Policy & Standards Council meeting 14 July 2009
Decisions to be taken

1. **Information Security and Communication decisions to be taken:**

   a) Standards on Data Protection:

      i) You are asked whether you wish to approve the following standard on data protection.

      Outcome: It was agreed that ISIS would make the following amendments to the document:

      - Add the definition of “sensitive” to the document, rather than in a separate link.
      - Under the first principle, include the need to obtain written consent
      - Under the eighth principle, change “may not comply” to “would not comply” in last sentence.
      - Add a link to the Government guidance on sharing information under “further information”

      It was also agreed that ## would arrange for someone from legal to review the document.

   b) Summary of Freedom of Information Principles Guidance for councillors (Elected Members)

      i) You are asked whether you wish to approve the following summary of freedom of information principles which is to be issued to all elected members.

      Outcome: It was agreed that ISIS would make the following amendments to the document:

      - The disciplinary statement at the end of the document would be altered to read; “If you fail to follow our policy on information security and communication or other supporting standards or procedures, action may be taken against you”.
      - A link would be added to the ICO guidance on Data Protection for elected members.

      It was also agreed that ## would arrange for someone from legal to review the document.

      Redacted under section 31 & 36

2) **Data Protection internal review**

   a) Update on review

Outcome: It was agreed that ISIS would find out the name of the project manager to be assigned to the working group who will be responsible for ensuring the actions from the audit are complete. ISIS will also send Margaret a list of the suggested names for the working group so that she can arrange for the first meeting to be set up. As soon as the DP review document has been signed off, it will be sent to all P&SC members.

3) AOB

a) Update on correspondence received from ICO.

Outcome: It was agreed that ISIS would send a copy of the ICO Audit terms of reference would be sent to all P&SC members.

enquired about the final outcome of the flu pandemic procedures document discussed at the last meeting. ## confirmed that changes had been agreed by P&SC members, and agreed to send a copy of the final document for information to all.

Policy & Standards Council meeting 18 August 2009 Decisions to be taken

2. Information Security and Communication decisions to be taken:

b) Our policy on information security and communications and our supporting standards:

i) You are asked whether you wish to approve the changing of all references from BT SMC to Essex Service Desk within our policy and standards documents, without each document coming through P&SC.

Outcome: This was approved.

4) Data Protection internal review

a) Update on review

b) Update on correspondence received from ICO – Adequacy Report.

5) AOB

a) Policy review update

Outcome: It was agreed that P&SC members would set aside time in their diary's to review the policy documents prior to the next P&SC meeting. ISIS will bring forward Septembers P&SC meeting in order to meet Data Protection review deadlines and will send policy documents a week before the meeting.

Outcomes from last meeting:

Policy & Standards Council meeting
16 September 2009
Outcomes

Note that these decisions were not presented in this paper to P&SC at their meeting, but the information was given to them.

3. Information Security and Communication decisions to be taken:

b) Policy review – outstanding actions from last meeting.

i) **Password protecting personal information sent by email within ECC**

Our standards for using email have been updated to reflect the changes requested at the last meeting

(1) P&SC were asked whether they agree that settings across the ECC estate should be changed to remove the functionality that suggests names while completing To: Cc: and Bcc: fields using email addresses used previously. This is to reduce the likelihood of sending confidential or highly confidential information outside ECC.

Outcome: **neither approved nor rejected**:

P&SC would like to know what other councils are doing, so asked that ISIS undertake some research and circulate the response by email, with voting buttons, so that a decision can be reached.

(2) P&SC were asked whether, if the agreed the point above, they would like to stipulate a trial period for this change.

Outcome: **not considered.**

ii) The provision of personal drives (also known as home directories), normally P:, O: or H: drive

Our standards for personal use of council facilities have been updated to reflect the changes requested at the last meeting.

P&SC were asked to decide whether to restrict the size of personal drives, or to eliminate them altogether, to reduce the implication that it is acceptable to store large amounts of non-business information on ECC's network.

Outcome: It was confirmed that there is no right or entitlement to have a personal drive. ISIS are to work with Internal Communications on a reminder that personal drives should not be used for storage of non-business information and that we intend to remove files that are clearly non-business after a defined interval (for example, 28 days)

c) Policy review – new policy documents

i) **Information governance framework:** the DPA review by Internal Audit recommended that ECC reviews, documents and agrees the governance structure a DPA governance framework which should clearly document ownership and accountability at all levels; includes key legal representation at a senior level, states the top level DP objectives of the organisation and describes our information governance structure including, where relevant, documented roles and responsibilities. P&SC were asked to approve the attached document to meet these recommendations.

Outcome: approved once the following amendments are made
Replace section 3.2.3 with words provided by Margaret Lee. The final version is attached below.

ii) **Information management strategy:** P&SC were asked to approve the attached Information Management Strategy.

Outcome: Not approved. P&SC were not clear about the purpose of this document, although they agreed that a clear information management strategy would be very useful.
Action: Mark Briggs to raise this at the DP steering group to understand exactly what risks are to be addressed with this document.

Post meeting note: An earlier version of this document was sent to the ICO who commented that it enabled the exchange of information with the general public and certain external agencies, such as the Health Community and the Police, where data sharing protocols are in place, but there is no timescale given for achieving the objectives.

Insert

Action: ISIS to arrange for next P&SC meeting to be dedicated to drawing out the points that need to be contained in ECC's information management strategy.

iii) **CCTV policy:** In their review of our documentation, the ICO commented that full CCTV subject access request (SAR) procedures are needed. They also made a number of details commented, including that there does not appear to be a full documented procedure of how these are processed to ensure consistency with the ICO's CCTV code of practice 2008 and that we do not state how the subject would be identified in the footage prior to the viewing. P&SC were asked to approve the attached CCTV policy to address this.

Outcome: approved once the following amendments are made
The final version will be circulated once the points have been addressed.

- Add statement at the beginning that this excludes covert cameras, which are managed under Regulation of Investigatory Powers (RIPA) and include in the text a hyperlink to that policy.
- Find out whether traffic cameras including (for example) those used in the traffic control centre, are covered by the same legislation, then add relevant statement under 'Scope'.
- Add ISIS email and phone contact details.

iv) Information Retention and Destruction Policy: the ICO commented that our documents included no related guidance on how files should be destroyed (for example, cross shredded) nor reference to responsibility for this and how the retention schedule is enforced. P&SC were asked to approve the attached revised Information Retention and Destruction policy to address this.

Outcome: approved once the following amendments are made

- Add links to retention schedule and other documents mentioned in the text;
- write guidance on how to destroy information securely (paper and electronic) and include link to that;
- give clarity on how to determine who is 'record owner' and add to glossary;
- Add statement that original documents (for example, passports, driving licences) must be returned to their owner as soon as reasonably practicable;

v) **Procedure for gaining exceptions:** this document widens the scope of the exceptions procedure, which was previously limited to areas such as local admin rights and Internet access. P&SC were asked to approve this version.

Outcome: make the following changes then circulate. The changes have been made and the final version is attached below the points.

- Change second paragraph to show that this applies to all policies, standards and procedures relating to the way information is handled within ECC. Remove the examples within the paragraph because they focus on technology.
- Ensure that all exceptions are time limited, and that a review date is recorded – add this detail to the document.
- Change point 3 in the procedure to remove reference to the Operational Security Manager and change "best" to "most appropriate".
- Remove points 5 and 6 from the procedure.

Updated version:

vi) **Standards for ECC Information Security Classification and Handling**

Outcome: make the following changes then circulate.

- Add a ‘disclosure’ section to each classification;
- Add reference to electronic info/web content to examples of published information;
- Put advice on removable media in one place because it is the same for all categories;
- Write ‘how to’ guide or similar for marking removable media, especially memory sticks/pen drives, and include example of what to put; add that guidance is available from ISIS and include link;
- Investigate whether we can give a Freepost address for return of removable media;
- Under disclosure section for published and restricted info, add statement that the principle of FOI is to publish as much as possible;
- Under ‘confidential’ examples, change ‘business tenders’ to be ‘business tenders during tendering process’;
- Under ‘confidential’ and ‘highly confidential’ protection measures, change ‘should’ to ‘must’ be sent be recorded delivery or secure courier unless encrypted electronic info.

d) Policy review – all policy documents

Outcome: P&SC asked that all policies, standards and procedures are presented more consistently, and specifically mentioned the following points:

- Wherever other documents are mentioned, include links to them.
- Layout including fonts, numbering, headers and footers;
- Metadata (the version control table at the end of each document).

6) Any other business

a) Call recording policy: a change of the technology used within ContactEssex means that our policy on call recording has been revisited. It is proposed to cease call recording but, before taking the decision, P&SC wished to check the impact on their services (for example, Trading Standards make use of this and want it to continue).

Action: Each P&SC member to check whether recording of calls to/through ContactEssex is used by their directorate.

Action: ## to send current policy to ## for a legal review and check whether it is published on the intranet.

b) Communication: P&SC recognised that effective communications with managers are essential to ensure that they know the policies because

they are responsible for ensuring their staff follow them; they also need understand what they are expected to do when policies are breached.

Action: ##/ISIS to work with Internal Comms on this.

c) Membership

i) There was concern that decisions were being taken which would impact the whole of ECC but one key service was not represented at the meetings.

Action: ## to talk to ## about SCF attendance at P&SC, recognising that previous arrangements for cover have been judged by Internal Audit to be insufficient, due to a requirement for separation of duties. ## to suggest that the SCF Customer Services and Communications Manager could deputise.

ii) Geoff Prudence is moving within ECC so Les Pilkington will be taking over his role on P&SC to represent FMS.

7) Attendance

a) The meeting was attended by:
Mark Briggs Head of Information Services
Geoff Prudence Head of Facilities Management
Craig Derry Caldicott Guardian for Adults, Health & Community Wellbeing
Jackie Roberts representing Change Director, ESH
Shirley Jarlett representing the County Solicitor
Keir Lynch Director for Human Resources & Customer Excellence
Cajetan Chukwulozie, Head of Internal Audit
##, Information Services (administration)

b) Apologies were received from:
Jayne Robinson, Assistant Director for Performance and Programmes, SCF
Margaret Lee, Chief Financial Officer

Policy & Standards Council meeting 21 October 2009 Decisions to be taken

4. Information Security and Communication decisions to be taken:

a) Mailbox limits: ECC are rapidly using email storage and it is predicted that we will run out of storage space within a couple of months. (This item was added to the agenda during the meeting).

i) You are asked to discuss whether ECC should implement limits on mailbox sizes.

Outcome: It was decided that a paper should be produced to P&SC detailing considered options and their implications. As part of that paper, it should investigate whether the cost purchasing additional storage space vs. the cost of employee time. ISIS to promote existing guidance on good housekeeping as part of ongoing comms campaign. **Action**: ISIS to confirm and report back on whether KVault is working as it should with VPN.

b) At the last P&SC meeting it was agreed that you would focus this session on determining which subject areas need to be covered by the Information Management Strategy. For information the current draft document is attached.

Some points you may wish to consider are:

- Section 46 code of practice says that "An authority should have in place an overall policy statement, endorsed by top management and made readily available to staff at all levels of the organisation, on how it manages its records, including electronic records."

- Freedom of Information requires us to be able to find and retrieve information and where necessary apply exemptions and public interest tests within 20 working days.

- Data Protection requires us to be able to find and retrieve all the information we hold about a specific person and where necessary seek third party agreement and apply exemptions within 40 calendar days.

- ISO27002 recommends that sensitive systems have a dedicated (isolated) computing environment.

- There have been various discussions over recent months about making better use of our email and email archiving capacity which have not yet resulted in actions being agreed.

Outcome: It was decided that further information was required in order to complete ECC's Information Management Strategy. It was agreed that the strategy would act as an overarching vision on what ECC wants to achieve

and how we will get there. There was discussion around aligning the strategy with the EssexWorks pledges particularly around the storing of information and moving towards a paperless environment. It was also felt that it should include information sharing protocols and improve how ECC manages the sharing of information. **Action**: ISIS to provide P&SC with Electronic Document and Records Management System (EDRMS) proposal which was put together in 2005. P&SC to review and decide if we should reinvestigate a corporate EDRM solution. **Action**: ISIS to provide P&SC with examples of what other organisation have in place as their Information Management Strategy.

Attendance

Tony Dawson, representing Head of Information Services
Craig Derry, Caldicott Guardian for Adults, Health & Community Wellbeing
Jayne Robinson, Caldicott Guardian for Schools, Children and Families
Margaret Lee, Section 151 Officer
Julie Ellis, Change Director, ESH
Philip Thomson, County Solicitor
Helen Burley, Information Services
##, Information Services (administration)

Policy & Standards Council meeting 8 December 2009
Decisions to be taken

5. Information Security and Communication decisions to be taken:

c) Our standards for acceptable use: Please see below the draft acceptable use standards (including personal use).

i) Our code of connections with the NHS and central government require us to have an acceptable use policy covering the use of our information and facilities, for both business and personal use. Currently we only have standards for personal use; this standard would replace the current standards for personal use as it has been incorporated into this proposed standard. You are asked to approve this standard.

Outcome: Following amendments to be made and then circulated for approval:

- Add wording “If you are not sure if you are authorised to disclose information, speak with your Information Champions or ISIS”;
- Add “and system” to statement relating to changing passwords every 30 days;
- Add “IT” to statement about reporting faults to Essex Service Desk;
- Move statement about removing personal use facilities to the end with compliance/consequence statement;
- Investigate risk and impact of removing “They must not contain real words” relating to password complexity;
- Check call retention in Contact Essex relating to statement about keeping call recordings for up to 6 months.

d) Application for GCSx accounts: The attached documents have been drafted based on guidance from our code of connection requirements and IT security.

i) You are asked to approve the application pack for new GCSx users (this includes an application form and commitment statement).

Outcome: It was agreed that the application form can be used in the interim to ensure those who require GSCx accounts as part of their role can continue their business. However, this is to go back to P&SC with the following information and amendments before it is signed off and published:

- ISIS to provide further information on what GCSx can be used for and the difference between GCSx and CJSM.
- ISIS to find out who our N3 users are and whether we have a secure email transfer with the NHS.
- Remove duplications of the work Applicant from the details section of the form and replace with one field called “Applicants details”.

ii) You are asked to approve IS to turn off auto-forwarding to external email accounts at mailbox level. This is Outlook functionality which

users can turn on themselves. (Requests where there is a genuine business need to auto-forward ECC mail to an external email account, this will continue to follow the exception procedure managed by ISIS and the auto-forward set up by IS at server level).

Outcome: This was approved. It was decided that comms are to go out to notify users before turning off this functionality.

e) BlackBerry passwords: Currently, BlackBerry's do not automatically require passwords to be enabled; it requires users set them up themselves. Windows Mobile devices are set up to automatically prompt for a 4 digit pin to be entered before access is granted, this is inline with security requirements of our code of connections and best practice.

   i) You are asked to approve IS to set the BlackBerry sever to enforce the requirement to have a password on all existing and new BlackBerry's from 31 January 2010. Information Champions have been provided with a list, for their service areas, of those BlackBerry users who have not set up passwords on their devices, they will be contacting them over the next couple of weeks to prompt and assist them. If approved, a further communications will be sent out to BlackBerry users who do not have passwords set up.

Outcome: This was approved.

f) Ministry of Justice (MOJ) consultation: The MOJ has issued a consultation paper around the introduction of new punishments, including custodial sentences, under section 55 of the Data Protection Act for the knowing or reckless misuse of personal information.

   (see page 15-16 for consultation questions)

   i) You are asked to comment and approve ECC's response to the consultation based on comments provided from Information Champions. (Please note that as this is a response to a central government consultation the Policy Unit are required to approve our response before it is sent – ISIS will arrange this).

      (Proposed r*esponse to the 4 questions will be provided within the meeting for discussion)*

Outcome: This was approved. Final version will be sent to P&SC members for their information and sent to Policy Unit for final sign off.

g) Review of outstanding actions from previous P&SC meetings:

Outcome: Target dates to be added to each action and reviewed at the next P&SC. Roll out for the Data Protection e-learning package to be sent to P&SC and include training on January agenda.

h) AOB:

   i) Update on correspondence received from ICO.

   ii) Outlook Web Access (OWA)

Outcome: OWA to be carried forward and discussed at next P&SC.

Attendance:

Alex Hallam, representing County Solicitor
Craig Derry, Caldicott Guardian for Adults, Health & Community Wellbeing
Jayne Robinson, Caldicott Guardian for Schools, Children and Families
Julie Ellis, Change Director, ESH
Margaret Lee, Section 151 Officer (comments provided virtually)

Policy & Standards Council meeting 15 January 2010
Decisions to be taken

6. Information Security and Communication decisions to be taken:

Redacted under Section 31 & 36

i) Freedom of Information documents: As part of our Information Governance statement of compliance to the Department of health, we need to demonstrate that we have 'publicly available, documented procedures for FOI Act compliance'. Failure to meet the requirements of the statement of compliance could result in ECC losing its N3 connection with the NHS.

(1) You are asked to approve the attached documents for publication on the ECC website.

Outcome: It was agreed that they can be published on ECC's website once the following changes have been made:

- *Process map*: amend wording from "Request logged and sent to relevant Information Champion" to "…and send to relevant Service Area"
- *Process map*: amend wording from "We will normally offer to transfer the request" to "We will offer to transfer the request where we can identify who holds the information"
- *Process map*: add the complaints section after each end point, regardless of whether the information is or is not held or provided.
- Written procedure: add address details to "From the website section"
- Written procedure: amend wording from "Received by ECC" to "How a request is handled by ECC?"

j) Internet filter update: the internet sites which P&SC agree to block are technically managed through our primary internet filter box. This filter box also manages any exceptions which have been granted to individuals.

i) You are asked to review the attached options paper and approve one for managing the internet filter in the unlikely event that the primary box fails.

Outcome: A combination of Options 1 & 2 was agreed. We will run our normal ECC filtering on the secondary box and then upload the exceptions. This will prevent users from accessing inappropriate sites and those with exceptions will be able their exceptions within 1 hour of the primary box failing.

k) Our standards for acceptable use: as agreed at the last P&SC, amendments to the wording have now been reflected in the attached and the further information requested has been provided below.

i) P&SC asked ISIS to investigate the risk and impact of removing "They must not contain real words" relating to password complexity and whether two words together added any additional complexity. ISIS can confirm two words together, does not add significant complexity (even though it may increase the number of characters in the password). Our current password standards follows the

industry Information Security best practice (ISO27002) and just meets the HMG Information Security and Assurance Policy and Guidance which are required to confirm with as ECC have signed up to GCSx. You are asked to approve the password requirements wording.

Outcome: This was approved. Current password requirements and wording will remain. ISIS to review guidance on “how to… choose a secure password” to ensure it is up to date and then raise awareness.

l) Outstanding Actions: Review of outstanding actions from previous meetings to track progress.

Outcome: Outstanding actions were reviewed.

- EIH training delivery: ISIS to identify how many people require EIH by comparing who has already attended against the number of people within ECC. ISIS to work with L&D and flag to DP steering group a need to identify resource to carry out the necessary training programme.
- Information retention and destruction policy (including service specific guidance): Confirm with ## they have been reviewed in line with comments from ICO and go back through the information governance.

m) Password protection: Current (and proposed) ECC policy and standards stipulate that password protection must be used for internal emails where confidential and highly confidential information is sent. P&SC requested information on what other local authorities do.

i) You are asked to review the attached and decide on what the password policy for internal documents should be. FYI - IS are also currently undertaking a piece of work to look at how we securely share information electronically.

Outcome: The group unanimously agreed to remove the policy requirement to password protect confidential and highly confidential documents when sending them internally. It was decided that individuals should make the judgement themselves as to whether or not this information should be protected when sharing it internally.

Policy & Standards Council meeting 19 February 2010
Decisions to be taken

7. Information Security and Communication decisions to be taken:

Redacted under Section 31 & 36

n) GCSx: ## (IS IT Security Manager) will be attending to provide a short overview on GCSx and what it means to ECC and the role of P&SC.

Outcome: This was removed from the agenda at the meeting.

o) Our standards for using information outside the office and looking after portable equipment:

ii) You are asked to approve the format change to bring this standard in line with our other standards. The change included removing subheading which read "*What security measures should I take when I use information outside the office?*" and adding the paragraphs numbers.

Outcome: This was approved.

iii) You are asked to approve the addition of points 4 and 10 following comments from I&ICTB.

Outcome: This was approved. However the group felt that point 3 (recorded delivery) was too strict on its classification and ISIS should reword the policy accordingly.

p) Procedure for unblocking ECC recommended internet sites for all ECC users: the current procedure requires support from their Manager and their Director; this then goes to P&SC for decision.

i) You are asked to approve amendments to the procedure to allow users to obtain support form their Information Champion instead of their Director. (Requester would still require their Mangers support and the decision would still be taken by P&SC).

Outcome: This was approved.

q) Our standards for using email:

i) You are asked to approve the format change to bring this standard in line with our other standards. The change included removing good practice guidance into a separate document.

Outcome: This was approved.

ii) You are asked to approve wording changes indicated by green text.

Outcome: This was approved.

r) Establishment controls policy: Please see page 4 of the attached for purpose and principles of this policy document.

ii) You are asked to review and approve the attached policy.

Outcome: This was approved.

s) Social Media policy: Communications have put together a policy on the use of social media sites (such as facebook).

i) You are asked to review and approve the attached policy.

Outcome: This was approved.

t) AOB:

i) Update on sites globally blocked by ECC

Policy & Standards Council meeting 15 April 2010
Update on information governance

8. Data Protection Steering Group:

u) Corporate FOI/SAR process review: a review is underway to analyse how ECC handles information requests and identify process improvements which will improve ECC compliance. Some of the key issue identified included insufficient resource in some areas; each service area having vastly different mechanisms to handle these requests; and the handling of cross-cutting requests (where input is required from multiple directorates). One recommendation put forward to the Data Protection Steering Group is to have one central team coordinating all information requests. Next actions: detailed implementation/improvement plan to be ready for sign off by end of June

v) Policy dissemination: ECC has a number of policies across the council which are currently held in various places on the intranet. The Data Protection Steering Group has recently reviewed a 2 pieces of software which could help ECC improve how manage our policies and disseminate them consistently.

w) Retention and Destruction pilot: To address breaches of Data Protection Principle 5: Keeping information only for as long as necessary, a pilot was undertaken to assess the feasibility of carrying out a project to review all records held beyond retention periods. Next Action: Review records retention schedule for each directorate; develop procedure for automatic destruction at the end of the retention period and options papers for dealing with existing records beyond review date.

9. Information Governance Toolkit (N3 connection):

a) IG toolkit: Each year ECC is required to submit a code of compliance in order to maintain our N3 connection with the NHS. Below is a daft briefing note for AH&CW Executive Board detailing the outcomes from the most recent (09/10) submission.

10. **Network folder security:**

a) Inheriting folder permissions: When setting up a new ECC account, it is possible to ‘model’ the account on an existing employees account. This means that the new user will receive the same access to networked folders (excluding personal drive) and also be added to the same distribution lists. There is risk that new users will have access to information which they are not authorised to view. AH&CW have produced the following paper further highlighting the issue. Next

Actions: ISIS to liaise with IS and produce an option paper which will be taken through the governance (I&ICTB and P&SC).

11. AOB

Policy & Standards Council meeting 17 May 2010
Update on information governance

12. Data Protection Steering Group:

x) Corporate FOI/SAR compliance: following the ICO audit a review was undertaken to analyse how ECC handles information requests and identify compliance improvements.

(1) You are asked to review the options paper and approve which option to progress.

Outcome: This paper was removed from the decision paper before the meeting. However, the group feedback the following comments:

- Update timetable with timescales;
- Check response time statistics for FOI requests;
- Establish resource options;

y) Policy dissemination: ECC has a number of policies across the council which are currently held in various places on the intranet. A single sourcing agreement has been considered for purchasing MetaCompliance to improve how we manage our policies and their dissemination.

(1) You are asked to approve the concept of the council acquiring and utilising a policy management tool.

(2) If yes, you are asked to approve MetaCompliance as the policy management tool. (If approved this will then be taken to CLT for approval).

Outcome: this was not approved. Questions below to be addressed and taken back to P&SC:

- Has ## been consulted?
- How will this impact on RoboHelp?
- What is Essex Online Partnership (EOLP) usage plan?
- Has a business case been completed?

z) Our standards on using email: Additional information has been added following an action from an Information Appeals Panel to ensure employees understand that information within emails are subject to disclosure under Data Protection and Freedom of Information Acts.

(1) You are asked to review the standards and approve the additional text highlighted in green.

Outcome: this was approved.

aa) Email good practice guidance: Additional information has been added following an action from an Information Appeals Panel relating to how employees address clients in correspondence and maintaining an appropriate distance with clients in order to ensure objectivity.

(1) You are asked to review the guidance and approve the additional text highlighted in green.

Outcome: this was approved.

8) GCSx delegates: Due to the strict 'need to know' requirements of GCSx and the small volume of users, many GCSx users are not able to identify two suitable email delegates, as required by our policy. Any delegates on a GCSx accounts must also be GCSx users.

   i) You are asked to approve GCSx users to only require a minimum of one delegate on their GCSx email account.

   Outcome: this was approved.

9) Encryption: An issue with Satellite Navigation (Sat Nav) systems has been identified when users attempt to download updated maps to the Sat Nav. Our encryption software attempts to encrypt the device which results in it wiping all the content and making the device unusable.

   i) You are asked to approve the creation of a Sat Nav exception group on our encryption management tool. Users will still be required to go through the exception to encryption process.

   Outcome: this was approved. However, further investigation should be carried out to determine who is using Sat Navs and ensure they are ECC owned.

13. AOB

a. Inheriting folder permissions

b. ISIS Transition

Policy & Standards Council meeting 23 June 2010
Decisions to be taken

14. Information security and communication policy:

b) Laptop security: in order to improve awareness around the importance of keeping our equipment secure and compliance with our policy, the following ongoing task is being proposed.

(1) You are asked to review the proposal and approve FM to carry out this exercise.

Outcomes: This was not approved. However, the group suggested the following feedback:

- Investigate if Kensington locks can be part of the standard laptop bundle for all new laptops;
- Discuss with EPF other options to conduct laptop security reviews including other ECC premises outside of County Hall, and produce options paper to P&SC;

15. Subject Access Requests:

a) Proof of Identity: When processing subject access requests, ECC is entitled to request information to satisfy themselves (ECC) as to the identity of the requester.

i) You are asked to approve ECC to accept photocopies of documentation. Enquires were made to find out whether other local authorities accept photocopies and many do, also Information Champions are happy to accept photocopies.

Outcomes: This was approved on the basis that we reserve the right to request originals at our discretion.

b) Subject Access Request form: Revisions have been made to update the ECC subject access request form to help target the information requesters are looking for.

i) You are asked to approve the form for publication on the ECC website.

Outcomes: This was not approved. ## to clarify what level of identification should be requested when making subject access requests on behalf of other individuals, this will then be brought back to P&SC. Also the following fields should be added

- Space for requesters to specify what information they are requesting;
- Date range for search field;
- Optional field for contact number

16. Information Commissioners Office (ICO) visit:

a) ICO visit: An update will be provided on the plans for the ICO follow up visit.

17. AOB

a. Publication scheme

b. Policy dissemination (MetaCompliance)

c. Inheriting folder permissions

d. ISIS Transition

Policy & Standards Council meeting 19 August 2010
Decisions to be taken

1) **Information Security and Communication decisions to be taken:**

   a) Policy review. Following the start of this yeas policy review, you are asked to agree the changes to our policy on information security and communications and our supporting standards which have previously been agreed by I&ICTB. Changes to current wording has been tracked within each document:

      i) **Our Policy on Information Security and Communication:**

   Outcomes: This was approved.

      ii) **Our standards on Data Protection:**

   Outcomes: This was approved.

      iii) **Our standards for making sure our buildings are physically secure**

   Outcomes: This was approved.

2) **Other Policy and Standards Council Decisions:**

   a) Anti Money Laundering Policy. Although this is not an information policy it was felt that there was no other appropriate forum with the necessary representatives for this corporate policy to be approved. Therefore you are asked to review and approve this policy.

   Outcomes: Before this is published, the group requested the following:

   - Philip to confirm with ## why the trigger is set to £10,000 (this was subsequently confirmed as the recommended amount form the regulations).
   - On page 4 the first time 'MLRO' is used, include the full description with MLRO in brackets after.
   - Include the standard policy compliance statement (as used on the information policy and standards) at the end of the policy.

3) **AOB**

   a. Publication scheme

   b. Access Control

   c. Subject Access Request guidance

Attendees:
(on behalf of Julie Ellis)
Jayne Robinson

John Varney
(on behalf of Keir Lynch)
Philip Thomson
Steven Tredinnick

Policy & Standards Council meeting 1 October 2010 (September meeting)

Decisions to be taken

18. Information Security and Communication decisions to be taken:

Redacted under Section 31 & 36.

c) MetaComplaince: ECC has a number of policies across the council which are currently held in various places on the intranet. ECC has been considering purchasing MetaCompliance to improve how we manage our policies and their dissemination (further information to be provided in the meeting).

i) You are asked to approve the concept of the council acquiring and utilising a policy management tool.

ii) If yes, you are asked to approve MetaCompliance as the policy management tool.

Outcome: to be part of New Ways of Working to decide if this should be carried forward.

d) Data protection in employment: This policy sets out the Council's responsibilities as an employer under the Data Protection Act (DPA) 1998 and provides guidance on the maintenance of and access to employment records, in accordance with the provisions of this Act. This has been updated to reflect views from the data protection audit.

i) You are asked to approve the attached policy.

Outcome: this was approved.

e) Standards for using information outside the office and looking after portable equipment:

i) You are asked to approve the tracked wording changes in relation to posting 'confidential' and 'highly confidential' information.

Outcome: this was approved.

f) Remove standards for managing information:

iii) You are asked to approve the removal of these standards as most of the points are within other standards.

Outcome: this was approved.

g) Standards on acceptable use:

ii) You are asked to approve the addition of two points (highlighted in our standards for managing information 1)e).

Outcome: this was approved.

2) Other Policy and Standards Council Decisions:

a) Establishment Control policy:

i) You are asked to approve the tracked changes to the attached policy.

Outcome: this was approved.

3) AOB:

i) Information Assurance briefing for CLT.

Outcomes from last meeting:

Policy & Standards Council meeting 26 January 2011
Decisions to be taken

19. Information Security and Communication decisions to be taken:

h) Redacted under Section 31 & 36

i) Password reset: IS are implementing a tool which will enable users to reset their own passwords from their ECC machine without needing to call the service desk.

i) You are asked to approve the attached set up for the password reset tool.

Outcome: This was approved.

j) Nightwatchman: This software switches off the desktop computers at night in order to save on costs and energy.

i) You are asked to approve the attached set up for Nightwatchman.

Outcome: This was approved.

k) BlackBerry email storage: Following losses of BlackBerry's it was suggested we limit the volume of information stored on them. It was suggested that a limit should be enforced and therefore all emails would be deleted within a period of time.

i) You are asked to approve a limit of 15 days to be set, any emails older than 15 days will be deleted from the BlackBerry, but still available through Outlook.

Outcome: This was approved, communications to go out to BlackBerry users to inform them of this change.

l) Digital voice recorders: There have been several requests for the use of Digital Voice Recorders but the current encryption software blocks their use.

i) You are asked to consider whether unencrypted voice recorders should be allowed by exception.

Outcome: the group decided that access should be granted by exception, where there is a business need for their use. ISIS to make the decision on whether an exception should be granted.

Information Champion Comments: Some areas felt that the risk was too great to allow unencrypted voice recorders to be used where personal, and particularly sensitive, information was involved; the recent ICO fines where a particular concern. However it was flagged that legal currently use voice recorders and to disallow them would negatively affect their business.

m) ICO Complaints Procedure: This procedure determines how complaints received from the ICO are handled.

i) You are asked to approve the procedure.

Outcome: This was approved with the following amendments; remove 'members of Policy and Standards Council' and 'Cabinet Member for central services' and add 'Monitoring Officer' on the notification list. It was decided that the group will receive monthly reports which will include ICO complaint information and the Monitoring Officer will make the judgement on whether to refer an ICO complaints to Cabinet Member/s on a case by case basis.

n) Unblocking websites for all ECC employees:

i) You are asked to approve unblocking www.videoarts.com for all ECC so that Libraries can access training packages. This is currently blocked under "streaming media".

Outcome: This was approved on the basis that there is sufficient bandwidth available to cope with the demand. If there is not sufficient bandwidth, this should be unblocked for individuals requiring immediate access and rolled out further once bandwidth capacity is no longer believed to be an issue.

ii) You are asked to approve unblocking of www.vimeo.com for all ECC. This is currently blocked under "R rated" which is defined as "*services pertaining to anything that involves 18 and over material such as lingerie and swimsuits, revealing pictures. Sites that are adult in nature without being explicitly pornographic. Sample sites: www.lingerie.com, www.maximonline.com, www.bikini.com*".

Outcome: This was approved to be unblocked on an individual by individual basis.

10) AOB:

i) Information Assurance update (##)
ii) ISMF (##)
iii) Information Assurance reporting

Attendees:
Jean Imray
Leslie Pilkington
(on behalf of Keir Lynch)
(on behalf of Julie Ellis)
Philip Thomson
(on behalf of John Varney)