POLICY AND RESOURCES

CABINET BOARD

27TH MARCH 2014

FINANCE AND CORPORATE SERVICES

JOINT REPORT OF THE HEAD OF LEGAL SERVICES – D.MICHAEL AND THE HEAD OF ICT – S.JOHN

INDEX OF REPORT ITEM

Part 1 - Doc. Code: PRB-270314-REP-FS-DM-J

SECTION A - MATTER FOR DECISION			
Report Item		**Page Nos.**	**Wards affected**
1.	Information Commissioner's Office Audit of Neath Port Talbot County Borough Council	2-29	All

ITEM 1
PART 1 SECTION A

INFORMATION COMMISSIONER'S OFFICE AUDIT OF NEATH PORT TALBOT COUNTY BOROUGH COUNCIL

1. Purpose of Report

1.1. To advise Members of an Audit undertaken by the Information Commissioner's Office and to obtain decisions in relation to some of the recommendations of that Audit.

2. Background

Glossary

2.1. Data protection is very much its own world and it generates specific terms and acronyms which will mean nothing to the general reader. We therefore set out below some define terms and acronyms used in the audit and in this report. Some terms which Members will already be familiar with which refer to internal Council bodies, are also included for ease of reference.

CDG	-	Corporate Directors Group. Consisting of the Chief Executive and Directors
CGG	-	Corporate Governance Group - Officer group consisting of Heads of Democratic Services, Finance and Legal Services together with other officers dealing with Corporate Governance matters.
CMG	-	Corporate Management Group. The extended management team including the Chief Executive, Directors and Heads of Service.
CRIMS	-	Corporate Risk Information Management System – an in-house developed software system recording corporate risks.
DPO	-	Data Protection Officer. The Head of Legal Services
EIR	-	Environmental Information Regulations
IAO	-	Information Asset Owner
ICO	-	Information Commissioner's Office
ISA	-	Information Sharing Agreements
ISG	-	Information Security Group
RMSC	-	The Records Management and Security Consultant- an in-house officer dealing with information security matters.
SIRO	-	Senior Information Risk Owner – the Head of ICT and Procurement.

2.2. The ICO have been conducting voluntary audits of data protection procedures in various organisations. The Council took up the offer of a voluntary audit in order to identify any areas where improvement was appropriate.

2.3. In some Local Authorities specific staffed units have been set up to deal with data protection issues often in combination with freedom of information and environmental information regulations. The approach here has been to regard these issues as part of the day job of management; this has limited the cost of providing these functions but can leave the Council vulnerable to criticism that these issues are not dealt with by the Council with the formality found elsewhere.

2.4. An extract from the report including the summary of audit findings and the detailed findings and action plan are reproduced in the Appendix to this report. The full report can be emailed to Members who wish to receive it and the Executive Summary will be available on the ICO website.

2.5. The overall findings of the Audit are ones of "limited assurance". Of the various grades of outcome this is the third out of four. In reporting this to Members we would mention the fact that we specifically asked the ICO to look at areas where we were conscious that improvement was necessary; rather than to look at areas where we were confident that we were performing well (e.g. Data Security).

Organisational Responsibilities

2.6. It was predictable that the ICO wished to see certain functions in relation to data protection more formally assigned to various persons and bodies inside the Council. This clarification is helpful and your officers consider that it can be accommodated within existing organisational structures without the need to create parallel duplicating structures.

2.7. This part of the report addresses recommendations (a) 2 to (a) 10. It is suggested that the Director of Finance and Corporate Services report to CDG annually on data protection matters and a similar report should be put before Policy and Resources Overview and Scrutiny Committee. This report should cover compliance with the ICO audit, any risks associated with data protection, compliance with the Council's data protection duties and, specifically, compliance with the duty to allow data subject access. The report may also cover ISA's with other bodies. The Director may also report on other specific data protection matters should circumstances determine that a report is necessary.

2.8. The CGG should have data protection, FOI and EIR added to its terms of reference. These matters should appear on the agenda for each meeting of the group and it should report up to CGG as necessary. The Head of Finance has accepted responsibility for risk and for the CRIMS and he shall ensure that new data protections risks are brought to the attention of CGG. The Head of Legal Services as DPO will also report to CGG any matters of concern which have been brought to his attention. The Corporate Solicitor will notify CGG of any ISA's executed and shall keep a register of these.

2.9. The current Information Security Group shall be reconstituted. It shall consist of the SIRO, the RMSC and representatives of the Internal Audit, Finance and Legal Services Sections.

Legal Services use standard documentation when drafting contracts

2.10. Specific clauses are added to industry appropriate documentation to cover specific issues. The bespoke clauses cover data protection and, indeed, FOI/EIR. All contracts that go through proper formal procedures processed by the Procurement Section and Legal Services have these clauses inserted automatically. The challenge is to ensure that all contracts go through this route. This will cover recommendation (a) 16. Recommendations (d) 2 to (d) 25 all deal with Information Sharing Agreements ("ISAs"). These agreements arise in two sets of circumstances; firstly, where the Council has a contract for the provision of services and the normal data protection clauses in the contract are not sufficient to cover the volume or nature of the information shared, and secondly, longer term general data sharing with other public sector bodies such as the Police or the Local Health Board. Legal Services should be consulted on all new ISAs.

2.11 These documents have generally been in differing formats over the years but greater standardisation is appropriate and there is justification for maintaining a register for arrangements put in place.

2.12. In Sections C of the Audit the ICO indicate that they wish to see greater formality and centralisation in the handling of subject access requests ("SARs"). Fortunately, many of these requests can also be categorised as FOI requests. There is already a procedure in hand for handling FOI requests and it is probable that SARs can be added to this procedure without too much work at the start. Of course work is then created in the centralised recording of dealings with SARs requests.

2.13. Section B of the Audit relates to training and awareness. In many ways this will be the most difficult area to deal with since it is difficult to identify additional resources for training at this time. It may be that the most efficient way of dealing with this will be to explore with HR whether the provision of electronic training packages to all staff handling personal data would be suitable to answer this need. This issue will be discussed by Head of Legal Services, Head of ICT and Procurement and the Head of HR.

3. Recommendations

3.1. That the recommendations in the ICO Audit be accepted together with the agreed actions.

3.2. That data protection matters be reported to CDG at least annually, that data protection issues be added to the remit of the Corporate Governance Group and that an Information Security Group be established.

3.3. That no information sharing agreement be agreed without consultation with the Head of Legal Services.

3.4. That officers examine the options for improving training and awareness.

3.5. That officers report back to Members twelve months from now on the outcome of the Audit, any feedback from the ICO and the actions undertaken.

4. Reason for proposed decision

To comply with the recommendations in the Audit.

5. List of Background Papers

Data Protection Audit Report

6. Wards Affected

All

7. Officer Contact

Mr. David Michael – Head of Legal Services
E-mail d.michael@npt.gov.uk. Tel: 01639 763368

COMPLIANCE STATEMENT

INFORMATION COMMISSIONER'S OFFICE AUDIT OF NEATH PORT TALBOT COUNTY BOROUGH COUNCIL

(a) Sustainability Appraisal

Community Plan Impacts

Economic Prosperity	-	no impact
Education & Lifelong Learning	-	no impact
Better Health & Well Being	-	no impact
Environment & Transport	-	no impact
Crime & Disorder	-	no impact

(b) Other Impacts

Welsh Language	-	no impact
Sustainable Development	-	no impact
Equalities	-	no impact
Social Inclusion	-	no impact

(c) Consultation

There has been no requirement under the Constitution for external consultation on this item.

APPENDIX

3. Audit opinion

3.1 The purpose of the audit is to provide the Information Commissioner and NPTCBC with an independent assurance of the extent to which NPTCBC, within the scope of this agreed audit is complying with the DPA.

3.2 The recommendations made are primarily around enhancing existing processes to facilitate compliance with the DPA.

Overall Conclusion	
Limited assurance	There is a limited level of assurance that processes and procedures are in place and delivering data protection compliance. The audit has identified considerable scope for improvement in existing arrangements to reduce the risk of non-compliance with the DPA. We have made one very limited assurance assessment in respect of training and awareness and three limited assurance assessments in respect of data protection governance, requests for personal data and data sharing, where controls could be enhanced to address the issues which are summarised below and presented fully in the 'detailed findings and action plan' section 7 of this report.

4. Summary of audit findings

4.1 Areas of good practice

- Internal Audit consider notification, data classification, data retention, availability of data, password protection, identity access management and access to manual records when conducting their annual systems review.
- Privacy Impact Assessments, in respect of new data processing systems, have been introduced over the past year.
- The Corporate Solicitor is consulted prior to Head of Service authorisation and sign off in respect of subject access redactions and / or exemptions.
- Records about data sharing decisions are maintained as an audit trail for approved Information Sharing Agreements (ISAs). Records include minutes and action plans from the ISA working group.

4.2 Areas for improvement

- There is lack of corporate oversight of data protection compliance as groups such as the Corporate Directors Group (CDG) and the Corporate Governance Group (CGG) lack clearly defined roles in this area. In addition, there are no Key Performance Indicators (KPIs) in respect of data protection compliance.
- There is no requirement for documented data protection policies to follow an agreed format or version control process.
- There is no corporate data protection training programme for all employees processing personal data. This leads to an increased risk that personal data will not be processed in accordance with the DPA.
- The central database of requests for information records their due dates and is capable of producing reports against this information, however there is no reporting of Subject Access Requests (SAR) figures or compliance, and therefore no monitoring of performance.
- No monitoring or quality assurance checks are carried out to ensure that disclosures to third parties are appropriate.
- There is currently no formalised central NPTCBC policy or procedural guidance for employees to follow in order to set up a new ISA. This leads to an increased risk that employees will not be aware of data sharing requirements and may share data without appropriate safeguards or authority in place.
- NPTCBC do not hold a central register of ISAs, this results in a lack of oversight of such agreements and resulting risks, such as that ISAs may not be reviewed on time.

7.2 The agreed actions will be subject to follow up to establish whether they have been implemented.

7.3 Any queries regarding this report should be directed to Sanjay Patel, Engagement Lead Auditor, ICO Good Practice.

7.4 During our audit, all the employees that we interviewed were helpful and co-operative. This assisted the audit team in developing an understanding of working practices, policies and procedures. The following staff members were particularly helpful in organising the audit:

Records Management & Security Consultant, Ian John;
Head of ICT, Steve John;
Head of Legal, David Michael;
and Corporate Solicitor, Paul Watkins.

Appendix A

Detailed findings and action plan

Action plan and progress

Recommendation	Agreed action, date and owner	Progress at 3 months	Progress at 6 months
a2. The CDG should have a more formally defined role in respect of corporate oversight of data protection compliance.	Agreed. Implementation date: 28 March 2014. Responsibility: David Michael.		
a3. The Head of ICT should regularly report to the CDG in his role as SIRO or the role of SIRO should be reassigned to an alternative individual at Director level to improve corporate oversight of information risk.	Agreed. Implementation date: 31 March 2014. Responsibility: Steve John.		
a4. The remit of ISG should be expanded to incorporate data protection and	Agreed. Implementation date: 31		

information governance, instead of focusing solely on information security. The ISG should meet regularly to monitor and mandate improvements to data protection and information governance and have clear reporting lines to the Corporate Governance Group (CGG) to improve corporate oversight of the same.	March 2014. Responsibility: Steve John.		
a5. The CGG should have a formally defined role in respect of corporate oversight of data protection compliance.	To be considered at the next meeting of the CGG. Implementation date: March 2014. Responsibility: David Michael, Steve John and Karen Jones.		
a6. The remit of CGG should be expanded to incorporate risk management and the CGG should ensure that information risk is included in their	To be considered at the next meeting of the CGG. Implementation date: March 2014. Responsibility: David		

consideration of corporate risk. This responsibility should be formally documented.	Michael, Steve John and Karen Jones.		
a9. NPTCBC should develop a data protection or information governance steering sub-group (for example, an ISG sub-group) or forum, with reporting lines to the ISG, to allow operational staff to raise data protection issues.	Issues will be raised with the Corporate Solicitor who will inform the ISG. Implementation date: 28 March 2014. Responsibility: David Michael.		
a10. All information risks should be reported, recorded and appropriately managed via the CRMIS.	To be considered at the next meeting of the CGG. Implementation date: March 2014. Responsibility: David Michael, Steve John and Karen Jones.		
a13. The development of the Information Asset Register and identification, appointment and training of IAOs should be undertaken and	Agreed. Implementation date: December 2014. Responsibility: Steve John.		

completed, to ensure that information assets are managed appropriately, risk assessed periodically and that the outcomes of such assessments are reported to the SIRO. Additionally, NPTCBC should consider including IAOs in the ISG and/or within the membership of the steering group referred to in a9.			
a14. NPTCBC should implement measures to raise awareness of the incident reporting process.	Agreed. Implementation date: February 2014. Responsibility: Ian John.		
a15. Analysis of the incident log should feed into the CRMIS to improve risk management.	Agreed. Implementation date: 1 July 2014. Responsibility: Steve John.		
a16. NPTCBC should ensure that agreements and / or contracts with data processors include data protection clauses and monitor that these	Agreed that Legal staff shall ensure that contracts include appropriate data protection provisions. Those managing contracts shall ensure that these provisions		

data processors are complying with these clauses and their obligations under the DPA.	are complied with. Implementation date: 28 March 2014. Responsibility: David Michael.		
a19. NPTCBC should seek to align themselves with appropriate external standards such as ISO27001 or the Local Public Services Data Handling Guidelines. This will allow them to benchmark their performance in this area.	PSN CoCo is aligned with ISO 27000 and we are accredited to the PSN network. Implementation date: Completed. Responsibility: Steve John.		
a20. NPTCBC should develop and maintain KPIs in respect of data protection compliance which should be monitored by the ISG and CGG.	Agreed. Implementation date: 28 June 2014. Responsibility: David Michael.		
a21. NPTCBC should develop a formal policy in regard to PIAs and continue to use PIAs, in the long term, for any projects with significant data	NPTCBC will assess the effectiveness of PIAs and availability of resources. Implementation date: 28 October 2014.		

protection implications, IT related or otherwise.	Responsibility: David Michael.		
a22. NPTCBC should initiate a procedure whereby each PIA is reviewed, after implementation of the system or process that was the subject of the PIA, to ensure that the agreed measures have been implemented and are effective. These reviews should also feed into regular, wider reviews of the PIA process as a whole, to ensure that it is operating effectively.	This will be an outcome of the previous recommendation. Implementation date: 28 October 2014. Responsibility: Steve John.		
a24. All data protection policies should follow an agreed format and carry information on the version control process (i.e. have named owners, an overview of amendments and dates of creation, last and next scheduled review), which should be set out within a brief 'Policy on Policies' guidance	Partially agreed. We don't see the relevance of the "Policy on Policies" document. Implementation date: 28 June 2014. Responsibility: David Michael.		

document.			
a25. There should be a clearly defined and consistent process in relation to the creation, ratification and review of policies, to ensure that these policies remain fit for purpose.	NPTCBC will ensure that the responsible officers (David Michael, Ian John and Paul Watkins) are consulted in the creation of these policies which will be further considered by the Corporate Governance Group (CGG). Implementation date: 28 June 2014. Responsibility: David Michael.		
a26. See a25.	See a25.		
a27. See a25.	See a25.		
b1. NPTCBC should assign specific responsibility for providing oversight of the completion and effectiveness of data protection training and for identifying and mandating any associated improvements to the CGG and / or ISG.	The ISG will provide advice and assistance to Directorate Management Teams in data protection training and obtain assurance that such training is being carried out (for example, a "dip sample"), but there will be no extra resource to provide central monitoring. Implementation date: 28 June 2014.		

	Responsibility: David Michael.		
b4. NPTCBC should assign clear ownership for the provision of and monitoring of the completion and effectiveness of, corporate data protection training, to a key post or individual of appropriate seniority who will be responsible for reporting regularly to the CGG and / or ISG to allow them to maintain the oversight referred to in b1.	See b1. Implementation date: 28 June 2014. Responsibility: David Michael.		
b5. NPTCBC should establish a corporate data protection training programme, including initial induction training, regular refresher training and on-going needs-based training. The programme should be designed to meet the training needs for all members of staff with access to (or specific responsibilities in	ISG will develop a programme for training and training needs assessment. Implementation date: 28 October 2014. Responsibility: David Michael.		

respect of) personal data within agreed timescales. This programme should be approved by the ISG and CGG.			
b6. NPTCBC should ensure that training needs analysis is regularly conducted for all staff groups, including temporary and contract staff, with access to, or specific responsibilities in respect of, personal data. This should feed into the training programme.	Guidance will be given to Directorates on the need to assess training requirements. Implementation date: June 2014. Responsibility: David Michael.		
b7. Records in respect of all data protection training should be maintained on Vision for central monitoring purposes.	Agreed. Implementation date: June 2014. Responsibility: David Michael.		
b8. Monitoring information in respect of any data protection training undertaken at NPTCBC must be reported through to the ISG and CGG, once a	ISG when constituted will consider whether this will be beneficial. Implementation date: 28 October 2014.		

corporate data protection training programme is established. NPTCBC should also develop KPIs in respect of data protection training to provide oversight and drive performance.	Responsibility: David Michael.		
b9. See b8.	See b8.		
b10. See b6. Training needs for individual staff should be regularly assessed, for example at performance appraisals.	Data protection training needs will be assessed by Directorate Management Teams in accordance with their own assessment methods. Implementation date: 28 October 2014. Responsibility: Graham Jones.		
b11. NPTCBC should ensure that there are appropriate processes to identify and follow up non-attendance at / non-completion of data protection training, once a corporate data protection training programme is established.	Non-attendance at data protection training will be identified and followed up by Directorate Management Teams, for example, via a "dip sample". Implementation date: October 2014. Responsibility: David		

	Michael and Graham Jones.		
b12. As part of the corporate data protection training programme, NPTCBC should develop and introduce an appropriate data protection training course which is mandatory for all members of staff. This training should be delivered at induction and refreshed annually.	Data protection material and a summary of the Data Protection Policy should be available to all new staff. We will look at the possibility of electronic training. Implementation date: October 2014. Responsibility: David Michael and Graham Jones.		
b15. NPTCBC should implement a mechanism to ensure that employees have read all relevant policies (for example, a question and answer exercise) and are aware of where to locate them.	Agreed. Implementation date: October 2014. Responsibility: David Michael and Graham Jones.		
b16. See b12.	See b12.		
b17. Specific data protection training for specialised roles (for example, DPO, Records Manager, Information Asset Owners, once introduced) and	Agreed. Implementation date: 28 June 2014. Responsibility: David Michael, Steve John and		

relevant senior posts should be provided.	Graham Jones.		
b18. All employees who are expected to process subject access requests should receive appropriate specialist training.	Agreed. Implementation date: 28 June 2014. Responsibility: David Michael and Graham Jones.		
b22. NPTCBC should consider regular spot checks to monitor staff knowledge of data protection policies and to ensure that those policies are fit for purpose as an extension to the mechanism cited at b15.	ISG when constituted will consider whether this will be beneficial. Implementation date: 28 October 2014. Responsibility: David Michael and Graham Jones.		
b25. NPTCBC should ensure that relevant data protection issues are discussed at team meetings and utilise the ICO 'Th!nk Privacy' materials to raise awareness more generally.	To be considered at the next meeting of CGG. Implementation date: March 2014. Responsibility: David Michael, Steve John and Graham Jones.		
c4. The FCWG should include SARs as a standing agenda item to ensure that relevant	Agreed. Implementation date: 28 March 2014.		

issues are discussed, reporting mechanisms and that processes are working effectively, and NPTCBC is processing SARs within DPA requirements.	Responsibility: David Michael & Dave Rees.		
c7. NPTCBC should produce and regularly review desk instructions for those employees who process SARs within all Directorates, to ensure that a consistent process is followed across NPTCBC. The Corporate Solicitor or the DPO should be consulted prior to sign off to ensure that this guidance is consistent and reflects the agreed process. NPTCBC may wish to consider the ICO SAR Code of Practice for reference.	Agreed. Implementation date: 28 June 2014. Responsibility: David Michael.		
c8. NPTCBC should ensure that employees have access to consistent guidance and information about SARs by placing the	Agreed. Implementation date: March 2014. Responsibility: Ian John.		

Data Protection Policy and SAR guidance and desk instructions in a dedicated area on the intranet. This area should include contact details for employees to use to request guidance or assistance when dealing with requests.			
c10. See c7.	See c7.		
c11. See c16.	See c16.		
c12. See b18. NPTCBC should develop SAR training to provide to staff at induction, and as required to maintain awareness after induction, to ensure that SARs are handled in accordance with NPTCBC policy and in compliance with the DPA. The DPO and Corporate Solicitor should have oversight of the content.	Agreed. Implementation date: 28 October 2014. Responsibility: David Michael & Graham Jones.		
c14. In order to accurately collate information about request processing, NPTCBC should create a template for use	Agreed. Implementation date: 28 October 2014. Responsibility: David		

within all Directorates to record requests. NPTCBC should ensure that information relevant to SARs is included, such as the relevant day, sign off, exemptions, redactions, quality assurance checks and requests which require further information. These should be collated and reviewed centrally and outcomes reported to the DPO on a regular basis.	Michael & Dave Rees.		
c14. NPTCBC should require employees to inform FOI Coordinators when they are dealing with a request so that it can be accurately recorded on the local record and central database.	Employees will be required to inform FOI Coordinators when they are dealing with formal subject access requests, as opposed to requests dealt with in the normal course of business. Implementation date: 28 June 2014. Responsibility: David Michael & Dave Rees.		
c15. Centralised standard guidance, included in desk	Agreed. Implementation date: 28		

instructions, should contain details of the information which should be kept in local SAR files for audit, monitoring and quality assurance purposes.	June 2014. Responsibility: David Michael.		
c15. Within Directorates, responsibility for retaining SAR files in a specified location should be assigned to suitable members of staff (e.g. the FOI Coordinators) to ensure that records are consistently held for all requests, and can be located in case they are required for review.	Agreed. Implementation date: 28 June 2014. Responsibility: David Michael.		
c16. To ensure that NPTCBC is processing SARs in compliance with the DPA requirements, SAR figures and compliance times from SAR logs should be reported, on a regular basis, by Directorates and Support Services to the DPO; for example,	Agreed. Implementation date: 28 October 2014. Responsibility: David Michael.		

through the FCWG. This will provide NPTCBC with more accurate information about SAR compliance and the resources used to respond to requests, as well as providing the DPO with appropriate oversight of processing. Where issues are identified, these should be escalated, by the DPO, to the CGG and / or ISG.			
c17. NPTCBC should introduce a quality assurance process to periodically review responses to requests and gain assurance that employees are responding to requests in compliance with DPA requirements. These could be linked to KPIs to drive performance going forward.	Agreed. Implementation date: 28 October 2014. Responsibility: David Michael & Dave Rees.		
c18. Subsequent to the implementation of the recommendations arising from this report, NPTCBC should carry	Will be included in normal internal audit work plan. Implementation date: 28 October 2014.		

out SAR compliance audits to provide a continuing level of assurance on the effectiveness of controls implemented for processing requests.	Responsibility: David Michael & Dave Rees.		
c19. See second recommendation at c15.	See second recommendation at c15.		
c21. See c7. NPTCBC should include a section about the process to follow for disclosures, within the desk instructions and the SAR guidance, to ensure that staff will follow the appropriate process.	Agreed. Implementation date: 28 June 2014. Responsibility: David Michael.		
c22. Quality assurance checks should be carried out on disclosures to assure NPTCBC that disclosures made by staff are appropriate and any issues are identified and reported as required.	ISG when constituted will consider whether this will be beneficial. Implementation date: 28 October 2014. Responsibility: David Michael.		
c23. Disclosures should be recorded in	Agreed.		

all Directorates, to provide an audit trail and accurate records / statistical information that can be reported to the DPO. See also second recommendation at c14.	Implementation date: 28 June 2014. Responsibility: David Michael and Directorate Management.		
d2. NPTCBC should draft and implement a corporate ISA policy and procedure which sets out a clear process for staff to follow when wishing to share data via an ISA.	Agreed. Implementation date: 28 October 2014. Responsibility: David Michael.		
d3. Ensure that Legal Services are consulted for all new proposed ISAs; NPTCBC should include the requirement for Legal Services referral within the ISA process, prior to sign off at Director level.	Agreed subject to sign off at Head of Service level. Implementation date: 28 March 2014. Responsibility: David Michael.		
d5. To reduce the risk of unauthorised disclosure or data loss, NPTCBC should provide specialist training for operational staff and	Agreed. Implementation date: 28 October 2014. Responsibility: David		

managers who regularly share data, especially those working within an ISA. As a matter of good practice, this should be provided to relevant staff at induction and refreshed on a regular basis and when any changes occur to the ISA. Additionally, once the new ISA policy has been approved, NPTCBC should disseminate it to relevant staff to ensure that they are up to date on the new process to be followed. See also b17.	Michael and Directorate Management.		
d6. Ensure that employees are aware of any additional or specific data sharing responsibilities they may have under an ISA; NPTCBC should produce awareness material which will draw attention to their areas of responsibility within related ISAs.	Agreed. Implementation date: 28 October 2014. Responsibility: David Michael.		

This will assist NPTCBC in complying with the requirements of WASPI.			
d10. As a matter of good practice, the provision of fair processing information should also be included in the policy referred to in d2.	Agreed. Implementation date: 28 October 2014. Responsibility: David Michael.		
d11. To help ensure that information is only shared when it is appropriate to do so, NPTCBC should document this process within the central policy or procedure referred to in the recommendation at d2.	Agreed. May require formal delegated authority. Implementation date: 28 October 2014. Responsibility: David Michael.		
d13. When they are next due for review, NPTCBC should update and standardise older ISA documentation to ensure that employees are clear that the ISA is still in effect and that it is still fit for purpose.	Agreed. Implementation date: 28 March 2014. Responsibility: David Michael.		
d14. NPTCBC should create and publish a central register, for all ISAs to which they are	Agreed. Implementation date: 28 March 2014.		

a party, on the intranet. Details about the nature of the sharing, the agencies involved and the renewal or review dates for each agreement should also be listed as a matter of good practice. The list should have appropriate senior oversight to ensure that signatories review their ISAs as required. Additionally, details about the review and approval process cited at d3 should be included in the ISA policy and procedures referred to in d2.	Responsibility: David Michael.		
d15. See d14.	See d14.		
d16. See d6.	See d6.		
d18. NPTCBC should ensure the quality of shared information by implementing reviews of data quality as part of regular checks or audits. Results should be reported to staff to raise awareness of any issues identified and	Agreed. Implementation date: 28 October 2014. Responsibility: Directorate Management.		

any concerns reported to senior management in order to identify any trends or risks and to allow appropriate action to be taken.			
d19. NPTCBC should implement agreed retention and deletion processes within ISAs at the next review. This should include a provision for related checks to be carried out, as appropriate, within the ISA and to be recorded as part of the review process. This will assist NPTCBC in complying with the requirements of WASPI.	Agreed. Implementation date: 28 March 2014. Responsibility: David Michael.		
d20. NPTCBC should regularly review requests for information and responses to ensure ongoing compliance with ISA requirements. The review should link in as part of a performance review process for employees who regularly share	Agreed. Implementation date: 28 June 2014. Responsibility: Directorate Management.		

data.			
d23. To ensure that any data sharing incidents continue to be reported appropriately, the ISA policy (once drafted) should include reference to the Incident Reporting Policy and the steps to be taken in the event of a data breach (or 'near miss') occurring. See also d2 and a14.	Agreed. Implementation date: 28 October 2014. Responsibility: David Michael.		
d25. NPTCBC should include a checking mechanism (such as signed compliance statements) within the ISA review process to provide assurance that partner organisations are adhering to the security requirements in respect of NPTCBC ISAs. This will assist NPTCBC in complying with the requirements of WASPI.	Agreed. Implementation date: 28 October 2014. Responsibility: David Michael.		