AGENDA ITEM NO. 6(4)

POLICY AND RESOURCES SCRUTINY COMMITTEE - 19TH JANUARY 2010

SUBJECT: ARRANGEMENTS FOR EXCHANGE OF INFORMATION BETWEEN PUBLIC SECTOR BODIES INVOLVING CCBC

REPORT BY: DIRECTOR OF CORPORATE SERVICES

---

1. PURPOSE OF REPORT

1.1 To inform Members of existing arrangements for exchange of information between Caerphilly CBC and other public sector bodies, in particular the exchange of personal data.

1.2 To inform Members of Corporate Management Team's response to recommendations on how exchange of personal data can be improved to ensure the Council complies with its legal obligations, in particular under the Data Protection Act 1998.

2. SUMMARY

2.1 Exchange of personal data across organisations is fundamental to providing services to the public. However personal data must be handled responsibly and with confidence, and recent media interest in illegal disclosures of personal data has led to increased interest by the Information Commissioner and auditors in ensuring that public bodies protect the personal data that they are entrusted with.

2.2 A survey of arrangements for exchanging personal data across the Council has led to a number of recommendations as outlined in section 8, including sign up to the Wales Accord for the Sharing of Personal Information (WASPI) and raising awareness Council-wide of the need to protect personal data.

3. LINKS TO STRATEGY

3.1 Information Governance Action Plan, agreed at Strategic Information Group in April 2008 as a strategy for information management for the Council.

4. THE REPORT

Introduction

4.1 CMT requested an update on information sharing arrangements that are currently in place to indicate areas in need of improvement, and a report was submitted for their consideration early in December 2009. The report was as follows.

4.2 The Head of Policy and Central Services, Tim Peppin, had previously submitted a report to CMT on 31 May 2007 on Information Sharing Protocols, focusing especially on information sharing with Gwent Police and the Wales Accord for the Sharing of Personal Information (WASPI).

4.3 The report gave an indication of arrangements for exchange of personal data with other public sector bodies based on responses to a request in November 2009 from the Head of Information, Communications, Technology and Property, Phil Evans, to all Heads of Service and Directors. The appendix to this report details the responses received.

4.4 This report principally addresses personal data sharing with other public sector bodies, and whilst recommendations will apply equally to personal data sharing with the voluntary sector, private organisations and internally within the Council, some additional work will be required to ensure all instances of personal data sharing by the Authority is satisfactory.

The Council's obligation to protect personal data

4.5 Exchange of personal data across organisations is fundamental to providing services to the public. However personal data must be handled responsibly, and organisations that fail in their obligations to do so are at risk of financial penalties as well as losing the trust of the public, as we have seen from recent media interest in handling of personal data. A recent press released from the Information Commissioner (ICO) said that in the two years since the HMRC data loss in 2007, 711 security breaches involving personal data had been reported, and the ICO have taken action against 54 organisations for significant security breaches. The ICO said 'We are keen to encourage organisations to achieve better data protection compliance and we expect that the prospect of a significant fine for reckless or deliberate data breaches will focus minds at Board level'.

4.6 The spotlight on mishandling personal data has also fostered confusion amongst professionals who are not sure when they may share personal data, and this poses the risk of either too much information being shared or not enough, with consequent detriment to service users.

4.7 Handling data responsibly means complying with the 8 principles of the Data Protection Act 1998, which are that personal data should be:

1. Fairly and lawfully processed
2. Processed for limited purposes
3. Adequate, relevant and not excessive
4. Accurate
5. Not kept for longer than necessary
6. Processed in line with data subject's rights
7. Securely processed
8. Not transferred outside European Economic Area

The ICO has developed a Personal Information Promise (see appendix 2) that all organisations can sign up to as a powerful message to the organisation's staff and the public from the very top of an organisation that protecting personal information in line with these eight principles is a key organisational aim. If the Council were to sign up to this Promise it would reinforce the Council's commitment to handling personal data responsibly.

4.8 Information sharing protocols provide a framework for sharing personal data. Existence of a protocol does not confer legal authority to share personal data, but they are a useful tool to ensure that the legislation that may enable the information sharing is considered carefully, and that the method of sharing personal data is selected to minimise risk of illegal and unfair disclosures. A protocol also allays much of the confusion that surrounds sharing personal data, as they provide clear ground rules on the circumstances in which information can be shared, what type of information can be shared, frequency of sharing, by what means (post, email, telephoned, meeting, etc), and so on. If a problem with CCBC's information sharing were to be investigated by the Information Commissioner, many of the areas of information sharing that the ICO would investigate (e.g. fairness, transparency, security, impact on privacy, etc) would be addressed by a well-drafted information sharing protocol, existence of which would indicate that good practice is being followed by the Council.

4.9 In addition, the Information Commissioner recommends that organisations involved in projects that might have implications for people's privacy consider undertaking Privacy Impact Assessments to identify any privacy concerns and address them at an early stage. The ICO argues that organisations take considerable care to manage a variety of risks, including natural disasters, environmental contamination and cyber-attacks, and in todays climate privacy now poses risks which need to be professionally managed in a similar way to other categories of risk. Incorporating the ICO Privacy Impact Assessment handbook into the early stages of project plans across the Council would enable the Authority to identify presence and level of risk and to make plans to mitigate the risk, and clearly this would be a sound basis for going forward.

Current analysis

Wales Accord on the Sharing of Personal Information

4.10 This report will provide an update on WASPI first, as WASPI underpins all information sharing work in the public sector, before going on to talk about other arrangements for sharing personal data.

4.11 Sign-up to tier 1 of WASPI was considered by Corporate Information Group at Caerphilly County Borough Council in early 2007, however it was felt that the protocol was very health focused, and it was decided to seek further information from the Design Team before committing. Other local authorities came to a similar conclusion, and few have signed up to date.

4.12 The WASPI Design Team rectified the problems with WASPI at a recent review, including simplifying the WASPI framework from 4 tiers down to 2 tiers, and the Design Team was restructured to make it less health-focused. Many initiatives are now referencing WASPI, for example in the areas of criminal justice, public safety, and recent Personal Information Sharing Protocols (PISP's) designed by CCBC for the Local Service Board (see paragraph 4.16c); and the Inspector of Police has indicated that WASPI will be recommended to Wales ACPO as it is potentially better than existing ACPO guidelines.

4.13 Responsibility for WASPI is being assumed by the Welsh Assembly Government and a decision has been taken in principle by a WAG committee that WASPI will be used throughout the public sector in Wales. WAG are looking at the corporate governance issues around how to enforce this and Richard Howells of Aneurin Bevan Health Board, a leading member of the Design Team, has recently advised Wales Information Group that mandating WASPI is very close for all public sector organisations.

4.14 WASPI gives a good framework for sharing personal data, instilling confidence in users that their activities are legal and fair to the data subject. If the Council were to sign-up to WASPI it would prevent the Council being forced to sign up at a later date, and it would provide a reference point for further information sharing protocols to be developed in areas of the Council that are experiencing problems with sharing personal data. It is advisable that the Council looks again at the WASPI self-assessment toolkit to determine how far we comply with the WASPI vision for data sharing, and what improvements need to be made. It is also advisable that any protocols the Council enters into in future are based as closely on WASPI as possible.

Other arrangements for sharing personal data

4.15 The responses in the appendix to this report indicate that whilst some of the arrangements for exchange of information are purely about sharing information (for example the Gwent Police S115 protocol and WASPI), the majority relate to Council functions within which information exchange is a core element (for example the All Wales Child Protection Procedures). Sub-sections 4.16 to 4.19 give examples of the different types of information sharing arrangements in use within the Council. The examples given are simply to illustrate the type of arrangement, and should not be taken in isolation.

4.16 Information sharing protocol

a) During compilation of this report, many respondents claim to be acting under specific information sharing protocols, but are not aware that the protocol has been superseded for example the Gwent Information Sharing Protocol between Health and Social Care Partners in Gwent 2004 has been superseded by WASPI); is still in draft (for example the draft South East Wales Public Protection Services protocol, which the police are trying to connect with WASPI); or the respondent did not have a copy of the protocol that they claim to be acting in accordance with. This alerts us to one of the dangers of having an information sharing protocol. Officers may develop a protocol as a 'tick-box' exercise, but then never refer to it again. If a protocol is developed the document must be referenced when sharing personal data, and must be updated frequently as needs evolve. This raises the question of whether application of protocols needs to be audited periodically.

b) Examples of specific information sharing protocols include the Gwent Police Information Sharing Agreement under S.115 of the Crime and Disorder Act, which existed for some time to facilitate information sharing between the police and a wide variety of other organisations. An updated version specific to sharing information between local authorities and Gwent Police and based on ACPO's Management of Police Information (MOPI) rules was brought to CMT in July 2008. The Community Safety and Housing Sections of the Council have commented that the updated protocol is useful and fit for purpose, although a return to a wider signatory list has been suggested and will be considered during review of the protocol early in 2010. The protocol will be publicised at a Management Network session soon. It is likely that this protocol will become a tier 2 Personal Information Sharing Protocol (PISP) under WASPI if Gwent Police decides to follow WASPI rather than existing ACPO guidelines. The Corporate Information Unit has developed good working relationships with Gwent Police, which will facilitate future developments in information sharing with the police.

c) The Caerphilly Mental Health Assertive Outreach Team, Multi-Agency Partnership Service (MAPS) for Mental Health Day Services and First Access Mental Health are tier 2 PISP's under WASPI. The MAPS and First Access protocols were developed as part of a Local Service Board led project to improve information sharing within priority areas in social care, and feedback has been received that the MAPS protocol in particular has improved day-to-day work. These protocols will be publicised on the WASPI website in order to share good practice in information sharing across Wales.

d) A number of protocols have been produced for personal data sharing that are specific to a particular service. For example the Local Resilience Forum has a protocol between several local organisations to formalise information relating to a major incident. CCBC are signed up to a protocol with Menter Iaith Cymru to share contact information about Welsh speaking individuals and organisations. The Council has also signed up to a Ryder Cup Wales Infrastructure Group information sharing protocol to facilitate sharing of information on contingency plans, transport, and attendees, including VIP protection.

4.17 Operational protocol/guidance

a. Preparation for this report has indicated that much information sharing takes place routinely as part of day-to-day business. Inconsistency in the type of information disclosed by Service Areas indicates that some officers have not thought to disclose certain occasions when they share personal data as this data sharing can not be considered in isolation from their day job. This means that it is unlikely all instances of personal data sharing with public sector bodies by the Council are contained within this report.

b. The fact that we cannot maintain an accurate inventory of all instances of sharing personal data supports the need for continued awareness raising across the Council on responsible handling of personal data. The Corporate Information Unit provides information to new starters at Induction Sessions, a section on data protection responsibilities has been

added to the revised Statement of Particulars for new employees, information is available on the intranet, and training sessions are run periodically, but more work needs to done, including ensuring managers are accountable for information sharing within their own area of work.

c. Operational protocols/guidance, which are focused on how to carry out a Council functions but also often contain guidance on information exchange, include the All Wales Child Protection Procedures; Referral arrangements for the General Teaching Council for Wales and for the Independent Safeguarding Authority; documented working relationships between the Council's Family Information Service and Care Standards Inspectorate for Wales; and Responsible Authority Memorandum of Understanding between several Council service areas (Trading Standards, Environmental Health, Planning, Social Services) & external bodies such as the Fire Service & Gwent Police. Further information on how each of these documents impact on information sharing can be found in appendix 1.

4.18 Data sharing without protocols in place

a. There will be many instances of personal data sharing that do not involve formal protocols. For example, Trading Standards share and request information as part of the Council's enforcement role using powers under numerous pieces of legislation. In some instances standard forms are supplied (for example by DWP or HMRC), in other cases Trading Standards will write stating powers & request the specific information. Registration Service share birth/death details with the local health board and details of suspected sham marriages or civil partnerships with the Home Office. NNDR share details of council tax and business ratepayers with HMRC in order to prevent and detect fraud. School Transport share information with other local authorities on serious issues relating to drivers and reference requests for drivers not known to the Council. All of these examples include sharing of personal data without abiding by the terms of an information sharing protocol, but this does not mean that the personal data sharing is flawed or will necessarily cause a problem.

b. However in some circumstances if no protocol is in place it raises the question whether the sharing of personal data has been thought through in sufficient detail to ensure it is i) fair and lawful, and ii) secure; and whether the process of sharing data is clear enough to prevent confusion and hesitation amongst officers which could affect service users. During data protection training courses, the Corporate Information Unit advises officers to consider whether having a clearly defined protocol would improve working practices. If the answer is yes, the Information Unit will provide further support in developing one.

4.19 Sharing information with data processors

a. As a result of this exercise and previous work undertaken by the Corporate Information Unit, the Council needs to evaluate how satisfactory our arrangements are for sharing personal data with other organisations that are undertaking work on the Council's behalf. For example, a social care contractor may be employed by the Council to provide care for a particular client, and would therefore need personal details of the client including his/her needs to provide appropriate care. If the third party organisation processes personal data on behalf of the Council, and makes a mistake, the Council would be liable for the mistake. To defend ourselves in this situation, it is important that contracts and Service Level Agreements include clauses on maintaining a good organisational knowledge of the Data Protection Act 1998, including staff awareness, procedures in place for keeping information secure, compliance with the eight DPA principles, and procedures to notify the Council in the event of a mistake occurring. The Council needs to be able to demonstrate that checks on the DPA awareness of the organisation were carried out before entering into an agreement with them, and awareness is continually monitored.

At the meeting on 3 December 2009, Corporate Management Team agreed the following:

4.20 The Council will sign up to the ICO's Personal Information Promise to reinforce the Council's commitment to handling personal data responsibly.

4.21 The Council will sign up to tier 1 of WASPI, and use the self-assessment checklist alongside Local Government Data Handling Guidelines to determine where improvements to personal information sharing practice must be made.

4.22 Future information sharing protocols entered into by the Council will be based on WASPI. Service Areas to refer to Corporate Information Unit for advice on developing new information sharing protocols, and when complete, the protocol will be appropriately signed, a copy lodged with the Corporate Information Unit, and officers must be made aware of how to share information responsibly using the protocol.

4.23 It was recommended that consideration be given to using the ICO's Privacy Impact Assessment handbook when undertaking new schemes of work within the Council. CMT requested further information on how the assessments work in practice, and on benefits that they could deliver for the Council's handling of personal data.

4.24 Managers need to ensure that when information is shared within an area of work for which an information sharing protocol exists, officers are referencing the protocol and acting in accordance with it. CMT requested that this principle should be reiterated at Departmental Management Team meetings. Key protocols/arrangements that apply to personal data sharing activities that present a high-risk level of risk to the authority will also be audited.

4.25 Where information sharing protocols are not in place, managers must ensure officers are aware of the need to comply with the data protection principles, in particular that the means of transferring data must be secure and appropriate authorisations of relevant managers are in place. CMT requested that this principle should be reiterated at Departmental Management Team meetings.

4.26 Ensure appropriate checks and contractual conditions are placed on third party organisations that process personal data on behalf of the Council, to protect the Council in the event of a mistake. CMT also requested this requirement to be raised at Departmental Management Team meetings.

4.27 Although the recommendations above will equally apply to personal information sharing with the voluntary sector, private organisations and internally across Service Areas of the Council, further work needs to be undertaken to ensure this type of personal sharing is carried out appropriately.

5. FINANCIAL IMPLICATIONS

5.1 Illegal disclosure of personal data could result in financial penalties and associated adverse publicity.

6. PERSONNEL IMPLICATIONS

6.1 Yet to be defined.

7. CONSULTATIONS

7.1 Corporate Management Team.

8. RECOMMENDATIONS

8.1 It is recommended that the contents of the report be noted.

9. REASONS FOR THE RECOMMENDATIONS

9.1 To ensure Members are aware of the measures being taken to safeguard personal data exchanged by the Council with other public sector organisations.

10. STATUTORY POWER

10.1 Data Protection Act 1998

Author: Joanne Jones, Information Officer
Consultees: Corporate Management Team

Background Papers:
Information Commissioner's Office – 'Sharing Personal Information: Our Approach', April 2007
Information Commissioner's Office – 'Framework Code of Practice for Sharing Personal Information', October 2007
Information Commissioner's Office – 'Privacy Impact Assessment (PIA) handbook (Version 2)', June 2009

Appendices:
Appendix 1 Table listing information sharing arrangements for exchange of information between public sector bodies involving Caerphilly County Borough Council.
Appendix 2 Personal Information Promise