The ICO has issued guidance to explain how such penalties will be applied. The guidance states that penalties will be incurred where the "data controller has seriously contravened the data protection principles and the contravention was of a kind likely to cause substantial damage or substantial distress." The critical point is that the data controller (i.e. the County Council) must have known or ought to have known that there was a risk that a breach could occur. The new powers granted will also enable the ICO to perform compulsory audits where breaches may have occurred. On 24 November, the ICO announced that it had issued its first fines to Hertfordshire County Council (£100,000) for faxing details of a child sex abuse case to the wrong recipients and to Sheffield based A4e (£60,000) for losing an unencrypted laptop containing details of thousands of people. The Information Commissioner has said that the fines imposed will 'send a strong message' to those handling data (see **Appendix 7** for further details).

- 4.2 As of the 29 October 2010, the NHS had reported the greatest number of data losses with 377 incidents (30% of all of the 1,254 breaches reported to date). This compares with 360 from the private sector, 184 from local government, 97 from central government and 149 from other public sector bodies. The biggest category of errors in local government arose from information being disclosed in error.

### **What the County Council is doing to protect its information**

- 4.3 The Information Governance Officer (IGO) (Veritau) and the Council's Information Security Officer (ISO) are working together to produce the relevant policy and guidance documents on information security related matters.
- 4.4 Although the ISO 27000 series of standards covers all aspects of information security (e.g. in relation to personnel, assets and contracts) the key area that is being targeted by the ISO is IT infrastructure, both hardware and software, and the methods by which the security of the infrastructure can be achieved. As preparation for the formal assessment of compliance with ISO 27001, two 'readiness reviews' were carried out by National Computing Centre (NCC) and the County Council's IT internal auditors, PricewaterhouseCoopers (PwC). Both reviews reported favourably. PwC issued their final report in October 2010 and concluded that the policies developed were of a high standard when compared to other local authorities. The report also stated that ICT had invested a significant amount of time, skill and effort in implementing a management system to support and maintain information security. On 5 November, the British Standards Institute (BSI) performed a Stage 1 audit and concluded that the areas assessed were effective and that Phase 1 had been met. The next step will be a four day assessment covering the implementation of the security controls (as defined in Phase 1). If successful, ICT will then be certified ISO 27001 and will enter the three year surveillance mode whereby the BSI can arrive at the County Council (with little notice) in order to perform another assessment to confirm that the criteria of certification is still being met. Whilst ICT is the only area of the County Council currently being assessed against the ISO Standard, the possibility of extending the Standard to other areas will be considered in due course.
- 4.5 The ISO has primary responsibility for ensuring the County Council has adequate electronic security arrangements in place and therefore has or will address security issues such as encryption, use of IT equipment, antivirus arrangements and technical incident reporting. The ISO works closely with Veritau's IGO to ensure that all policies and procedures within the overall IG Framework are complementary and consistent.
- 4.6 The County Council continues to address a number of priority areas in relation to information security by devising appropriate policies and strategies to ensure that the County Council's confidential and personal data is adequately protected from unauthorised disclosure. For example, as of 17 November, ICT Services has introduced 'port blocking'. This means that only hardware encrypted devices (as issued by ICT) can be connected to the County Council's USB ports. There are a limited number of exemptions (e.g. camera cards) to this rule. However, detail of all such exemptions will be maintained and monitored by ICT.

4.7 Although the emphasis in the above paragraphs has been on the application of technology in relation to IG, it must be remembered that the County Council will still have many paper records etc that require the same principles and standards of management to be applied to them.

## 5.0 COMPLIANCE

5.1 In addition to the review of ICT's Information Security Management System, PwC have also completed an audit of the County Council's high level IG policies. PwC reviewed the overarching IG Policy, the Freedom of Information Policy, the Data Protection Policy, the Data Quality Policy and the Records Management Policy. No significant issues were identified during the audit although PwC made a number of suggestions that either have already or will be taken into account when the relevant policy is next reviewed.

5.2 Veritau's auditors also carried out an audit of the County Council's Freedom of Information processes and concluded that high assurance could be placed on the processes involved. Veritau auditors will carry out further audit work towards the end of the financial year to consider the extent to which IG risk is being effectively managed by Directorates across the County Council. This will include a preliminary assessment of the County Council's position when audited against the Information Assurance Assessment Framework.

### Freedom of Information Act 2000

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

5.3 Between 1 April and 31 October 2010, the County Council has received a total of 599 FOI requests compared to 477 and 315 for the same period in 2009/10 and 2008/09. This represents an increase in workload of over 90% since 2008/09. It has responded to 99% of these requests within the 20 working days time frame defined by the legislation (compared to a performance target of 95%).

## 6.0 INFORMATION QUALITY

6.1 The Council's revised Data Quality Policy and Strategy were included in the suite of documents approved by Management Board in April 2010. Monitoring of the Data Quality Action Plan will commence and progress will be reported to this Committee accordingly.

## 7.0 RECORDS MANAGEMENT

7.1 Records management is concerned with the application of systems and processes to control access, retention and disposal of records. This includes capturing and maintaining evidence of business activities and transactions in the form of records



regardless of the technology used to create and store them. The revised Records Management Policy has now been approved by CIGG2.

7.2 Records management works alongside the Electronic Document and Record Management (eDRM) Programme Board to provide records management input into the design and implementation of new systems, including the management of a new central scanning bureau at the County Record Office.

7.3 The Assistant Director – ICT has carried out an investigation into the use of local scanners and multi functional devices (MFDs) within the County Council. The findings of this investigation concluded that the number of local scanners being used within directorates was not as high as originally thought although there are opportunities to rationalise, relocate and re-use scanners. It also recognised the need for a formal process to maintain records of the number, location and usage of scanners and for the need to monitor usage and scanning needs. Further meetings will therefore be held between the eDRMS team and Directorate Information Governance Champions to define the criteria in determining whether central scanning facilities are applicable to their scanning requirement or, how permitted local scanning can best be achieved. A set of guiding principles on the use of local scanners will form part of the County Council's Scanning of Documents and Records Policy. It is also essential for consistency purposes that any local scanning is undertaken to the same control standards as adopted by the Central Scanning Bureau.

7.4 To assist the County Council achieve efficient records management, the Records Management Service (part of ACS) is positioned within the existing Information Governance corporate structure. The Records Manager (RM) attends CIGG and works closely with the eDRM Programme Board and the Veritau IGO in order to:

- develop records management strategy and policy
- agree format and content of information audits
- develop file plans
- review and update the corporate records retention and disposal schedule

## 8.0 **TRANSPARENCY**

8.1 Following the Government announcement earlier in the year that local authorities, as well as other public bodies will be required to be more open and transparent on a range of information to be provided to the public, further guidance has been provided on the format and content. The Government's intention is, by making this information available, in some cases in a common searchable format, that the public at large will be able to scrutinise these matters and act as "armchair auditors", gaining information about this authority and an ability to compare information across authorities nationally. Coordination of the County Council's approach to meeting these requirements has been through CIGG2.

- 8.2 Most coverage has been given to the need to publish details of all expenditure items over £500. This must be available no later than January 2011, and work is nearing completion on putting the systems in place that will enable this deadline to be met. The information will be published and accessible through a webpage on the County Council's internet site under a banner of Open Data.
- 8.3 As well as the spend data, information will be provided through these pages on contract information, information on senior staff salaries and the roles and responsibilities of the Management Board. In addition, the webpage will provide access to other information on the financial accounts, overall staffing numbers, links to current vacancies and wider information on service responsibilities.
- 8.4 At this stage, the main outstanding issue relates to the publication of contract detail. In the initial announcement by the Government, their intention was that local authorities would make information available for all contracts over £500. No further guidance has been provided at this stage. There are significant issues on interpreting this original announcement (eg in relation to care packages). At this stage, the approach that is being taken is to make available information for all contracts and procurement matters above £10,000, with the exception of individual packages of care in Adult and Community Services, Childrens Social Care and Special Educational Needs. The information will utilise the existing web based procurement system (SCMS) together with its related Contracts Register. This initial approach will be reviewed as further information and guidance becomes available from the Government.

## 9.0 PRIORITIES FOR THE NEXT SIX MONTHS

- 9.1 Based on the CIGG2 roll out plan, the following have been identified as priority tasks for the next six months: -
- (a) as the SIRO for the County Council, the Corporate Director – Finance and Central Services continues to chair CIGG2 to ensure that the County Council's IG Framework is implemented across the Council; the SIRO reports progress directly to the Management Board
  - (b) the IGO, ISO and RM to work together to continue producing and updating the necessary policy and guidance documentation for the IG Framework and ISO 27000 Series
  - (c) the DIGCs to continue to address IG issues within their directorates and to promote compliance with approved policies
  - (d) the roll out of the security marking mechanism for the County Council that will identify the level of security required for each type of information. To provide guidance to relevant officers on the application of this mechanism
  - (e) to continue with the IG roll out plan including raising staff awareness of IG requirements and the County Council's Framework via a series of training and awareness raising sessions
  - (f) to update the Council's Records and Retention Schedule

- (g) to develop a coordinated and consistent approach to the prevention and management of data security breach incidents.
- (h) to complete the roll out of the initial arrangements to meet the Government's Transparency agenda, and to review this in the light of further guidance and emerging best practice.

**10.0 RECOMMENDATION**

10.1 Members are asked to note the progress made on information governance and transparency issues to date.

JOHN MOORE  
Corporate Director - Finance and Central Services

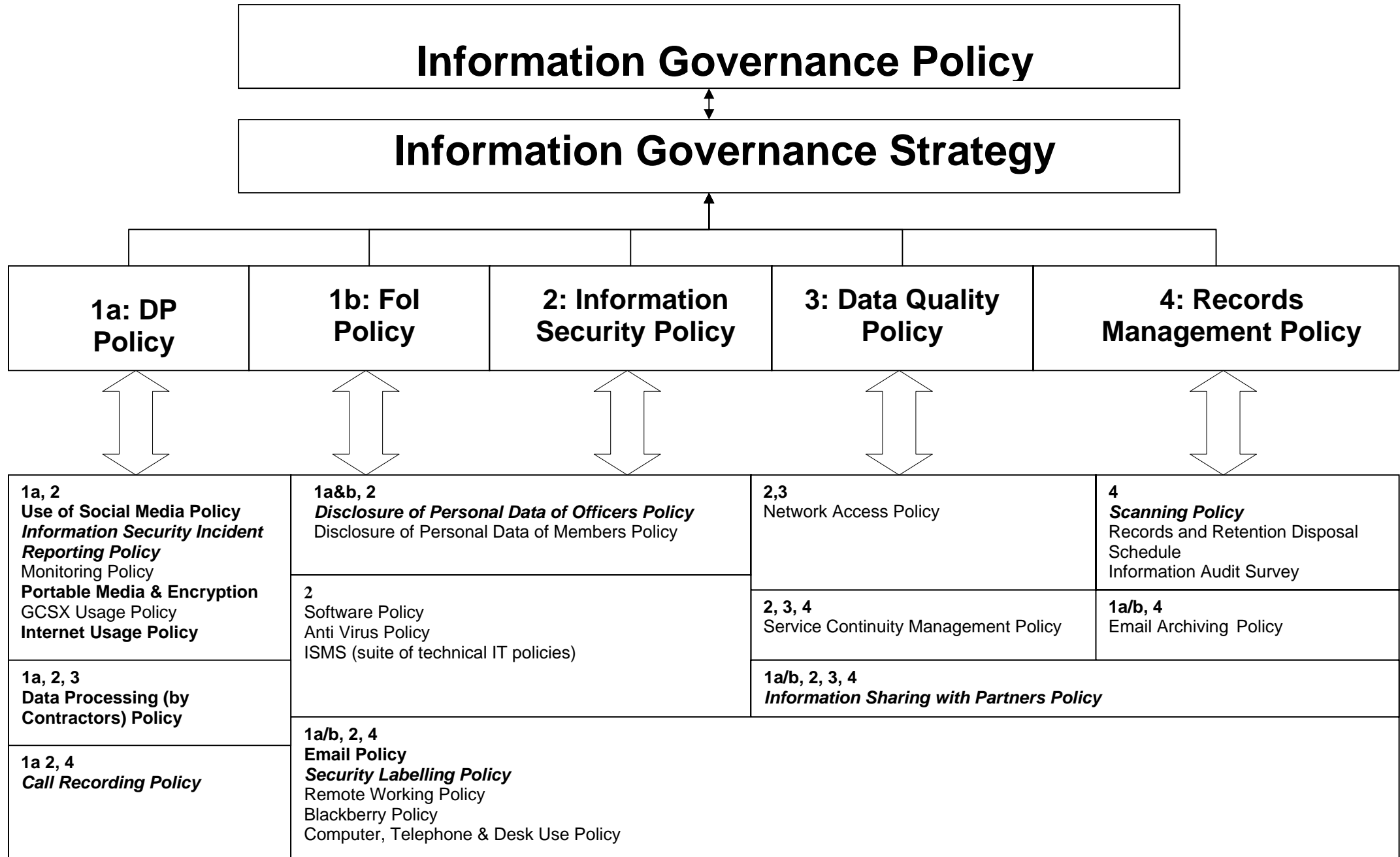
**Background Documents**

Contact Helen Fowler, Audit & Information Assurance Manager (extension 2284)

Report prepared by Helen Fowler, Audit & Information Assurance Manager and presented by John Moore, Corporate Director, Finance and Central Services.

County Hall  
Northallerton

30 November 2010



**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

# Corporate Information Governance Officers Group 2 Meeting I

**Wednesday, 26 May 2010 @ 2.00pm in B17**

**Attendees**

- John Moore (JSM) - Senior Information Risk Owner and Chair
- Fiona Sowerby (FS) - Head of Risk and Insurance, Secretary to Group **Apologies**
- Helen Fowler (HF) - Audit & Information Assurance Manager, Veritau

**Champions**

- Sukhdev Dosanjh (SD) - DIGC ACS
- Kevin Tharby (KT) - DIGC CYPS
- Shaun Lee (SL) - DIGC FCS
- Tracy Harrison (TH) - DIGC BES **Apologies**
- Helen Edwards (HE) - DIGC CEG **Apologies**

**Advisors**

- Isabel Esteves (IE) - Legal **Apologies**
- Carol Dickinson (CD) - HR **Apologies**
- Phil Jones (PJ) - Property **Apologies**
- Kelly Hanna (KH) - HR **Apologies**
- 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

**CC:** David Sadler  
Carole Dunn

## ACTION NOTES

ITEM			Action by
<b>PART A</b>	<b>FORMALITIES / STANDING ITEMS</b>		
<b>1</b>	<b>Introductions and Apologies</b> Apologies – see above.		
<b>2</b>	<b>Future meetings for CIGG2</b> <b>2010 dates (to be confirmed)</b> – ALL previous dates 18/8/10, 14/10/10, 16/12/10 are now deleted.		<b>ALL</b>
	Wednesday 30 June @ 2.00pm Wednesday 4 August @ 2.00pm Wednesday 8 September @ 2.00pm	Wednesday 27 October @ 2.00pm Wednesday 1 December @ 2.00pm Wednesday 19 January 2011 @ 2.00pm	
	JSM asked the Group for views on how frequently meetings should be held. It was agreed that initial meetings should be more frequent until the Group had established itself. He pointed out that there are a number of dates already set (for the old CIGG) and enquired as to whether these would be suitable for members of CIGG 2. The next scheduled meeting is Wed 30 June at 2.00pm. A couple of members of the Group noted that they would not be able to make this date although cover could be provided by other officers. The Group agreed that Wed afternoons were convenient for most members. It was agreed that JSM would organise another meeting towards the end of June and another for the end of July (if possible) plus in September, October and December.		<b>JSM/FS</b>


ITEM		Action by
3	<p><b>Role of CIGG 2</b></p> <p>The draft Terms of Reference was presented to the Group for consideration. JSM pointed out that their content had been lifted from the Information Governance Strategy Framework. The Group accepted the ToR.</p>	
<b>PART B POLICY DEVELOPMENT</b>		
4	<p><b>Set 1 – as previously submitted to Management Board ()</b></p>	
4.1	<p>Information Governance Policy Information Governance Strategy Data Quality Policy Data Protection Policy Freedom of Information Policy</p>	<p>as attached to previous emails to Group members</p>
4.2	<p>JSM updated new members of the Group on the position regarding the above documents. He explained that they represented those elements of the overall IG Framework that have, to date, received Management Board approval. JSM asked the new members of the Group whether they were prepared to accept the documents as they had been approved or whether they would appreciate the opportunity to comment on the content.</p> <p><b>Action</b> - It was agreed that members of the Group would have 10 working days in which to send any comments on the above 5 policies/strategies to JSM. After which, the documents would be signed off as Council policy/strategy.</p>	
5	<p><b>Set 2</b></p> <p>JSM explained that he intends to submit further IG related policy and strategy documents to Management Board for approval. He therefore requested the Group to consider the following:</p> <ul style="list-style-type: none"> <li>• How many documents could be practically processed by CIGG2 at a time?</li> <li>• Which are considered to be a priority?</li> <li>• How CIGG 2 should discuss and approve each document?</li> </ul> <p>SD stated that it would be useful for directorates to have a chance to ‘road test’ the policies/strategies/procedures before they are formally accepted. JSM put forward a suggestion he had received from another Group member (not present) that the following ‘two meeting revolution’ could be applied:</p> <ul style="list-style-type: none"> <li>• Draft documents circulated with CIGG 2 agenda for Meeting A</li> <li>• First discussion of documents at the CIGG 2 Meeting A</li> <li>• Drafts amended to reflect comments and amendments at Meeting A</li> <li>• Revised drafts re-circulated to Group before next Meeting B</li> <li>• Final drafts signed off at next CIGG 2 Meeting B</li> <li>• Final drafts then submitted by JSM to Management Board</li> </ul>	<p><b>ALL</b> ↳ JSM</p>

ITEM		Action by
5(cont)	<p>Whilst it was acknowledged that some documents would require greater discussion than others, members of the Group agreed that the above process was appropriate, but would retain the right to flex the arrangements should a particular document warrant further discussion / research, etc.</p> <p>It was then agreed that, in general, no more than 3 documents should be processed at a time although this may vary depending on complexity of documents.</p> <p>The Group then discussed the priority areas and agreed the following:</p> <p><b>Priority 1</b> – Records Management Policy (IK); Email Policy (CC); Internet Acceptable Usage Policy (CC); Portable Media and Encryption Policy (CC)</p> <p><b>Priority 2</b> – Scanning Policy (IK/JW); Partnerships and Data Sharing Policy (RB) and Information Security Policy (CC)</p> <p><b>Priority 3</b> – Reporting Breach Procedures (Non Technical and Technical) (CC &amp; HF); Security Labelling (RB); Data Processing (RB); Call Recording (RB)</p> <p><b>Action</b> - Those officers responsible for the Priority 1 documents were requested to ensure that the relevant versions are submitted to FS in advance of the next meeting so that they may be circulated with the agenda.</p>	IK/CC to FS
<b>PART C ACTION PLAN</b>		
6	<p><b>CIGG 2 Action Plan</b></p> <p>HF went through the Plan and explained Appendices 5 and 6. Appendix 5 relates to Phase 1 which includes approval of policies, training and awareness and setting up Information Governance groups within Directorates etc. Appendix 6 relates to Phase 2 which involves the information audits within the Directorates.</p> <p>It was pointed out that this document would be a living document and would be amended to reflect new tasks and shifting priorities. The Plan is essentially an operational plan for members of CIGG 2 to monitor progress of the roll out of the IG Framework. In future, only these appendices will be presented to the Group to enable progress against the various action points to be monitored.</p> <p>Specific actions allocated to the DIGCs were highlighted in P1a and P1b of the Plan.</p> <p>It was agreed that the following should be the first considerations for the DIGCs:</p> <ul style="list-style-type: none"> <li>to decide how IG will be taken forward/communicated within their directorates i.e. Champions will need to decide whether a separate Directorate Information Governance Group (DIGG) should be established within their directorate. If this is required, the Champion should be the Chair of the DIGG and should ensure that key officers (Information asset owners) are members. Alternatively, the Champion may decide that there is an alternative means of taking IG forward such as having IG as a standing agenda item at DMTs.</li> </ul> <p>Champions asked to provide feedback at the next CIGG 2 meeting as to how they intend to take IG forward within their directorate.</p> <ul style="list-style-type: none"> <li>to identify the main information assets and/or risks within their directorates and to identify the associated information asset owners (those responsible for that information). HF stated that Veritau's Information Governance Team would assist Champions with this identification and that a template would be distributed to each Champion for their completion.</li> </ul>	<p>HF</p> <p>DIGCs</p> <p>DIGCs/HF</p>

ITEM		Action by
6(cont)	<p>HF pointed out that Champions were welcome to contact her or RB at any time with any queries.</p> <p><b>Action</b> - HF to distribute information asset template. RB to make contact with each Champion in the near future. DIGCs to consider their key information assets and how IG will be progressed within their directorates.</p>	<p>DIGCs</p> <p>HF/RB/ DIGCs</p>
7	<p><b>Information Essentials (Data Matters) Intranet Site</b></p> <p>RB stated that the new IG Intranet site has still to be developed. The Group discussed the name of this site and it was agreed that 'Information Essentials' may cause some confusion and that users may interpret this as meaning a site to obtain key facts and contacts of the Council rather than a source of IG material. It was agreed that suggestions for names for the IG Intranet site be submitted to JSM within 10 working days. JSM will provide a suitable prize for the best idea.</p>	<p>ALL JSM</p>
<b>PART D OTHER MATTERS</b>		
8	<p><b>Government Connect</b></p> <p>JSM explained that NYCC has made the necessary investment in order to be connected to the Government Connect Secure Extranet (GCSX). This enables secure data transfer between local authorities and central government. However, JSM pointed out that the facility is not being used as much as expected. David Sadler will be raising this issue at TAG. However, Champions were requested to consider the extent to which GCSX is being used within their directorates and if not, why not.</p> <p><b>Action</b> - Champions to feedback at next meeting.</p>	<p>DIGCs</p>
9	<p><b>Strategic Transformation and Integration Capability (STIC)</b></p> <p>JW advised that a group was considering scanning issues and that there were some requirements to change the current (informal) Scanning Policy. Questions had been raised such as whether 100% of incoming post should be scanned and if so, did this support the need for a central post room?</p> <p>The issue of legal admissibility arose and it was highlighted that the courts would not commit on whether or not scanned documents would be acceptable as evidence. There is therefore a need for the Council to make a decision as to how it wishes to proceed in this area and which prime documents have to be retained. If the law is unclear then a risk assessment will have to be undertaken and a decision made as to what the Council's policy will be. JSM stated that the policy on Scanning would have to go through the CIGG 2 approval process with legal input from Carole Dunn.</p> <p>Based on discussion at Item 5, Scanning Policy is a Priority 2. However, given the issues raised, the Group asked JW / IK to do further preparatory work and contact Legal as necessary (Isabel Esteves is the contact) in advance of the CIGG2 meeting.</p>	<p>JW/IK</p>



ITEM		Action by
10	<p><b>Violent Warning Marker System</b></p> <p>RB advised that he was not aware of any further developments. JSM stated that a report had been submitted to the Corporate Risk Management Group and suggested that RB contact Dominic Passman for an update.</p> <p><b>Action</b> – RB to contact DP.</p>	RB
11	<p><b>Disaster Recovery</b></p> <p>Deferred to future meeting – JSM to talk to David Sadler and will arrange full presentation at subsequent meeting.</p>	JSM→DS
12 12.1  12.2-12.3	<p><b>Information Security - Compliance with ISO/IEC 27001 and ISO/IEC 27002</b></p> <p><b>Update on Certification for ICT Services</b></p> <p>CC confirmed that ICT Services are scheduled to go for certification in October 2010 and if successful, will be one of the first councils to be certified. The first step is to have all policies in place; the second is to receive an audit visit. Any policies relating only to ICT Services can be ratified by David Sadler, Head of ICT. However, CC to talk to JSM to resolve how such policies will be fitted into the IG “world map”, and therefore linked on the new Intranet site.</p> <p><b>Outcome of NCC audit and update on PwC audit and Information Security Management System (ISMS) update</b></p> <p>CC advised that the NCC audit provided advice on some areas requiring improvement and these will be included in the action plan.</p>	CC→JSM  CC
13  13.1  13.2	<p><b>Records Management</b></p> <p>The Records Management Policy is in draft and will be circulated with the next meeting’s agenda (as per Item 5 it is a Priority 1).</p> <p><b>Business Plan</b></p> <p>IK confirmed that two new staff had been appointed which would enable the section to address the storage issues and allow IK to update the Records Retention &amp; Disposal Schedule and to commence information audit work. IK stated that the database of users needs updating. It was agreed that the current details of this database will be brought to the next meeting of this Group so that members can update their areas.</p> <p><b>Action</b> – IK to bring database details to next meeting of CIGG 2.</p> <p><b>Central Scanning Bureau</b></p> <p>IK explained that all was going to plan and that the upgrade had been completed.</p> <p>It was agreed that the next CIGG 2 meeting would be held at Malpas Road so that members of the Group could have the opportunity to view the Central Scanning Bureau before the start of the meeting – FS to arrange ½hour viewing time pre-meeting with IK/JW.</p>	IK→FS  IK→FS  FS IK/JW

ITEM		Action by
<p><b>14</b></p> <p><b>14.1</b></p>	<p><b>DP and FOI Issues</b></p> <p>RB explained that elected members are data controllers and that each Member therefore has to be notified to the ICO as such (to the cost of £35 each). It is important that elected Members are aware of their responsibilities as data controllers and that they understand that information gained within their role as a councillor cannot be disclosed in another role.</p> <p>RF will progress this with the help of Geoff Wall (who chairs MITE – the Members’ IT Group involving Cllr Les).</p>	<p><b>RF/GMW</b></p>
<p><b>15</b></p> <p><b>15.1</b></p>	<p><b>Internal Audit Reports</b></p> <p>HF briefly outlined the findings of the Records Management audit report (copy attached). All agreed actions have now been included in the CIGG 2 Action Plan and will be monitored accordingly.</p> <p>Other relevant audit findings will be reported to the Group as appropriate including details of any security breaches.</p>	<p><b>HF</b></p> <p><b>HF</b></p>
<p><b>16</b></p> <p><b>16.1</b></p>	<p><b>ICO Powers re Monetary penalties</b></p> <p>JSM outlined the potential risk (as of 6 April 2010) to the Council of the ICO imposing monetary fines of up to a maximum of £500,000 for serious breaches of the DPA.</p> <p><b>Action</b> - JSM agreed to circulate the ICO guidance on how these penalties will be applied (copy attached).</p>	<p><b>JSM</b></p>
<p><b>17</b></p>	<p><b>Coalition Government Latest Proposals</b></p> <p>JSM requested the members of the Group to track any relevant or topical Information Governance issues arising in their respective service or specialist areas, and to send relevant details to JSM (for possible inclusion on CIGG2 agendas).</p>	<p><b>ALL</b>   <b>JSM</b></p>
<p><b>18</b></p> <p><b>18.1</b></p>	<p><b>Any Other Business</b></p> <p>RB raised the issue of disclosing officer names within FOI responses and suggested that a policy on this should be discussed at the next CIGG 2 meeting.</p>	<p><b>RB</b></p>

# Corporate Information Governance Officers Group 2

## Meeting 2

**Wednesday, 30 June 2010 @ 2.00pm in Park Room, Malpas Road**

### Attendees

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

#### **Champions**

Sukhdev Dosanjh (SD) - DIGC ACS  
 David O'Brien (Do'B) - DIGC CYPS **Apologies**  
 Shaun Lee (SL) - DIGC FCS  
 Tracy Harrison (TH) - DIGC BES  
 Helen Edwards (HE) - DIGC CEG

#### **Advisors**

Isabel Esteves (IE) - Legal **Apologies**  
 Helen Atkinson (HA) - Legal  
 Carol Dickinson (CD) - HR  
 Colin Parkin (CP) - HR  
 Phil Jones (PJ) - Property **Apologies**  
 Kelly Hanna (KH) - HR **Apologies**  
 Helen Fowler (HF) - Audit & Information Assurance Manager, Veritau  
 Robert Beane (RB) - Information Governance Officer, Veritau **Apologies**  
 Colin Cottrell (CC) - Information Security Officer **Apologies**  
 Andrew Whittaker (AW) - Head of ICT Architecture  
 Ian Kaye (IK) - Records Manager  
 Janice Williams (JW) - eDRMS Project Manager  
 Simon Wright (SW) - Senior Emergency Planning Officer **Apologies**

**CC:** Kevin Tharby - CYPS  
 Keith Sweetmore - ACS  
 Max Thomas - Veritau

## ACTION NOTES

ITEM			Action by
	<b>Scanning Bureau</b>		
	Some Members of the Group attended a demonstration in the Scanning Bureau provided by Janice Williams and her team.		
<b>PART A</b>	<b>FORMALITIES / STANDING ITEMS</b>		
<b>1</b>	<b>Introductions and Apologies</b>		
	Apologies – see above.		
<b>2</b>	<b>Future meetings for CIGG2</b>		
	<b>2010 dates (confirmed at this meeting) –</b>		
	Wednesday 4 August @ 2.00pm	Wednesday 1 December @ 2.00pm	<b>ALL</b>
	Wednesday 8 September @ 2.00pm	Wednesday 19 January 2011 @ 2.00pm	
	Wednesday 27 October @ 2.00pm		



ITEM		Action by
	<b>Action:</b> RB to notify Karen Scott that these Policies are to be communicated to NYCC staff.	<b>RB</b>
<p data-bbox="188 309 209 338"><b>6</b></p> <p data-bbox="177 376 220 405"><b>6.1</b></p> <p data-bbox="177 1043 220 1072"><b>6.2</b></p> <p data-bbox="177 1816 220 1845"><b>6.3</b></p>	<p data-bbox="277 320 699 349"><b>Set 2 Policies – initial discussion</b></p> <p data-bbox="320 376 687 405"><b>Records Management Policy</b></p> <p data-bbox="320 439 1294 468">IK introduced the Policy to the Group. Observations were provided to IK including</p> <ul data-bbox="360 501 1294 916" style="list-style-type: none"> <li data-bbox="360 501 1294 562">➤ SD advising that the scope of the Policy should include records that are sent to us by third parties. <b>Action:</b> SD/IK to agree appropriate words.</li> <li data-bbox="360 640 1294 701">➤ SD suggesting that para 4.7 should be more robust so that managers and staff understand what the Policy requires them to do.</li> <li data-bbox="360 734 1294 795">➤ HF advised that PwC had put forward comments and she will advise IK. <b>Action:</b> HF to forward PwC audit comments to IK.</li> <li data-bbox="360 828 1294 916">➤ Other observations on other paragraphs were provided, for example para 4.12 where it was suggested that reference to records retention should be more explicit.</li> </ul> <p data-bbox="320 949 1294 1010"><b>Action:</b> IK will amend the Policy as suggested but track changes and present the revised Policy to the next meeting.</p> <p data-bbox="320 1043 488 1072"><b>E mail Policy</b></p> <p data-bbox="320 1106 1214 1167">AW introduced the Policy to the Group. Observations were provided to AW including:</p> <ul data-bbox="368 1200 1310 1693" style="list-style-type: none"> <li data-bbox="368 1200 1310 1261">➤ Definitions – there needs to be some common narrative and there are two sets.</li> <li data-bbox="368 1294 1310 1355">➤ Para 6.2 – Confirmation of receipt should be received for ‘outgoing’ important e mails.</li> <li data-bbox="368 1388 1310 1449">➤ Para 6.2 – ‘Store’ not ‘make and keep’ copies of important e mails sent and received. JW confirmed that eDRMS can mark e mail as ‘record’.</li> <li data-bbox="368 1482 1310 1543">➤ Para 6.3 – HE suggested that this requirement is checked against ‘Plain English’ requirements.</li> <li data-bbox="368 1576 1310 1693">➤ Para 6.8 – FS noted classifications of ‘Protect’ and ‘Restricted’ and reference to GCSx but felt that there needed to be more definition/explanation around this subject. HF advised that this is work in progress.</li> </ul> <p data-bbox="320 1727 1294 1787"><b>Action:</b> AW/HF will amend the Policy as suggested but track changes and present the revised Policy to the next meeting.</p> <p data-bbox="320 1821 746 1850"><b>Internet Acceptable Usage Policy</b></p> <p data-bbox="320 1883 1214 1944">AW introduced the Policy to the Group. Observations were provided to AW including:</p> <ul data-bbox="368 1977 863 2067" style="list-style-type: none"> <li data-bbox="368 1977 863 2007">➤ Take ‘Acceptable’ out of title of Policy</li> <li data-bbox="368 2040 863 2067">➤ Take para 6.9 out or amend</li> </ul>	<p data-bbox="1366 501 1445 530"><b>SD/IK</b></p> <p data-bbox="1366 734 1445 763"><b>HF/IK</b></p> <p data-bbox="1390 949 1422 978"><b>IK</b></p> <p data-bbox="1358 1727 1453 1756"><b>AW/HF</b></p>

ITEM		Action by
	<ul style="list-style-type: none"> <li>➤ Check Appendix 1 is the latest version</li> <li>➤ Para 6.3 - CD suggested that reference should be made to the fact that NYCC's liability should not extend to use of sites that are accessible through You at Work.</li> <li>➤ Para 6.5 – reference is made to the Council's Software Policy – is there one? <b>Action:</b> AW will follow this up.</li> <li>➤ JSM suggested that the format of the Policy (and other Policies) is brought in line with FCS guidance.</li> <li>➤ It was agreed that the E mail and Internet Usage Policies should go together.</li> </ul> <p><b>Action:</b> AW will amend the Policy as suggested but track changes and present the revised Policy to the next meeting.</p>	
6.4	<p><b>Portable Media and Encryption Policy</b></p> <p>AW explained that the requirement of the Policy is to protect portable data. A discussion took place around how to work on documents at home and Webmail. JSM confirmed that staff should be using the available technology (NYCC issue Blackberry and VPN) when working on documents at home. It was suggested that reference to WebMail should be included in this Policy.</p> <p>JSM also suggested that it would be useful to have an "ICT meets Flexible Working Policy/Statement". This should also be included/made reference to on the Change and Improvement – Flexible Working intranet site.</p> <p><b>Action:</b> AW/JSM/CP to draft a Flexible Working Policy/Statement and present at the next meeting.</p> <p>AW confirmed that the roll out of this Policy will include the disabling of all USB sticks other than encrypted NYCC issued sticks.</p> <p>AW confirmed that access can be still be gained by external consultants using USB sticks to NYCC hardware by making arrangements with the ICT Helpdesk.</p> <p><b>Action:</b> AW will amend the Policy as suggested but track changes and present the revised Policy to the next meeting.</p>	<p><b>AW/JSM/ CP</b></p> <p><b>AW</b></p>
7	<p><b>Set 3 (confirmed for initial discussion @ Meeting 3)</b></p> <p><b>7.1 Scanning Policy</b></p> <p>JW advised that there is ongoing discussion with Legal Services but JW will present a draft Policy to the next meeting.</p> <p><b>7.2 Partnerships and Data Sharing Policy</b></p> <p>SD confirmed that he is in dialogue with RB.</p> <p><b>7.3 Information Security Policy</b></p> <p>AW confirmed that this will be ready for the next meeting.</p>	<p><b>JW</b></p> <p><b>SD/RB</b></p> <p><b>AW</b></p>

ITEM		Action by
8	<b>Set 4 (confirmed for initial discussion @ Meeting 4)</b>	
8.1	<b>Reporting Breach Procedures (Non Technical and Technical) Policy</b>	<b>CC/HF</b>
8.2	<b>Security Labelling Policy</b>	<b>RB</b>
8.3	<b>Data Processing Policy</b>	<b>RB</b>
8.4	<b>Call Recording Policy</b>	<b>RB</b>
9	<p><b>Other Policies to be considered</b></p> <p><b>Use of Social Media Policy and Guidance Note</b></p> <p>JSM explained that this element is not regulated. A discussion took place around the use of social media sites. HE advised that she will add to the draft Policy and include outcomes of discussions with Legal Services.</p> <p>JSM confirmed that this Policy and Guidance will be included in Set 2.</p> <p><b>Action:</b> HE will present the revised Policy to the next meeting as part of Set 2.</p>	<b>HE</b>
<b>PART C</b>	<b>ACTION PLAN</b>	
10	<b>Roll out Plan</b>	
10.1	<p><b>Update on Progress</b></p> <p>HF outlined progress on the Roll out Plan and confirmed that 1to1s have been arranged with DIGCs.</p>	
10.2	<b>Preferred Method of Communication within Directorates</b>	
10.3	<b>Identification of main Information Assets - progress</b>	
10.4	<p><b>Identification of Information Asset Owners - progress</b></p> <p><b>BES</b> –TH advised that the method of communication will be through the leadership team that meets once a month and not through a separate group.</p> <p>Information Audit – this will be co-ordinated by TH's team who will support service areas. TH has already agreed that additional fields should be added.</p> <p><b>ACS</b> – SD advised that he is still working on how to roll out Information Governance although Libraries and Community Services have a ready made structure to do this. It may be necessary to set up a separate Group for the rest of the Directorate.</p> <p>Information Audit - SD advised that he is in the process of identifying the main Information Assets and Information Asset Owners.</p> <p><b>FCS</b> – SL advised that this will be an agenda item on FSMT to discuss the preferred method of communication and how best to identify Information Assets and their Owners. JSM suggested that SL may wish to prioritise. SL is meeting with RB to discuss what is required and how to make best progress.</p>	

ITEM		Action by
	<p><b>CEG</b> – HE advised that the method of communication will be through the CEG management team that meets quarterly.</p> <p>Information Audit – HE has identified Information Owners and Assets and will prioritise and audit. It was suggested that the Customer Service Centre should be dealt with separately. HE is talking to Robin Mair on this subject.</p> <p><b>CYPS</b> – to be advised.</p> <p>HF advised that details of learning and key staff for training will be discussed and identified at 1to1s with Directorates.</p>	
11	<p><b>New Name for Information Essentials (Data Matters) Intranet Site</b></p> <p>No name could be identified.</p> <p><b>Action:</b> HE will ask the Web Team to provide a suggested list for consideration.</p>	<b>HE</b>
<b>PART D</b>	<b>OTHER MATTERS</b>	
12	<p><b>Government Connect</b></p> <p>BES – TH advised that this is being used by Trading Standards.</p> <p>ACS – SD advised that he still needs to find out.</p> <p><b>Action:</b> JSM advised that ALL except BES to report to next meeting. In the meantime AW will ask Dave Sadler to provide details of usage to JSM.</p>	<b>ALL except BES plus AW</b>
13	<p><b>Strategic Transformation and Integration Capability (STIC)</b> – linked to 6.1 and 7.1</p> <p>JW advised that initial investigations show that over 300 multi functional devices (MFDs) are being used for scanning across the County Council. JSM advised that scanning should be done centrally unless there is a good reason for doing it locally ie. there is a substantial business case for carrying out work this way. JSM asked JW to contact DIGCs and respective ICT client officers to find out the following:</p> <ul style="list-style-type: none"> <li>➤ where MFDs are being used for scanning</li> <li>➤ what scanning is taking place</li> </ul> <p><b>Action:</b> JW will report information received to the next meeting as well as to TWIG.</p>	<b>JW</b>
14	<p><b>Violent Warning Marker System</b></p> <p>JSM outlined this system as a corporate database which will record details of potentially violent people that staff may come into contact with as part of their daily working roles. This issue is being dealt with by the Corporate Risk Management Group and at this time all Directorates have given their agreement in principle to such a system proceeding, but further detail is required as to how the system would work in practice. In particular processes around how markers would be communicated to those affected, how they would be reviewed &amp;/or removed and how further details of the type of threat posed would be obtained by those visiting potentially dangerous locations. It is proposed that a group will now be formed by Dominic Passman to discuss and agree those details.</p> <p><b>Action:</b> this Group can be updated when relevant progress has been made.</p>	<b>FS</b>



ITEM		Action by
<p><b>15</b></p> <p><b>15.1</b></p> <p><b>15.2</b></p> <p><b>15.3</b></p>	<p><b>Information Security - compliance with ISO/IEC 27001 and ISO/IEC 27002</b></p> <p><b>Update on Certification for ICT Services</b></p> <p>AW advised that work continues to resolve issues identified in the action plan. It is anticipated that ICT Services is still scheduled to go for certification in October 2010.</p> <p><b>Outcome of:</b></p> <ul style="list-style-type: none"> <li>➤ <b>NYCC and PwC audits</b></li> </ul> <p>Issues identified have been fed into the action plan.</p> <ul style="list-style-type: none"> <li>➤ <b>Audit Committee (29/6/10)</b></li> </ul> <p>JSM confirmed that Audit Committee are satisfied with progress.</p> <p><b>Actions included in Roll-Out Plan – progress?</b></p> <p>AW confirmed that actions identified in the Roll-out Plan have been included in the action plan.</p> <p><b>Action for 15:</b> AW will ensure a further update is provided to the next meeting.</p>	<p><b>AW</b></p>
<p><b>16</b></p> <p><b>16.1</b></p>	<p><b>Records Management</b></p> <p><b>Database of Users of Records Retention and Disposal Schedule – how to keep up to date</b></p> <p>IK advised that the database of users of the Records Management Service is out of date. He confirmed that he will send details to DIGCs and advise how often the database should be updated.</p> <p><b>Action:</b> IK to forward existing list of users of the database to DIGCs. This includes those who have authorised deposits of paper records to the store as well as users of the retention and disposal schedule. DIGCs to update.</p>	<p><b>IK/DIGCs</b></p>
<p><b>17</b></p> <p><b>17.1</b></p> <p><b>17.2</b></p>	<p><b>DPA/FOIA Issues</b></p> <p><b>Councillors - update</b></p> <p>HF reported that there is no change on this item.</p> <p><b>Disclosing Officers Names within FOI Responses</b></p> <p>HF explained that when an FOI request is received which relates to disclosure of names, at the present time only Management Board names are provided. The Group decided that names to Assistant Director level could be advised.</p> <p><b>Action:</b> RB will draft a Policy on this subject and present to the next meeting.</p>	<p><b>RB</b></p>
<p><b>18</b></p> <p><b>18.1</b></p>	<p><b>Internal Audit Reports</b></p> <p><b>Details of 2010/11 Audit Plan that refer to Information Governance</b></p> <p>HF advised that no further audits had been carried out but there are such audits to carry out in 2010/11. HF will keep the Group advised of developments.</p>	

ITEM		Action by
19	<p><b>Coalition Government Latest Proposals</b></p> <p><b>Letter to Govt Depts on opening up data and Publishing itemised local authority expenditure</b> - JSM introduced the papers relating to transparency and the need to publish granular local spending data. JSM advised that he has requested SL to co-ordinate such information from Directorates so that such information is managed in a controlled way when published on the website. JSM asked DIGCs to ensure this information is passed to SL to ensure a co-ordinated approach.</p> <p><b>Action:</b> DIGCs to provide necessary information to SL who will co-ordinate this information and manage it on the website.</p>	<b>DIGCs to SL</b>
20	<p><b>Latest Data Breaches</b></p> <p>Noted. It is requested that CC continues to provide this information and advise if possible the fines that are imposed.</p> <p><b>Action:</b> CC to continue to provide this information to future meetings.</p>	<b>CC</b>
21	<p><b>Information Charter</b></p> <p>It was agreed that an Information Charter is not required and that the existing Information Promise is sufficient. It was suggested that this should be an appendix to the Information Governance Policy.</p> <p><b>Action:</b> HF/JSM will ensure that the Promise is displayed in a prominent position and attached as an appendix to the Information Governance Policy.</p>	<b>HF/JSM</b>
22	<p><b>Items for Subsequent Meetings</b></p> <ul style="list-style-type: none"> <li>➤ Disaster Recovery</li> </ul> <p>This item relates to resilience and storage of electronic data. JSM confirmed that further information would be provided on this issue when it has been resolved.</p>	
23	<p><b>Any Other Business</b></p> <p>None.</p>	

# Corporate Information Governance Officers Group 2

## Meeting 3

**Wednesday, 4 August 2010 @ 2.00pm in Meeting Room 2**

**Attendees**

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

**Champions**

- Sukhdev Dosanjh (SD) - DIGC ACS
- David O'Brien (Do'B) - DIGC CYPS
- Shaun Lee (SL) - DIGC FCS
- Tracy Harrison (TH) - DIGC BES
- Helen Edwards (HE) - DIGC CEG

**Advisors**

- Isabel Esteves (IE) - Legal
- Helen Atkinson (HA) - Legal
- Carol Dickinson (CD) - HR
- Colin Parkin (CP) - HR
- Phil Jones (PJ) - Property
- Kelly Hanna (KH) - HR
- Helen Fowler (HF) - Audit & Information Assurance Manager, Veritau
- Robert Beane (RB) - Information Governance Officer, Veritau
- Colin Cottrell (CC) - Information Security Officer
- Andrew Whittaker (AW) - Head of ICT Architecture
- Ian Kaye (IK) - Records Manager
- Janice Williams (JW) - eDRMS Project Manager
- Simon Wright (SW) - Senior Emergency Planning Officer

**Apologies**

**Apologies**

**Apologies**

**Apologies**

- CC:** Kevin Tharby - CYPS  
 Keith Sweetmore - ACS  
 Max Thomas - Veritau

## ACTION NOTES

ITEM			Action by
<b>PART A</b>	<b>FORMALITIES / STANDING ITEMS</b>		
<b>1</b>	<b>Introductions and Apologies</b> Apologies – see above.		
<b>2</b>	<b>Future meetings for CIGG2 - 2010/11 dates</b>		
	Wednesday 8 September @ 2.00pm	Wednesday 1 December @ 2.00pm	
	Wednesday 27 October @ 2.00pm	Wednesday 19 January 2011 @ 2.00pm	<b>ALL</b>
<b>PART B</b>	<b>POLICY DEVELOPMENT</b>		
<b>3</b>	<b>Consultation/Communication Process</b>		
	<ul style="list-style-type: none"> <li>➤ Corporate Policies applying in schools</li> </ul> <p>CP advised that schools have generally adopted policies and procedures recommended by the County Council. RB advised that the ICO states that schools are independent from NYCC, directly responsible for their actions and considered to be their own data controller.</p>		

ITEM		Action by
	<p><b>Action:</b> JSM requested that CYPs DIGC, RB and IE conclude discussions and advise the Group of the position at the next meeting.</p> <ul style="list-style-type: none"> <li>➤ Minimum communication requirements</li> </ul> <p>HE advised that there is a template available for communications. This is then picked up through the Communications Group which will decide what route eg intranet, is most effective for the communication to go through.</p> <p><b>Action:</b> HE/CP will provide written advice to the Group for further discussion.</p> <ul style="list-style-type: none"> <li>➤ other issues to be clarified <ul style="list-style-type: none"> <li>○ Intranet site – RB advised that prepared material is ready to be put on to the site.</li> </ul> </li> </ul> <p><b>Action:</b> RB to arrange for prepared material to be put on to the site once signed off by JSM – see 4.5 below.</p> <ul style="list-style-type: none"> <li>▪ Consultation with Trade Union on policies being developed– CP advised that there is an existing process for this.</li> </ul> <p><b>Action:</b> CP to provide FS with a copy of the paper for circulation with the notes of the meeting (will be circulated with papers for Meeting 4).</p>	<p><b>DOB/RB/IE</b></p> <p><b>HE/CP</b></p> <p><b>RB/JSM</b></p> <p><b>CP</b></p>
<p><b>4</b></p> <p><b>4.1</b></p> <p><b>4.2</b></p> <p><b>4.3</b></p> <p><b>4.4</b></p> <p><b>4.5</b></p>	<p><b>Set 1 Policies and Strategy – progress on communication to all NYCC staff</b></p> <p><b>Information Governance Policy</b></p> <p><b>Information Governance Strategy</b></p> <p><b>Data Quality Policy</b></p> <p><b>Data Protection Policy</b></p> <p><b>Freedom of Information Policy</b></p> <p>A discussion took place around input from Legal Services for Set 1 draft policies. It was agreed that Legal Services should have a look and comment on Set 1 as soon as possible. On future draft policies it was requested that Legal Services discuss/comment on these prior to the Group meeting.</p> <p>CP also advised that the Policy Statement on these policies should be amended re certain HR related matters. CP will provide the appropriate words.</p> <p>RB advised that there is now a standard format for all policies and this will be agreed with JSM.</p> <p>It is intended that Set 1 will be fully signed off at Meeting 4. HE to then progress to Communication stage.</p> <p><b>Action:</b> IE will provide comments to RB and CC on Set 1 policies.</p> <p>CP to provide the wording for the Policy Statement.</p> <p>JSM/RB to agree standard format for all policies.</p>	<p><b>RB</b></p> <p><b>CP</b></p> <p><b>JSM/RB</b></p>

ITEM		Action by
<p><b>5</b></p> <p><b>5.1</b></p>	<p><b>Set 2 Policies – 2<sup>nd</sup> reading</b></p> <p><b>Records Management Policy</b></p> <p>IK advised that the draft Policy has been amended following comments from HF and SD. It was agreed that this Policy can now be communicated to Directorates and put on the intranet site.</p> <p><b>Action:</b> As soon as HE provides advice on how to communicate to Directorates, IK to carry out necessary action and arrange for the Policy to go on to the intranet site.</p> <p>A discussion took place around building in a review process after all policies have been implemented. It was suggested that this could be informed by audits.</p> <p><b>Action:</b> FS to note requirement for a cyclical review process and put on as an agenda item at a future meeting.</p>	<p><b>HE/IK</b></p> <p><b>FS</b></p>
<p><b>5.2</b></p>	<p><b>E mail Policy</b></p> <p>CC advised that the Policy had been amended in line with the comments previously provided. Some discussion took place around sections 6.2.3 and 6.2.4 with comments from both IE and CP.</p> <p>It was also suggested that reference should be made to:</p> <ul style="list-style-type: none"> <li>▪ e mails relating to charitable walks etc.</li> <li>▪ the retention policy for e mails.</li> </ul> <p><b>Action:</b> CC will amend the Policy as suggested, discuss further with IE and agree correct wording and present the amended Policy to the next meeting.</p>	<p><b>CC/IE</b></p>
<p><b>5.3</b></p>	<p><b>Internet Usage Policy</b></p> <p>CC advised that the Policy had been amended in line with the comments previously provided. CC further advised that some paragraphs from the E Mail Policy will also need to be included.</p> <p>Paragraph 6.3 - further discussion took place around “Personal Use of the Council’s Internet Service”. Suggested amendments included:</p> <ul style="list-style-type: none"> <li>▪ RB will advise the standard protocol to CC.</li> <li>▪ some sort of parallel facility should be looked at such as an intranet social networking site.</li> <li>▪ a separate policy is required to cover high end users (eg below 24 year olds) – JSM said that this is not desirable and would create a ‘dangerous’ precedent re other policies..</li> </ul> <p>Paragraph 6.5 – further discussion took place around “Things you must not do”. DO’B to suggest words linking this paragraph and then a business case to confirm exemptions. It was also decided that there is no need to advise ‘blocked categories of websites’.</p> <p>Paragraph 6.6 – there needs to be a link between this Policy and the Social Networking Policy.</p> <p><b>Action:</b> RB to advise standard protocol on the personal use of the internet service.</p> <p>DO’B will draft a paragraph and then a business case relating to exemptions.</p>	<p><b>RB</b></p> <p><b>DO’B</b></p>

ITEM		Action by
	<p>CC will amend the Policy as suggested but track changes and present the revised Policy to the next meeting.</p> <p>HE to note link required with Social Media Policy.</p>	<p>CC</p> <p>HE</p>
<p>5.4</p>	<p><b>Portable Media and Encryption Policy</b></p> <p>The Group approved this Policy.</p> <p>A discussion then took place around not being able to use personal computers, remote/flexible working and what is sensitive/non sensitive data. It was agreed that TH and SD will look at this further from a Directorate user point of view and provide a policy/statement relating to this matter at the next meeting.</p> <p>CC advised that an acceptable option for this could be use of a hardware encrypted stick.</p> <p>Remote/flexible working should also be referenced in the E Mail, Internet Usage, Portable Media and Encryption and Information Security Policies.</p> <p><b>Action:</b> TH/SD to provide a draft policy/statement relating to remote/flexible working and sensitive/non sensitive data to Meeting 5 on 27 October 2010.</p> <p>CC/RB to reference remote/flexible working in the E Mail, Internet Usage, Portable Media and Encryption and Information Security Policies.</p>	<p>TH/SD</p> <p>CC/RB</p>
<p>5.5</p>	<p><b>Use of Social Media Policy and Guidance Note</b></p> <p>HE advised that this draft Policy has been amended in line with previous comments and also discussions with IE. It was therefore signed off in principle by the Group.</p> <p>HE will make the link with the Internet Usage Policy.</p> <p><b>Action:</b> HE to make the appropriate link with the Internet Usage Policy</p>	<p>HE</p>
<p>6</p> <p>6.1</p>	<p><b>Set 3 (initial discussion @ Meeting 3)</b></p> <p><b>Scanning Policy</b></p> <p>IK introduced the Policy to the Group advising that it relates to corporate scanning and authorised local scanning.</p> <p>JW is obtaining information relating to scanners by location and scanners by Directorate but this is still work in progress.</p> <p>Further work still needs to be done on best practice principles that can be applied to 'to be permitted' local scanning operations eg Pensions.</p> <p>It was noted that the eDRMS information audit identifies every document.</p> <p>There is the issue of documents being scanned and then still being retained. Directorates will be required to provide a business case in these circumstances as there is the cost of the scanning and then also the cost of the storage of documents.</p> <p><b>Action:</b> JW to provide (with assistance from DIGCs) details of local scanning operations.</p> <p>JW to also provide best practice principles that can be applied to local scanning operations.</p>	<p>JW</p> <p>JW</p>

ITEM		Action by
6.2	<p><b>Partnerships and Data Sharing Policy</b></p> <p>RB introduced the Policy to the Group and advised that routine data sharing should be based on this Policy. However links should be made to generic protocol and to individual policies/protocols that already exist so that the intranet site can be comprehensive. RB will need Directorates help with this.</p> <p>A discussion also took place around the disclosure of information and what the appropriate level is.</p> <p><b>Action:</b> DIGCs to identify where local protocols exist which involve NYCC sharing data and advise them to RB.</p> <p>RB will amend the Policy as suggested but track changes and present the revised Policy to the next meeting.</p>	<p><b>DIGCs/RB</b></p> <p><b>RB</b></p>
6.3	<p><b>Information Security Policy</b></p> <p>CC introduced the Policy to the Group and advised that the Policy still needs to go to the Trade Union for consultation. IE will advise legal comments. It was decided that paragraph 5 does not need to list all the Acts, instead it should only be one sentence and provide an example of the legislation.</p> <p><b>Action:</b> CC to consult with the Trade Union.</p> <p>IE to provide legal comments to CC.</p> <p>CC will amend Policy as suggested but track changes and present the revised Policy to the next meeting.</p>	<p><b>CC</b></p> <p><b>IE to CC</b></p> <p><b>CC</b></p>
7	<p><b>Set 4 (confirmed for initial discussion @ Meeting 4)</b></p>	
7.1	<p><b>Reporting Breach Procedures (Non Technical and Technical) Policy</b></p>	<p><b>CC/HF</b></p>
7.2	<p><b>Security Labelling Policy</b></p> <p>CC advised that there is some difficulty in marking policies 'restricted'.</p> <p>Also see item 17.1</p>	<p><b>RB</b></p> <p><b>FS/RB</b></p>
7.3	<p><b>Data Processing Policy</b></p>	<p><b>RB</b></p>
7.4	<p><b>Call Recording Policy</b></p> <p><b>Action:</b> RB and CC confirmed that these Policies will be ready for the next meeting</p>	<p><b>RB</b></p> <p><b>RB/CC</b></p>
8	<p><b>Other Policies to be considered</b></p> <ul style="list-style-type: none"> <li>▪ HE queried the order in which the policies are being introduced to the Group in light of how they should be communicated to NYCC staff. JSM advised that there is a 'world map' (in the Info Gov Strategy – see 4.2 above) which explains the hierarchy. HE should see this to identify possible 'batches' of policies that might best be released as a 'set'. HE to consider and report back.</li> </ul> <p><b>Action:</b> JSM to provide a copy of the 'world map' to assist Communications in advising Policies to NYCC staff. HE to consider and report back.</p> <ul style="list-style-type: none"> <li>▪ It was suggested that a future Policy should be 'Governing Archiving'.</li> </ul> <p><b>Action:</b> Need a volunteer to lead on this, lead to be confirmed at Meeting 4.</p>	<p><b>JSM/HE</b></p> <p><b>ALL</b></p>

ITEM		Action by
<b>PART C</b>	<b>ACTION PLAN</b>	
<b>9</b>	<b>Roll Out Plan</b>	
<b>9.1</b>	<p><b>Update on Progress</b></p> <p>HF advised that the Roll Out plan has been revised as original deadlines are not being met. She confirmed that the Framework has been completed. Training will be the next challenge but the e learning package is nearly ready. TH advised that the learning package will need an Equality Impact Assessment carried out on it. RB will also need to contact Sue Porter, Learning and Development to make sure that the process of going through the QA Group is followed.</p> <p>It was suggested that HF makes the training dates more realistic and if necessary separates each Directorate as each Directorate may move at a different pace and nobody should be held up if they are willing/able to proceed.</p> <p><b>Action:</b> HF to amend Roll Out Plan, amend dates and ensure training can take place in Directorates at the pace they dictate.</p> <p>RB to carry out an EIA for the e learning package and ensure the package follows the process through the QA Group.</p>	<p><b>HF</b></p> <p><b>RB</b></p>
<b>9.2</b>	<p><b>Preferred Method of Communication within Directorates</b></p> <p><b>BES and CEG</b> already advised.</p> <p><b>CYPS</b> – DO'B will review and advise.</p> <p><b>ACS</b> – SD advised that this will be through Directorate Management team.</p> <p><b>FCS</b> – SL advised that this will be through Directorate Management team (FSMT).</p>	<b>DO'B</b>
<b>9.3</b>	<p><b>Identification of main Information Assets – progress</b></p> <p>Deferred until next meeting as little progress to date.</p>	
<b>9.4</b>	<p><b>Information Audit – progress</b></p> <p><b>BES</b> – TH advised that she is still gathering information</p> <p><b>CEG</b> – HE will use information provided via the PwC Organisational Review and the list supplied by IK to provide comprehensive details.</p> <p><b>CYPS</b> – DO'B will now progress.</p> <p><b>ACS</b> – SD will progress. HF will explore where the IAS (client record) system ties in.</p> <p><b>FCS</b> – SL still to identify information asset owners. A pilot audit is being carried out in Central Finance and is proving successful.</p> <p>RB tabled a paper on what an Information Asset Owner is. It is hoped that this will assist DIGCs.</p>	<p><b>TH</b></p> <p><b>HE</b></p> <p><b>DO'B</b></p> <p><b>HF</b></p> <p><b>SL</b></p>
<b>10</b>	<p><b>New Name for Information Essentials (Data Matters) Intranet Site</b></p> <p>The Group agreed that this will be called <b>Information Management</b>.</p>	<b>HF/RB</b>
<b>PART D</b>	<b>OTHER MATTERS</b>	



ITEM		Action by
11	<p><b>Information Governance Implications for Joint Partnership Working</b></p> <p>SD introduced the paper prepared by David Halliday. This has been necessary as a result of communities starting to run libraries where they would otherwise be closed. The example in question is Hawes Library where a voluntary organisation will run the library and use NYCC ICT equipment and materials. Various issues were discussed including:</p> <ul style="list-style-type: none"> <li>➤ how to use ICT equipment and maintain security – there is a particular issue around ‘password reset’ for volunteers.</li> <li>➤ who is the responsible body in the eyes of the ICO, NYCC or the voluntary organisation.</li> <li>➤ what other Councils have already done this.</li> </ul> <p>As this approach may become a recurring theme under the ‘Big Society’ initiative of the Government, JSM suggested that this issue is looked at together with the existing draft Recruiting Volunteers Policy and Guidance and any existing draft Agreement between the voluntary organisation and NYCC.</p> <p><b>Action:</b> FS will contact appropriate people including Legal Services, CPLU and David Halliday and coordinate draft guidance.</p>	FS
12	<p><b>Government Connect</b></p> <p>DO'B advised that there is some difficulty in CYPS using Government Connect that needs to be resolved. CC will assist with this.</p> <p>It was agreed that this item would be reviewed at every other meeting.</p> <p><b>Action:</b> CC to assist CYPS with using Government Connect.</p> <p>FS to put on the agenda for every other meeting (next one 27 October 2010).</p>	CC FS
13	<p><b>Strategic Transformation and Integration Capability (STIC)</b> – linked to 5.1 and 6.1</p> <p>See item 6.1 re local scanning operations.</p>	JW
14	<p><b>Violent Warning Marker System</b></p> <p>JSM advised that this issue appears to be progressing through the Corporate Risk Management Group. Assistance will also be required from DIGCs.</p> <p><b>Action:</b> DIGCs to assist RB in progress.</p>	RB/DIGCs
15 15.1	<p><b>Information Security - update</b></p> <p>CC reported that Information Security has been audited successfully.</p> <p>Although internal breaches are occurring, they are being identified and necessary follow up action is being taken. This is because policies and software are in place.</p> <p>JSM requested that breaches (not technology breaches) are reported to this Group so that DIGCs are made aware. JSM requested that breaches that result from lack of training are distinguished from breaches where policies have not yet been approved and implemented.</p>	
	<p><b>Action:</b>CC to provide details of internal breaches in the manner described above to</p>	CC

ITEM		Action by
	this Group.	
16 16.1	<p><b>Records Management</b></p> <p><b>Database of Users of Records Management Service – how to keep up to date</b></p> <p>Item carried forward to next meeting</p>	IK
17 17.1	<p><b>DPA/FOIA Issues</b></p> <p><b>Disclosing Officers Names within FOI Responses</b></p> <p>RB tabled a paper called Guidance on Publication of Officers' Personal Data. JSM suggested that this Policy is developed rather than the Security Labelling Policy for the next meeting. The Policy will relate to FOI and DP requests only. RB will discuss further with CP and IE and bring back to the next meeting.</p>	
	<p><b>Action:</b> RB to progress a Policy with CP and IE and present it to the next meeting.</p> <p>FS to substitute the Security Labelling Policy for the Publication of Officers' Personal Data Policy in Set 4.</p>	<p>RB</p> <p>FS</p>
18 18.1	<p><b>Internal Audit Reports</b></p> <p><b>Current Audit Reports that refer to Information Governance</b></p> <p>None to report.</p>	
19	<p><b>Coalition Government Latest Proposals</b></p> <p>SL tabled a paper on Transparency in Local Government Spending. He explained that this related amongst other things, to spending over £500 either to an organisation or an individual. This therefore translates into over 200,000 items and may disclose some sensitive information (eg. payments to foster carers).</p> <p>SL advised that a transparency page will be created on the NYCC website with links to relevant information elsewhere on the NYCC website.</p> <p><b>Action:</b> DIGCs to advise SL of relevant areas within their Directorate where information is already publicly available.</p>	DIGCs to SL
20	<p><b>Latest Data Breaches</b></p> <p>CC explained the security breach incident at Birmingham NHS and advised that this can be overcome by using hardware encrypted sticks (see CC's e mail to Group dated 3 August 2010). This is also linked to item 5.4 Portable Media and Encryption Policy.</p> <p>It was agreed that external breaches should be reported at every other meeting (next meeting 27 October 2010).</p> <p><b>Action:</b> CC to amend the Portable Media and Encryption Policy accordingly.</p> <p>FS to note that external breaches are reported at every other meeting.</p>	<p>CC</p> <p>FS</p>
21	<b>Items for Subsequent Meetings</b>	

ITEM		Action by
	<p>➤ Disaster Recovery</p> <p>Carry forward to future meeting.</p>	
22	<p><b>Previous Meeting Notes and Matters Arising from Meeting 2</b></p> <p>Previous Meeting Notes agreed.</p> <p>Matters arising:</p> <p>Information Promise needs to be displayed in a prominent position and attached as an appendix to the Information Governance Policy.</p>	HF/JSM
23	<p><b>Any Other Business</b></p> <p>None</p>	

# Corporate Information Governance Officers Group 2

## Meeting 4

Wednesday, 8 September 2010 @ 2.00pm in Meeting Room 3

### Attendees

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

#### Champions

- Sukhdev Dosanjh (SD) - DIGC ACS
- David O'Brien (Do'B) - DIGC CYPs *Apols – sub Michael Lord*
- Shaun Lee (SL) - DIGC FCS
- Tracy Harrison (TH) - DIGC BES *Apols – sub Joel Sanders*
- Helen Edwards (HE) - DIGC CEG

#### Advisors

- Moirá Beighton (MB) - Legal
- Carol Dickinson (CD) - HR *Apols*
- Colin Parkin (CP) - HR
- Helen Fowler (HF) - Audit & Information Assurance Manager, Veritau
- Robert Beane (RB) - Information Governance Officer, Veritau
- Colin Cottrell (CC) - Information Security Officer
- Andrew Whittaker (AW) - Head of ICT Architecture *Apols*
- Ian Kaye (IK) - Records Manager
- Janice Williams (JW) - eDRMS Project Manager *Apols for part of the meeting*
- Simon Wright (SW) - Senior Emergency Planning Officer

- CC:** Kevin Tharby CYPs  
 Robin Mair CEG  
 Keith Sweetmore ACS  
 Phil Jones Property  
 Kelly Hanna HR  
 Max Thomas Veritau

## ACTION NOTES

ITEM		Action by
<b>PART A</b>	<b>FORMALITIES / STANDING ITEMS</b>	
<b>1</b>	<b>Introductions and Apologies</b> Apologies – see above.	
<b>2</b>	<b>Future meetings for CIGG2 - 2010/11 dates</b>  Wednesday 27 October @ 2.00pm                      Wednesday 19 January 2011 @ 2.00pm  Wednesday 1 December @ 2.00pm  <b>Schedule of further meeting dates – agreed.</b>  Advance apologies from JSM for 16 March 2010 meeting.	
<b>PART B</b>	<b>POLICY DEVELOPMENT</b>	

ITEM		Action by
3	<p><b>Consultation/Communication Process</b></p> <ul style="list-style-type: none"> <li>➤ Corporate Policies applying in schools</li> </ul> <p>CP/ML reported that advice and support is provided to schools by the Council. RB confirmed that the ICO states that schools are independent from the Council, directly responsible for their actions and considered to be their own data controller. Information Governance is a clear responsibility of the school governing body.</p> <p><b>Action:</b> CYPS DIGC will ensure that policies, guidance and advice approved by this Group will be provided to schools although it is recognised that each school is free to adopt, amend or reject these as they see fit.</p> <ul style="list-style-type: none"> <li>➤ Minimum communication requirements</li> </ul> <p>HE tabled a paper providing guidance on communication requirements and opportunities – <b>to follow</b>. This should be used in conjunction with the advice from HR on consultation and communication (see item below).</p> <p>The onus of communicating a Policy is on the Policy owner.</p> <p>It was discovered that there is presently no link between Veritau/RB and the Communications Group and this should be rectified.</p> <p>For the policies that have been approved by this Group, JSM will discuss with HE/RB and decide the appropriate channel of communication as the policies are loaded onto the intranet.</p> <p><b>Action:</b> Establish link between Veritau and the Communications Group.</p> <p style="padding-left: 40px;">JSM/HE/RB to discuss appropriate channel of communication and load polices onto the intranet.</p> <ul style="list-style-type: none"> <li>➤ Consultation with Trade Union on policies being developed</li> </ul> <p>The draft guidance was discussed. It was suggested that examples of policies that require formal consultation or informal consultation should be given to make the appropriate consultation clearer.</p> <p><b>Action:</b> CP to provide a further version showing examples to the next meeting.</p> <ul style="list-style-type: none"> <li>➤ other issues to be clarified</li> </ul> <ul style="list-style-type: none"> <li>• Communication of policies – it was suggested that a 2 tier approach should be taken; a detailed document should be provided to this Group and then a summary communicated to employees. The summary should then have a signpost to the more detailed document for reference on the intranet site.</li> </ul> <p>The Policy owner is responsible for producing the summary.</p> <p><b>Action:</b> Policy owners to produce a summary (use friendly version) of their policies.</p>	<p><b>DO'B</b></p> <p><b>Advisors</b></p> <p><b>HE/RB</b></p> <p><b>JSM/HE/RB</b></p> <p><b>CP</b></p> <p><b>Advisors</b></p>
4	<b>Set 1 Policies and Strategy – progress</b>	

ITEM		Action by
<p>4.1</p> <p>4.2</p> <p>4.3</p> <p>4.4</p> <p>4.5</p>	<p><b>Information Governance Policy – signed off?</b></p> <p><b>Information Governance Strategy – signed off?</b></p> <p><b>Data Quality Policy – signed off?</b></p> <p><b>Data Protection Policy – signed off?</b></p> <p><b>Freedom of Information Policy – signed off?</b></p> <p>Legal Services have provided their comments on these policies and they have been amended where necessary.</p> <p>RB will ensure that these policies are in the correct format, pass them to JSM for final comment and then communicate them through the appropriate channel.</p> <p>It was suggested that the policies are revisited every 6 months to ensure they are up to date.</p> <p><b>Action:</b> JSM/RB to agree standard format of policies and arrange appropriate communication.</p> <p>FS to ensure a cyclical review process for policies is put in place.</p>	<p><b>JSM/RB</b></p> <p><b>FS</b></p>
<p>5</p> <p>5.1</p> <p>5.2</p>	<p><b>Set 2 Policies – 3rd reading of revised Policies</b></p> <p><b>Records Management Policy – ready for sign off?</b></p> <p>IK advised that the Policy has been reformatted. JSM suggested that RB/IK carry out a final check before the Policy moves on to the appropriate channel of communication. Otherwise this Policy has been signed off by the Group.</p> <p><b>Action:</b> RB/IK to check format and then arrange appropriate communication.</p> <p><b>E mail Policy</b></p> <p>CC advised that the Policy had been amended in line with the comments previously provided. Further discussion took place and amendments included the following:</p> <ul style="list-style-type: none"> <li>• How to deal with reference to the Acts</li> <li>• How to highlight that work time should not be used to send personal e mails</li> <li>• Reference in para 6.3 to an e mail signature is ambiguous and needs clarification. RB advised that the signature should be controlled by the owner of the signature.</li> </ul> <p><b>Action:</b> MB to provide assistance to CC on how to ensure reference is made to up to date legislation without having to amend the Policy document on a regular basis (applies to all relevant policies).</p> <p>MB to provide a legal statement which highlights that work time should not be used to send personal e mails (applies to all relevant policies).</p> <p>RB to provide assistance to CC regarding guidance on e mail signatures.</p> <p>CC will amend the Policy as suggested and present the revised Policy to the next meeting.</p>	<p><b>RB/IK</b></p> <p><b>MB/CC and Advisors</b></p> <p><b>MB/CC and Advisors</b></p> <p><b>RB/CC</b></p> <p><b>CC</b></p>
<p>5.3</p>	<p><b>Internet Usage Policy</b></p>	

ITEM		Action by
5.4	<p>CC advised that the Policy had been amended in line with the comments previously provided. Discussion took place and further amendments included the following:</p> <ul style="list-style-type: none"> <li>• Para 6.4 – reference to disciplinary needs to be changed</li> <li>• How to deal with reference to the Acts</li> </ul> <p><b>Action:</b> MB to provide assistance to CC on how to ensure reference is made to up to date legislation without having to amend the Policy document on a regular basis.</p> <p>MB to provide a legal statement which highlights that work time should not be used to surf the internet on personal issues.</p> <p>CC will amend the Policy as suggested and present the revised Policy to the next meeting.</p> <p><b>Portable Media and Encryption Policy – ready for sign off</b></p> <p>CC advised that the Policy had been amended in line with the comments previously provided.</p> <p>TH/SD will provide a draft Policy/statement relating to remote/flexible working and sensitive/non sensitive data to the next meeting. This is to assist in overcoming the problem of being unable to use personal computers when working at home and the inability to use non NYCC encrypted USB sticks.</p> <p>Further comments were provided to CC on the current Policy.</p> <p><b>Action:</b> CC to amend the Policy with the comments that were provided.</p> <p>TH/SD to provide a draft Policy/statement relating to remote/flexible working and sensitive/non sensitive data to the next meeting.</p>	<p><b>MB/CC</b></p> <p><b>MB/CC</b></p> <p><b>CC</b></p> <p><b>CC</b></p> <p><b>TH/SD</b></p>
5.5	<p><b>Use of Social Media Policy and Guidance Note – ready for sign off</b></p> <p>HE advised that she is amending the Policy into the agreed format, incorporating comments from Legal Services and including references to the use of social media at home which could bring the Council into disrepute.</p> <p><b>Action:</b> HE will amend the Policy, circulate to the Group for final comments and sign off.</p>	<p><b>HE/ALL</b></p>
6	<p><b>Set 3 – 2nd reading of revised Policies</b></p>	
6.1	<p><b>Scanning Policy</b></p> <p>JW advised that the Policy had been amended in line with the comments previously provided. Further discussion took place and amendments included the following:</p> <ul style="list-style-type: none"> <li>• Para 1.3 – ‘notable exceptions’ should be amended to read ‘permitted exceptions’</li> <li>• Para 6.1 – ‘valid business reasons’ should be amended to read ‘permitted reasons’</li> <li>• Para 3.1 – the scope needs to define to whom the Policy applies to, for example, does it apply to schools</li> <li>• Para 9.9 should be in para 6 ‘Applying the Policy’</li> </ul>	<p><b>IK/JW</b></p>
	<ul style="list-style-type: none"> <li>• Paras 1.3 and 1.4 should include reference to back scanning</li> </ul>	

ITEM		Action by
	<p>JS queried what the use of the central scanning bureau is based on. JW advised that because the present amount of local scanning is not known then it is not possible to decide what use there will be for the CSB. JSM advised that we should agree a Policy and then look at local scanning.</p> <p>JW circulated a list of current local scanning facilities derived from the corporate ICT asset register. JW will arrange meetings with the DIGCs to obtain information on where the facility is in the Directorate, what the service function is, and volume/frequency of use. JSM suggested that DIGCs obtain assistance from their Directorate ICT Client Officer.</p> <p><b>Action:</b> JW will amend the Policy as suggested and present the revised Policy to the next meeting.</p> <p>JW to arrange meetings with DIGCs before the next meeting date of 27 October 2010 to obtain further information on local scanning facilities and present her findings to the next meeting.</p> <p><b>6.2 Partnerships and Data Sharing Policy</b></p> <p>RB advised that the Policy had been amended in line with the comments previously provided. Discussion took place and further amendments included the following:</p> <ul style="list-style-type: none"> <li>• Rename the Policy “External Data Sharing”</li> <li>• Policy should not apply to Members</li> <li>• Legal Services will provide their further comments on this Policy to RB.</li> </ul> <p><b>Action:</b> RB will amend the Policy as suggested, receive further comments from MB and present the revised Policy to the next meeting.</p> <p><b>6.3 Information Security Policy</b></p> <p>CC advised that the Policy had been amended in line with the comments previously provided. Discussion took place and further amendments included the following:</p> <ul style="list-style-type: none"> <li>• HE advised the scope needs further clarification</li> <li>• JSM suggested that as this Policy applies to information on paper as well as electronic information this should be highlighted more clearly.</li> <li>• Para 6.2 – it was suggested that the wording should state that it would be good practice to include awareness training in the induction process rather than ‘should be included’.</li> <li>• Para 6.3 – information security expectations will not be included in job descriptions. May be best to refer to the code of conduct.</li> <li>• Include a standard para relating to the obligation of the worker (rather than employee) which should then also cover volunteers.</li> <li>• Para 6.11 and 6.13 – change information department to ICT</li> <li>• Para 7 to include a standard paragraph provided by Legal Services.</li> </ul> <p><b>Action:</b> CC will amend the Policy as suggested, receive further comments from MB and present the revised Policy to the next meeting.</p>	<p><b>JW</b></p> <p><b>JW/DIGCs</b></p> <p><b>RB/MB</b></p> <p><b>CC/MB</b></p>
<p><b>7</b></p> <p><b>7.1</b></p>	<p><b>Set 4 (initial discussion @ Meeting 4)</b></p> <p><b>Reporting Breach Procedures (Non Technical and Technical) Policy</b></p>	



ITEM		Action by
7.2	<p>CC and HF introduced the Policy and Procedure to the Group.</p> <p>A discussion took place and it was agreed that the two documents should be amalgamated into one document and be renamed.</p> <p><b>Action:</b> CC/HF will carry out some further work on this and present a revised Policy and Procedure as one document to the next meeting.</p> <p><b>Disclosure of Personal Data of Officers and Members Policy</b></p> <p>RB introduced the Policy to the Group. JSM asked how people would know if this applied to them and RB advised that they would find out like any other issue that may apply in the course of their work. RB advised that at the present time people are asked for their consent to disclose personal data and referred the Group to Appendix A for comment. It was also asked whether the Policy applies to volunteers.</p> <p>JSM suggested that CP and MB provide their comments on the Policy and then it should be referred to ACS and CYPs DIGCs in particular for comment.</p> <p><b>Action</b> RB will carry out some further work as mentioned above with colleagues and present a revised Policy to the next meeting.</p>	CC/HF
7.3	<p><b>Data Processing Policy</b></p> <p>RB introduced the Policy to the Group. It was questioned whether the Policy applied to contractors.</p> <p>JSM suggested that MB provides comments from Legal Services on the Policy.</p> <p><b>Action:</b> RB will carry out some further work with MB and present a revised Policy to the next meeting.</p>	RB/ACS and CYPs DIGCs
7.4	<p><b>Call Recording Policy</b></p> <p>RB introduced the Policy to the Group. It was questioned whether the Policy had been referred to Robin Mair and Sarah Foley. HE confirmed that she would refer it on.</p> <p>It was suggested that the Telephone User Policy could be included within this Policy.</p> <p><b>Action:</b> HE to refer to Robin Mair and Sarah Foley for comment and possible inclusion of the telephone usage Policy.</p> <p>RB to carry out some further work with HE and present a revised Policy to the next meeting.</p>	RB/MB  HE  HE/RB
8	<p><b>Set 5 (for initial discussion at Meeting 5)</b></p> <p><b>8.1 Security Labelling (Marking) Policy</b></p> <p>It was confirmed that this Policy would be discussed at Meeting 5. A discussion took place around the name of this Policy, what categories of security would apply, what these categories would mean to Directorates, how it could be applied intelligently in Directorates etc.</p>	RB
8.2	<p><b>Action:</b> RB will do some prior work with DIGCs to determine the best way forward.</p> <p><b>Archiving Policy</b></p>	RB/DIGCs

ITEM		Action by
	It was decided that this Policy would be deferred until other Policies have been approved and communicated.	
9	<p><b>Other Policies to be drafted?</b></p> <p>None at this time.</p>	
<b>PART C ACTION PLAN</b>		
10	<b>Roll Out Plan</b>	
10.1	<p><b>Update on Progress</b></p> <p>HF advised that the Roll Out Plan has been revised as original dates were not realistic.</p> <p>HF will consult with the Learning and Development Unit on a realistic date for the completion of the e learning package.</p> <p>HF will find out what date is realistic for information to be loaded onto the intranet site.</p> <p>It was advised that the Information Security Group and the PIGG no longer exist.</p> <p>It was suggested that HF tracks updates to the Roll Out Plan so that everyone can identify changes.</p> <p><b>Action:</b> HF to amend Plan with realistic dates and highlight future changes in the Plan so that they are easier to follow.</p>	HF
10.2	<p><b>EIA for e Learning Package</b></p> <p>Deferred to next meeting.</p>	RB
10.3	<p><b>Preferred Method of Communication within CYPS Directorate</b></p> <p>ML advised that CYPS are forming a Directorate Information Governance Group which will report to the leadership team and be chaired by DO'B.</p>	DO'B
10.4	<p><b>Identification of Information Asset Owners – progress</b></p> <p>In progress.</p>	DIGCs
10.5	<p><b>Information Audit – progress</b></p> <p>In progress. RB will provide practical examples of what an information asset is to DIGCs.</p>	DIGCs
11	<p><b>Information Management Intranet Site – update on position</b></p> <p>RB advised that this will be updated and populated when Policies are signed off and communication methods confirmed.</p>	RB
<b>PART D OTHER MATTERS</b>		
12	<b>Information Governance Implications for Joint Partnership Working/Big Society - update</b>	

ITEM		Action by
	FS advised that this is in progress.	FS
13	<p><b>Strategic Transformation and Integration Capability (STIC)</b> – linked to 5.1 and 6.1</p> <p>Deferred to next meeting.</p>	JW
14	<p><b>Violent Warning Marker System - update</b></p> <p>RB advised that he is meeting with Wendy Parkin and will advise progress to the next meeting.</p>	RB
15	<p><b>Information Security</b></p>	
15.1	<p><b>Update</b></p> <p>Deferred to next meeting.</p>	CC
15.2	<p><b>Latest Breaches – internal</b></p> <p>CC advised that he will circulate details to the Group - <u>see attached</u>.</p>	CC
16	<p><b>Records Management</b></p>	
16.1	<p><b>Database of Users of Records Management Service – how to keep up to date</b></p> <p>Deferred to next meeting. IK advised that the database of users has been circulated to DIGCs. The next step is for DIGCs to confirm information asset owners which may then feed back into updating the database.</p>	IK/DIGCs
17	<p><b>DPA/FOIA Issues</b></p>	
17.1	<p><b>Circulation of FOI requests</b></p> <p>RB advised that the FOI User Group does not exist corporately and so the question arose around how to keep the FOI responder list in Directorates up to date. It was confirmed that Geoff Wall/Gary Fielding/JSM will continue to act as ‘the sieve’.</p> <p>Other practical issues will need to be considered.</p> <p><b>Action:</b> RB to provide a paper on issues to be resolved for discussion at the next meeting.</p>	RB
17.2	<p><b>Internal audit report</b> (see 18.1 below)</p>	
17.3	<p><b>Charging for FOI requests</b></p> <p>Deferred to next meeting.</p>	RB
18	<p><b>Internal Audit Reports</b></p>	
18.1	<p><b>Current Audit Reports that refer to Information Governance</b></p> <ul style="list-style-type: none"> <li>➤ PwC audit report/NYCC response</li> </ul>	
	<p>HF advised that the report has been circulated to the Group for information.</p> <p>Suggestions were made by PwC, satisfactory answers have been provided or suggestions have been challenged by NYCC.</p>	

ITEM		Action by
	<ul style="list-style-type: none"> <li>➤ Draft Freedom of Information audit report</li> </ul> <p>HF advised that the report has been circulated to the Group for information. This is also linked to 17.2 and 17.3 above.</p>	
<p><b>19</b></p> <p><b>19.1</b></p> <p><b>19.2</b></p>	<p><b>Coalition Government Latest Proposals</b></p> <p><b>Publishing itemised local authority expenditure update</b></p> <p>Deferred to next meeting.</p> <p><b>Anything new?</b></p> <p>Nothing to report.</p>	<p><b>SL/DIGCs</b></p>
<p><b>20</b></p>	<p><b>Items for Subsequent Meetings</b></p> <ul style="list-style-type: none"> <li>➤ Disaster Recovery</li> </ul> <p>Carry forward to future meeting.</p> <ul style="list-style-type: none"> <li>➤ Draft Policy/statement relating to remote/flexible working and sensitive/non sensitive data</li> </ul> <p>Will be an item on Meeting 5 agenda (see item 5.4).</p> <ul style="list-style-type: none"> <li>➤ Government Connect</li> </ul> <p>Will be an item on Meeting 5 agenda.</p> <ul style="list-style-type: none"> <li>➤ Details of external breaches</li> </ul> <p>Will be an item on Meeting 5 agenda.</p>	<p><b>Dave Sadler</b></p> <p><b>TH/SD</b></p> <p><b>DIGCs</b></p> <p><b>CC</b></p>
<p><b>21</b></p>	<p><b>Matters Arising from Meeting 3 not mentioned elsewhere on agenda</b></p> <p>None.</p>	
<p><b>23</b></p>	<p><b>Any Other Business</b></p> <ul style="list-style-type: none"> <li>➤ JSM referred to the e mail that was circulated relating to a request for information from Mr Schneider (linked to item 7.2).</li> </ul> <p><b>Action:</b> SL will lead on the implications of this request at the next meeting.</p> <ul style="list-style-type: none"> <li>➤ FS suggested that a Sharepoint site should be created and further documentation placed on the site for future meetings rather than circulated by e mail. This was agreed by the Group.</li> </ul> <p><b>Action:</b> CC to assist FS in creating a Sharepoint site for CIGG 2 documents.</p>	<p><b>SL</b></p> <p><b>CC/FS</b></p>

# Corporate Information Governance Officers Group 2

## Meeting 5

**Wednesday, 27 October 2010 @ 2.00pm in Meeting Room 2**

**Attendees**

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

**Champions**

- Sukhdev Dosanjh (SD) - DIGC ACS Apologies
- Larry Orlando (LO) - ACS **Sub for Sukhdev Dosanjh**
- David O'Brien (Do'B) - DIGC CYPS
- Shaun Lee (SL) - DIGC FCS
- Tracy Harrison (TH) - DIGC BES
- Helen Edwards (HE) - DIGC CEG

**Advisors**

- Moira Beighton (MB) - Legal **Apologies**
- Isobel Esteves - Legal **Sub for Moira Beighton**
- Carol Dickinson (CD) - HR
- Helen Fowler (HF) - Audit & Information Assurance  
Manager, Veritau
- Robert Beane (RB) - Information Governance Officer,  
Veritau
- Colin Cottrell (CC) - Information Security Officer
- Dominic Passman - Health & Safety **Attended for item 15**
- Dave Sadler - ICT **Attended for item 6.1b**
- Ian Kaye (IK) - Records Manager
- Janice Williams (JW) - eDRMS Project Manager
- Simon Wright (SW) - Senior Emergency Planning  
Officer **Apologies**
- Phil Jones - Property **Apologies**

- CC:** Kevin Tharby - CYPS
- Robin Mair - CEG
- Keith Sweetmore - ACS
- Kelly Hanna - HR
- Max Thomas - Veritau

## ACTION NOTES

ITEM		Action by
<b>PART A</b>	<b>FORMALITIES / STANDING ITEMS</b>	
<b>1</b>	<b>Introductions and Apologies</b> Apologies – see above.	
<b>2</b>	<b>Future meetings for CIGG2 - 2010/11 dates</b>	
	<div style="display: flex; justify-content: space-between;"> <span>Wednesday 1 December @ 2.00pm</span> <span>Wednesday 19 January 2011 @ 2.00pm</span> </div> <p>Future dates will be forwarded to diaries</p>	

ITEM		Action by
<b>PART B</b>	<b>POLICY DEVELOPMENT</b>	
<p><b>3</b></p> <p><b>3.1</b></p> <p><b>3.2</b></p> <p><b>3.3</b></p> <p><b>3.4</b></p>	<p><b>Consultation/Communication Process</b></p> <p>➤ Communication requirements and methods - update</p> <p>HE advised that the intranet needs to be populated before Frequently Asked Questions can be developed. Once this is done the Communication Plan can be populated and fed into the ICT Communications Group.</p> <p><b>Action:</b> CC/RB/IK to populate the intranet which will enable the production of the FAQs.</p> <p>HE to populate the Communication Plan for the attention of the ICT Comms Group.</p> <p>HE/HF will ensure the Communication Plan links in with the Roll Out Plan.</p> <p>➤ Communication requirements and methods - link with Veritau</p> <p>See above.</p> <p>➤ Guidance on consultation stages</p> <p>CD went through her e mail dated 25 October 2010 that was circulated to the Group. She advised that there are monthly meetings with Unison, the next one on the 2 November and then 14 December 2010. She advised that it is necessary to send a summary of the key issues in a Policy to the Union for consideration before the meeting and it is important to give realistic timescales. She suggested that a simultaneous consultation can be carried out with the Union at the same time as consideration of a Policy by this Group in order to speed the process up.</p> <p>CD advised that the Teaching Unions meet four times a year.</p> <p><b>Action:</b> All policies that need consultation with the Union should be sent in the agreed format (as per previous discussions and CD's e mail) to Wendy Nichol, copy to Ann Ward in readiness for the meeting on 2 November 2010 or if necessary, 14 December 2010. Anyone sending policies for consultation should attend the meeting.</p> <p>RB/CC/IK/HE need to devise a system which forms a sub loop of the consultation with the Union. The timetable will sensibly link with the timetable in the Communications Plan.</p> <p>➤ Other issues to be clarified</p> <p>None.</p>	<p><b>CC/RB/IK</b></p> <p><b>HE</b></p> <p><b>HE/HF</b></p> <p><b>Advisors</b></p> <p><b>RB/CC/IK/HE</b></p>
<p><b>4</b></p> <p><b>4.1</b></p> <p><b>4.2</b></p> <p><b>4.3</b></p> <p><b>4.4</b></p> <p><b>4.5</b></p>	<p><b>Set 1 Policies and Strategy – progress</b></p> <p><b>Information Governance Policy</b></p> <p><b>Information Governance Strategy</b></p> <p><b>Data Quality Policy</b></p> <p><b>Data Protection Policy</b></p> <p><b>Freedom of Information Policy</b></p>	

ITEM		Action by
	<p><b>Action:</b> RB to put all policies into the agreed standard format together with an appropriate summary for consultation with the Union.</p> <p>HE will draft the Communications Plan to show the timing for all policies including policies mentioned in item 5 onwards.</p>	<p><b>RB</b></p> <p><b>HE</b></p>
<p><b>5</b></p> <p><b>5.1</b></p> <p><b>5.2</b></p> <p><b>5.3</b></p> <p><b>5.4</b></p> <p><b>5.5</b></p>	<p><b>Set 2 Policies – ready for sign off?</b></p> <p><b>Records Management Policy – progress on standard format and communication</b></p> <p><b>Action:</b> IK will send this Policy in the agreed format together with the appropriate summary to the Union for consultation with them on the 2 November 2010.</p> <p><b>E mail Policy</b></p> <p>CC advised that he had received assistance from MB/IE on legal issues. RB had provided advice on e mail signatures.</p> <p><b>Action:</b> CC will send this Policy in the agreed format together with the appropriate summary to the Union for consultation with them on the 2 November 2010.</p> <p><b>Internet Usage Policy</b></p> <p>CC advised that he had received assistance from MB/IE on the legal issues raised and amended the Policy accordingly.</p> <p><b>Action:</b> CC will send this Policy in the agreed format together with the appropriate summary to the Union for consultation with them on the 2 November 2010.</p> <p><b>Portable Media and Encryption Policy – progress on standard format and communication</b></p> <p><b>Action:</b> CC will send this Policy in the agreed format together with the appropriate summary to the Union for consultation with them on the 2 November 2010.</p> <p><b>Draft Options Appraisal of Remote/Flexible Working relating to Sensitive/Non Sensitive Data</b></p> <p>TH provided a précis of the paper that was circulated with the agenda. She advised that a lot of ad hoc work of a non sensitive nature is being done on home computers. It was suggested that perhaps the 3 options provided in the paper are the options that should be considered by the manager and the manager then decides as a result of the nature of the work what option should be taken.</p> <p>It was agreed that it should be possible to identify what information is sensitive/non sensitive following the information audit.</p> <p>A discussion took place around the different classifications for information and that it is necessary to provide interim guidance with examples which say what is permissible on home computers.</p> <p>It was agreed that the guidance relating to the type of documents that can be worked on upon home computers should also be applied to WebMail.</p> <p>TH will also discuss this issue with Richard Flinton in relation to the corporate work that she is carrying out with him.</p>	<p><b>IK</b></p> <p><b>CC</b></p> <p><b>CC</b></p> <p><b>CC</b></p>

ITEM		Action by
	<p>Any policies/guidance will cross reference with the existing Home Working Policy.</p> <p><b>Action:</b> TH/SD/CC to produce a set of Guidance Notes for managers relating to the options available for ad hoc working from home linked to the type of information (sensitive/non sensitive) that can be worked on when using those options.</p> <p>TH to discuss this issue with Richard Flinton in relation to the work that she is carrying out with him.</p> <p>TH to ensure any Policy/guidance notes link back to the existing Home Working Policy.</p>	<p><b>TH/SD/CC</b></p> <p><b>TH</b></p> <p><b>TH</b></p>
<p><b>5.6</b></p>	<p><b>Use of Social Media Policy and Guidance Note</b></p> <p>HE confirmed that she has incorporated comments from Legal Services and HR. She will discuss and agree further with Justine Brooksbank.</p> <p><b>Action:</b> HE to discuss and agree with Justine Brooksbank.</p> <p>HE to send this Policy in the agreed format together with the appropriate summary to the Union for consultation with them on the 2 November 2010.</p>	<p><b>HE</b></p> <p><b>HE</b></p>
<p><b>6</b></p> <p><b>6.1</b></p> <p><b>6.1a</b></p>	<p><b>Set 3 – 3<sup>rd</sup> reading of revised Policies</b></p> <p><b>Scanning Policy</b></p> <p>JW advised that IK is the owner of this Policy. She further advised that paras 1.3 and 1.4 refer to local scanning and para 6.5 relates to permitted local scanning.</p> <p>TH noted that the Policy states that it is to be reviewed quarterly and it was suggested that this may be too frequent. JSM suggested that this Policy will fall in line with the cyclical review of all policies.</p> <p>TH advised that scanning is included in her review of business support and administration. TH/JW confirmed that they would meet to discuss both pieces of work being carried out in mid November.</p> <p>It was agreed that this Policy would be held back until local scanning investigations have been completed.</p> <p><b>Action:</b> JW to continue her review of local scanning arrangements and include the conclusions of this review in the conclusion of this Policy.</p> <p>TH to feed in any conclusions from the review of business support and administration that she is carrying out.</p> <p><b>Review of local scanning arrangements</b></p> <p>JW tabled a paper on Local Scanning (e copy to follow) and advised the conclusions and recommendations of the outcome of her recent meetings with DIGCs. She advised that there has been some confusion and misinterpretation of what a scanner is and further work needs to be done with Directorates to clarify the position. However interim work suggests that there are many less scanners than first thought. It should also be possible to reduce the need for local scanners further as MFDs have/will have the functionality to do local scanning in a secure manner.</p> <p>HE suggested that if MFDs are used for local scanning as well as printing, this may cause a blockage and create criticism. This also needs to be taken into account.</p>	<p><b>JW</b></p> <p><b>TH</b></p>



ITEM		Action by
	<p>TH advised that there is a cross over with Comms and BES as a result of the business process review that is ongoing in BES and that JW needs to take this into account.</p> <p>It was agreed that DIGCs continue to be involved in assessing the business needs for local scanning.</p> <p><b>Action:</b> JW will continue to work with DIGCs to review where scanners are located, why they are there and what they are used for.</p> <p>JW will advise the outcome of her further work with ICT Client Officers and Ricoh on the additional functionality of MFDs and how they can be used for local scanning etc. and thus reduce the number of local scanners.</p> <p>JW will discuss the use of the Central Scanning Bureau for scanning correspondence with Joel Sanders in BES.</p>	<p><b>JW/DIGCs</b></p> <p><b>JW</b></p> <p><b>JW/Joel Sanders</b></p>
<p><b>6.1b</b></p>	<p><b>ICT issues per scanning</b></p> <p>DS advised that investigations are ongoing to identify where scanners are and what they are being used for within the organisation versus use of the scanning bureau. The other issue that is being investigated is the location of MFDs in relation to local scanners and also whether they can be used from a security point of view. DS then asked JW to advise the present position on investigations regarding local scanning arrangements. (see item 6.1a)</p> <p><b>Action:</b> see item 6.1a.</p>	<p><b>JW</b></p>
<p><b>6.2</b></p>	<p><b>External Data Sharing Policy</b></p> <p>JSM queried the name of the Policy. It was agreed that it would be called 'Information Sharing with Partners' Policy.</p> <p>RB advised that the Policy has been amended in line with the comments previously provided. Discussion took place and further amendments include the following:</p> <ul style="list-style-type: none"> <li>• Scope – this should be changed to 'This Policy applies inclusively to all services and Directorates of the Council in relation to information being provided to Partners to the organisation.'</li> <li>• All reference to Departments should be amended to Directorates.</li> </ul> <p><b>Action:</b> RB will amend the Policy as suggested and present the revised Policy to the next meeting.</p> <p>Simultaneously, RB will send this Policy in the agreed format together with the appropriate summary to the Union for consultation with them on the 2 November 2010.</p>	<p><b>RB</b></p> <p><b>RB</b></p>
<p><b>6.2a</b></p>	<p><b>Consultation on data sharing code of practice</b></p> <p>JSM asked RB for his comments on this. RB advised that he is not familiar with this consultation from the Information Commissioner's Office. RB will do some research on this and build his findings into the review of the Policy.</p> <p>JSM advised that the Connect Partnership work being carried out by Robin Mair and Gary Fielding needs to be linked in with this review and Policy.</p> <p><b>Action:</b> RB will familiarise himself with this consultation and report back its implications on the draft Policy to the next meeting.</p>	<p><b>RB</b></p>

ITEM		Action by
6.3	<p>RB will link in the Connect Partnership work that is being carried out by Robin Mair and Gary Fielding.</p> <p><b>Information Security Policy</b></p> <p>CC advised that previous comments and suggestions have been incorporated into the Policy.</p> <p>A discussion took place around para 6.2 and ICT training in the induction process. CC suggested that employees should get training on ICT systems before they are allowed to use them. TH advised that she would take up the question of employee training on ICT systems through another group.</p> <p>Para 6.14 Protection from Malicious Software - HE will issue a key message on the subject.</p> <p>CC also suggested that a Change Control Policy is needed but this would probably be referred to a different group and not be dealt with by this Group.</p> <p>JSM suggested that this Policy was not ready to be signed off yet by this Group.</p> <p><b>Action:</b> TH will look into ICT training being included in induction training and report back to the next meeting.</p> <p>HE will issue a key message on the issue of malicious software.</p> <p>Simultaneously, CC will send this Policy in the agreed format together with the appropriate summary to the Union for consultation with them on the 2 November 2010.</p>	<p><b>RB</b></p> <p><b>TH</b></p> <p><b>HE</b></p> <p><b>CC</b></p>
7  7.1          7.2	<p><b>Set 4 (2<sup>nd</sup> reading of revised Policies)</b></p> <p><b>Information Security Incident Reporting Policy</b></p> <p>CC explained that this Policy covers both technical and non technical issues rather than having two separate Policies.</p> <p>Discussion took place and suggested amendments included the following:</p> <ul style="list-style-type: none"> <li>• The FOI wording needs to be updated</li> <li>• Para 7 needs to be checked to ensure it is the standard wording. IE and CD will assist with this.</li> </ul> <p>Legal Services still need to comment on this Policy.</p> <p><b>Action:</b> CC will amend the Policy as suggested, receive further comments from IE and CD and present the revised Policy to the next meeting.</p> <p>Simultaneously, CC will send this Policy in the agreed format together with the appropriate summary to the Union for consultation with them on the 2 November 2010.</p> <p><b>Disclosure of Personal Data of Officers and Members Policy</b></p> <p>Legal Services and HR confirmed that they have commented on this Policy.</p> <p>Discussion took place and suggested amendments included the following:</p> <ul style="list-style-type: none"> <li>• In Annex A, is the word 'likely' understood?</li> </ul>	<p><b>CC/IE/CD</b></p> <p><b>CC</b></p>

ITEM		Action by
7.3	<ul style="list-style-type: none"> <li>• This Policy needs to be linked to the transparency issues (see item 20).</li> <li>• This Policy needs to be linked to the FOI Policy where it states who makes decisions on whether personal data will be disclosed.</li> <li>• Personal data can not be disclosed in certain circumstances such as covert workers.</li> <li>• Move Annex A into the body of the Policy and have an FAQ appendix eg. questions given in Annex B para 4.2.</li> <li>• Split this Policy into two, one relating to Members and one relating to Officers.</li> <li>• Refer to Members Policy to the Standards Committee or wherever Carole Dunn advises.</li> </ul> <p>JSM suggested that everyone provide examples to RB on this matter to assist in the understanding of application of this Policy.</p> <p><b>Action</b> RB will amend the Policy as suggested, receive further comments from ALL and present the revised Policy to the next meeting.</p> <p>Simultaneously, RB will send this Policy in the agreed format together with the appropriate summary to the Union for consultation with them on the 2 November 2010.</p> <p><b>Data Processing Policy</b></p> <p>It was suggested that this Policy is renamed as 'Data Processing by Contractors' Policy.</p> <p>The contract with the contractor should already include a clause relating to this matter and this should only need to be a backup.</p> <p>It was agreed that this Policy has been signed off by this Group.</p> <p><b>Action:</b> RB will send this Policy in the agreed format together with the appropriate summary to the Union for consultation with them on the 2 November 2010.</p>	<p><b>RB/ALL</b></p> <p><b>RB</b></p> <p><b>RB</b></p>
7.4	<p><b>Call Recording Policy</b></p> <p>It was suggested that this Policy is not necessary. Is it not possible to use the privacy statement already in use in the Customer Centre?</p> <p><b>Action:</b> RB will discuss the need for this Policy with Robin Mair and refer back to this Group at the next meeting</p>	<p><b>RB</b></p> <p><b>RB</b></p>
8	<p><b>Set 5 (for initial discussion)</b></p>	
8.1	<p><b>Security Labelling (Marking) Policy</b></p> <p>RB introduced this Policy and advised that it is necessary to have security marking on documentation. There are normally 5 categories, restricted, protect, unclassified, for publication and private. Private relates to material that is private to an individual not NYCC. RB drew the Group's attention to the definitions of these categories. He also advised that 'protect' is likely to be the category for a large proportion of documents.</p>	

ITEM		Action by
8.2	<p>The Government Connect system should be used for transferring information if a document falls into the 'restrict' category. 'Restrict' would also apply to documentation that needs to be kept under lock and key.</p> <p>This marking applies to home working (see item 5.5, scanning etc.)</p> <p>JSM suggested that the Group needs to read this Policy and agreement can then be reached on the labelling of documentation.</p> <p>HE suggested examples are provided of what documentation the different categories will apply to.</p> <p>Another issue that needs to be addressed is how documents that are restricted are kept under lock and key (before the cleaners go home).</p> <p>It was suggested that DIGCs link this issue with the information audits and discuss categories of documentation at this time.</p> <p>HE/CC/RB will discuss a key message on this matter.</p> <p><b>Action:</b> ALL to read this draft Policy to be able to comment before the next meeting.</p> <p>ALL to supply examples of documentation for different categories to RB at Information Audit discussions.</p> <p><b>Information Enquiry Charges Policy</b></p> <p>JSM advised that this issue has become complicated and suggested that it is deferred to the next meeting.</p>	<p><b>ALL</b></p> <p><b>RB</b></p>
9	<p><b>Other Policies to be drafted?</b></p> <p>9.1 <b>Archiving Policy</b></p> <p>It was agreed that this Policy has been put to one side for the moment. However the world map should be updated by RB.</p> <p><b>Action:</b> RB to update world map and circulate.</p> <p>9.2 <b>Any Others</b></p> <p>None</p>	<p><b>RB</b></p>
<b>PART C ACTION PLAN</b>		
10	<p><b>Roll Out Plan</b></p> <p>10.1 <b>Update on Progress</b></p> <p>HF took the Group through the Plan and advised that amendments included the following:</p> <ul style="list-style-type: none"> <li>• Various target dates need to be changed</li> <li>• Reference to Management Board needs to be changed to CIGG 2</li> <li>• The Charter is now on display</li> </ul>	

ITEM		Action by
<p>10.2</p>	<p>HF advised that a pilot information audit will be carried out in FCS with SL and then further audits will be rolled out into other Directorates.</p> <p>See item 10 for other issues that could be mentioned.</p> <p><b>Action:</b> HF to amend Roll Out Plan as discussed and Group to note position.</p> <p><b>EIA for e Learning Package</b></p> <p>HF advised that the content of the e learning package is with L &amp; D (Will Bunn) for uploading onto the system.</p> <p>RB is still to do the EIA but this does not need to be included on the agenda in future.</p> <p><b>Action:</b> HF/CD will discuss progress and timescales on uploading the e learning package with Kelly Hanna.</p> <p>RB will carry out the EIA.</p>	<p><b>HF/ALL</b></p> <p><b>HF/CD</b></p> <p><b>RB</b></p>
<p>10.3</p>	<p><b>Identification of Information Asset Owners – progress</b></p> <p>In progress.</p>	
<p>10.4</p>	<p><b>Definition of an Information Asset</b></p> <p>Noted.</p>	
<p>10.5</p>	<p><b>Information Audit – progress</b></p> <p>In progress.</p>	
<p>10.6</p>	<p>TH advised that information is expected back from services by end of January 2011.</p> <p>DFoB advised that information is expected back from services by end of March 2011.</p> <p>HF advised on behalf of SD that an initial list for ACS has been provided.</p> <p>SL advised that the list for FCS is nearly complete.</p> <p>HE advised that there has been resistance within CEG to produce a list but she constructed a draft list which is now under consideration.</p>	
<p>10.6</p>	<p><b>Cyclical Review of Policies</b></p> <p>FS is working on this.</p>	
<p>11</p>	<p><b>Information Management Intranet Site – update on position</b></p> <p><b>HE will advise JSM on when the site needs updating as this is linked in with the Communication Plan.</b></p>	<p><b>HE</b></p>
<p>12</p>	<p><b>Sharepoint – update</b></p> <p>FS advised that she has received some training on the development and use of Sharepoint.</p> <p>A discussion took place around the directory of folders that are needed. It was agreed to keep this simple and FS will send a link to Group members as soon as possible.</p>	<p><b>FS</b></p>

ITEM		Action by
<b>PART D</b>	<b>OTHER MATTERS</b>	
13	<p><b>Information Governance Implications for Joint Partnership Working/Big Society - update</b></p> <p>Nothing to report at present.</p>	
14	<p><b>Strategic Transformation and Integration Capability (STIC) – linked to 5.1 and 6.1</b></p> <p>Nothing to report at present.</p>	
15	<p><b>Violent Warning Marker System - update</b></p> <p>DP provided a précis of the Data Protection Good Practice Note that has been issued by the Information Commissioner's Office in 2006 on the use of violent warning markers. He advised that NYCC do not have a consistent way of capturing information and there is no consistent procedure across Directorates.</p> <p>HO advised that ACS and CYPS are probably the two Directorates that need to address this issue. He advised that information is held on a case management system in ACS and there has been some analysis of alerts since April.</p> <p>DFoB advised that he needs to find out what systems there are within CYPS.</p> <p>JSM queried why the system used in York cannot be used in NYCC. DP advised that NYCC ICT cannot support the system used in York.</p> <p>It was agreed that if details of people are put onto the database those people will need to be told this in order to be compliant with the Guidance.</p> <p><b>Action:</b> DP, DfOB, SD and Robin Mair will look into how existing VWMSs work and come to a conclusion on how data can be shared and what database can be used. DP will bring a report on this matter to the next meeting.</p>	<p><b>DP/DfOB/ SD/Robin Mair</b></p>
16	<p><b>Information Security</b></p> <p><b>16.1 Update</b></p> <p>CC advised that generic accounts are being deleted amongst other issues that are being addressed.</p> <p><b>16.2 Latest Breaches – internal and external</b></p> <p>Noted.</p>	
17	<p><b>Records Management</b></p> <p><b>17.1 Database of Users of Records Management Service – how to keep up to date</b></p> <p>IK advised that he is waiting for updates from DIGCs.</p> <p><b>Action:</b> DIGCs to update IK.</p>	<p><b>DIGCs</b></p>

ITEM		Action by
<p><b>18</b></p> <p><b>18.1</b></p> <p><b>18.2</b></p> <p><b>18.3</b></p>	<p><b>DPA/FOIA Issues</b></p> <p><b>Publication of FOI requests on the NYCC website</b></p> <p>JSM referred the Group to the copy e mail dated 16 September 2010 from Information Governance and the briefing note on the Summary of the FOI process that were circulated with the Agenda. He advised that co-ordination of FOI requests is required and that there is now a system in place.</p> <p><b>Officer Contact Arrangements</b></p> <p>JSM requested DIGCs keep the hierarchy of officer contacts for FOI requests up to date.</p> <p><b>Summary of FOI process</b></p> <p>The briefing note has been drafted as a result of the deteriorating responses from Directorates to FOI requests.</p> <p>JSM requested comments from DIGCs on the draft Briefing Note.</p> <p>TH advised that she will pick this matter up with FOI co-ordinators.</p> <p>It was advised that in the meantime, judgement on FOI responses is ongoing in Veritau and the Communications Unit.</p> <p><b>Action:</b> DIGCs to comment on the Briefing Note and feedback to HF/RB.</p>	<p></p> <p><b>DIGCs</b></p> <p><b>DIGCs → HF/RB</b></p>
<p><b>19</b></p> <p><b>19.1</b></p>	<p><b>Internal Audit Reports</b></p> <p><b>Current Audit Reports that refer to Information Governance</b></p> <p>➤ Final PwC Report on Information Governance</p> <p>HF advised that the final audit report is for information and the difference to the report presented to the last meeting is that the management response has been inserted into the report. There were only a couple of minor issues and overall the audit was reported as good with 'moderate assurance'.</p>	<p></p>
<p><b>20</b></p> <p><b>20.1</b></p>	<p><b>Coalition Government Latest Proposals</b></p> <p><b>Publishing itemised local authority expenditure update</b></p> <p>SL reminded the Group that this relates to transparency of data for payments over £500. Three key areas have been used: personal details, invoice payments and contract details.</p> <p>SL advised that the deadline to produce this information is January 2011 and that it has been difficult to put together for various reasons including the following:</p> <ul style="list-style-type: none"> <li>• Coding blocks need to detail 'proper' information so that invoices can be categorised.</li> <li>• There is a need to identify if payments are made to private individuals such as foster carers in the ledger so that an item can be labelled 'redacted'</li> </ul>	<p></p>

ITEM		Action by
20.2	<ul style="list-style-type: none"> <li>• SCMS only includes contracts over £20,000 and so the detail required for payments over £500 is not there.</li> <li>• No code of practice has yet been issued on procurement.</li> </ul> <p>A discussion took place around the need to publish salary data for senior officers and possibly job descriptions providing the scope of their responsibilities. This is over and above these details being published in the Statement of Accounts.</p> <p>Further links will be made with other statistics over time.</p> <p>SL advised that information is still in the process of being fine tuned and categorised. It will then be made available to FCS Directorate management team and can be made available to DIGCs.</p> <p><b>Anything new?</b></p> <p>Deferred to next meeting.</p>	
21	<p><b>Items for Subsequent Meetings</b></p> <p>21.1      ➤ Disaster Recovery - deferred</p> <p>                 Noted.</p> <p>21.2      ➤ Use of Government Connect</p> <p>                 Noted.</p>	
22	<p><b>Matters Arising from Meeting 4 not mentioned elsewhere on agenda</b></p> <p>None</p>	
23	<p><b>Any Other Business</b></p> <p>None.</p>	





## Press release

24 November 2010

### **First monetary penalties served for serious data protection breaches**

The Information Commissioner today served two organisations with the first monetary penalties for serious breaches of the Data Protection Act.

The [first penalty](#), of £100,000, was issued to Hertfordshire County Council for two serious incidents where council employees faxed highly sensitive personal information to the wrong recipients. The first case, involving child sexual abuse, was before the courts, and the second involved details of care proceedings.

The [second monetary penalty](#), of £60,000, was issued to employment services company A4e for the loss of an unencrypted laptop which contained personal information relating to 24,000 people who had used community legal advice centres in Hull and Leicester.

The Hertfordshire County Council breaches occurred in June 2010 when employees in the council's childcare litigation unit accidentally sent two faxes to the wrong recipients on two separate occasions. The council reported both breaches to the Information Commissioner's Office (ICO).

The first misdirected fax was meant for barristers' chambers and was sent to a member of the public. The council subsequently obtained a court injunction prohibiting any disclosure of the facts of the court case or circumstances of the data breach.

The second misdirected fax, sent 13 days later by another member of the council's childcare litigation unit, contained information relating to the care proceedings of three children, the previous convictions of two individuals, domestic violence records and care professionals' opinions. The fax was mistakenly sent to barristers' chambers unconnected with the case. The intended recipient was Watford County Court.

The Commissioner ruled that a monetary penalty of £100,000 was appropriate, given that the Council's procedures failed to stop two serious breaches taking place where access to the data could have caused substantial damage and distress. After the first breach occurred, the council did not take sufficient steps to reduce the likelihood of another breach occurring.

The A4e data breach also occurred in June 2010 following the company issuing an unencrypted laptop to an employee for the purposes of working at home. The laptop contained sensitive personal information when it was stolen from the employee's house.

The laptop contained personal information relating to 24,000 people who had used community legal advice centres in Hull and Leicester. An unsuccessful attempt to access the data was made shortly after the laptop was stolen. Personal details recorded on the system included full names, dates of birth, postcodes, employment status, income level, information about alleged criminal activity and whether an individual had been a victim of violence.

A4e reported the incident to the ICO. The company subsequently notified the people whose data could have been accessed.

The Commissioner ruled that a monetary penalty of £60,000 was appropriate, given that access to the data could have caused substantial

distress. A4e also did not take reasonable steps to avoid the loss of the data when it issued the employee with an unencrypted laptop, despite knowing the amount and type of data that would be processed on it.

Information Commissioner, Christopher Graham, said:

“It is difficult to imagine information more sensitive than that relating to a child sex abuse case. I am concerned at this breach – not least because the local authority allowed it to happen twice within two weeks. The laptop theft, while less shocking, also warranted nothing less than a monetary penalty as thousands of people’s privacy was potentially compromised by the company’s failure to take the simple step of encrypting the data”.

“These first monetary penalties send a strong message to all organisations handling personal information. Get it wrong and you do substantial harm to individuals and the reputation of your business. You could also be fined up to half a million pounds.”

## **ENDS**

If you need more information, please contact the ICO press office on 0303 123 9070 or visit the website at: [www.ico.gov.uk](http://www.ico.gov.uk)

### **Notes to Editors**

1. The monetary penalty for Hertfordshire County Council is available on the ICO website here:  
[http://www.ico.gov.uk/~media/documents/library/Data\\_Protection/Notices/hertfordshire\\_cc\\_monetary\\_penalty\\_notice.ashx](http://www.ico.gov.uk/~media/documents/library/Data_Protection/Notices/hertfordshire_cc_monetary_penalty_notice.ashx)
2. The monetary penalty for A4e is available on the ICO website here:  
[http://www.ico.gov.uk/~media/documents/library/Data\\_Protection/Notices/a4e\\_monetary\\_penalty\\_notice.ashx](http://www.ico.gov.uk/~media/documents/library/Data_Protection/Notices/a4e_monetary_penalty_notice.ashx)
3. Monetary penalties are listed on the ICO website here:  
[http://www.ico.gov.uk/what\\_we\\_cover/promoting\\_data\\_privacy/taking\\_action.aspx](http://www.ico.gov.uk/what_we_cover/promoting_data_privacy/taking_action.aspx)
4. The Information Commissioner’s Office upholds information rights in the public

interest, promoting openness by public bodies and data privacy for individuals.

5. The ICO has specific responsibilities set out in the Data Protection Act 1998, the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Privacy and Electronic Communications Regulations 2003.
6. For more information about the Information Commissioner's Office subscribe to our e-newsletter at [www.ico.gov.uk](http://www.ico.gov.uk). Alternatively, you can find us on Twitter at [www.twitter.com/ICOnews](https://www.twitter.com/ICOnews).
7. Anyone who processes personal information must comply with eight principles, which make sure that personal information is:
  - Fairly and lawfully processed
  - Processed for limited purposes
  - Adequate, relevant and not excessive
  - Accurate and up to date
  - Not kept for longer than is necessary
  - Processed in line with your rights
  - Secure
  - Not transferred to other countries without adequate protection
8. The Data Protection Act (1998) does not cover the acts of interception of communications or 'hacking' of personal information. The interception of communications falls under the Regulation of Investigatory Powers Act (2000) which is regulated by the Interception of Communications Commissioner.
9. The ICO has legal powers to ensure that organisations comply with the requirements of the Data Protection Act. In using its regulatory powers, the ICO considers the nature and severity of the breach which has occurred. Dependent on circumstances, the powers the ICO has at its disposal include:
  - serving information notices requiring organisations to provide the ICO with specified information within a certain time period;
  - serving enforcement notices requiring organisations to take specified steps in order to ensure they comply with the law;
  - issuing monetary penalties of up to £500,000 for serious breaches of the Data Protection Act;
  - conducting audits to assess whether organisations are processing personal data in accordance with good practice;
  - reporting to Parliament on data protection issues of concern;
  - prosecuting those who commit criminal offences under the Act. The ICO prosecutes individuals and organisations for specific breaches of the Act such as the illegal trading of personal data and non-notification.