

**READING BOROUGH COUNCIL**  
**RESPONSE TO DATA SHARING REVIEW**

This is the response of Reading Borough Council to the independent review of the use and sharing of personal information in the public sector, commissioned by the Prime Minister from the Information Commissioner and the Wellcome Trust.

**Q1 –**

The Council is a Unitary local authority and therefore holds and processes personal data across a wide range of public services. On a recent count we had in use around 180 different databases containing personal information, ranging from major corporate and Borough-wide systems (Council Tax, Elections, Rents) to local service information held on Excel spreadsheets.

We have a particular interest in joint working with partner public and volunteer bodies, i.e. Police, Health, Local Authorities, Youth Justice Board, Housing Partners, etc. We also receive from and pass personal data to Government Departments and agencies, including the Department of Work and Pensions and the Audit Commission. We use a number of external contractors to process personal data on our behalf, including Council Tax, Housing Benefits, Electoral Registration. We have externalised our IT services, and also the provision of some Housing and Parking Services, and therefore have private contractors who process personal data as part of their contract to deliver services on our behalf.

The information we hold and share ranges from Name/Address all the way through to many years of complete social care and housing data including full tenancy history and full social care client history (i.e. sexual abuse, mental health, etc). Information is shared verbally, via email (mostly secure / encrypted), electronically via floppy disk/CD and in paper copies.

We hold and collect this information to meet our statutory requirements and duties, and in some cases these are prescriptive in the extent to which we can share the data (Electoral Registration, Council Tax).

**Q2 –**

Sharing personal data allows us to protect our residents, tenants and customers from unsafe, unruly and abusive situations, and fraud, as well as protecting child and adults from physical/mental abuse. Basically, it allows us to meet our statutory duties as a Council with Community Safety, Childcare and Adult Social Care Responsibilities, and as a Registered Social Landlord, education, public health, trading standards and planning authority.

a) We share to individuals as per Subject Access Requests and on individual cases in relation to specific incidents.

b) Personal data is not supplied in general to society. It may be provided to other Council services, and to Councillors, under the Council's data protection registration.

**Q3 –**

We consider the risks of sharing personal information to individuals and to society as being comparable.

The principal risk is that the Council could find itself in breach of the Data Protection Act. Personal information may be disclosed to third parties without proper consent or checking.

In addition, the data could be misunderstood and/or incorrect/wrong information could be given (or worse case someone else's). For example, someone could ask for Subject Access Request on all information about them, and we get a hit on an adoption case in which the child's new address could be given out to with SAR to a parent from whom the child had been taken away. Such situations are addressed through local data sharing protocols which introduce controls on disclosure (linked to consent) based on a risk assessment.

Other risks are linked to the transfer of personal data between the Council and other bodies (including our own contractors), where we consider there to be a number of areas of potential insecurity (loss, interception), and where we are currently reviewing and tightening our own methods of transmission, both electronic and manual.

**Q4 –**

There are numerous reasons as to why we need to share data, but they can appear sometimes to conflict with DPA requirements. More emphasis should be placed on sharing the information securely, rather than why we share the information: if a child/adult life is at risk then we are going to share no matter what the DPA states. Recent incidents in the press highlight the dangers of being over-cautious in sharing (cause people fall back onto DPA - i.e. Soham murders). In the more recent data loss cases the issue was not whether the data should be shared, but how – ie transmission: this appears to be a significant area of risk, both for manual records (non-recorded delivery) and electronic records (non encrypting data).

**Q5 –**

The issue is less the volume of data held, but the length of time we hold it. There is always the potential to hold the data for too long, by not having or following retention/deletion processes. Data management is not usually seen as a high profile administrative task, whilst there is a natural tendency to caution in retaining records where there is a likelihood of the subject reappearing.

Generally the authority has good and secure processes for holding the data for its specific purpose, but may sometimes see difficulties in sharing it internally with other services. This applies particularly to Council Tax and Electoral data, which have the potential to be a good base sources of information on property and residents in the borough, but where the data can only be used for legally prescribed purposes. A more flexible approach could assist with data accuracy, consistency and cleansing.

**Q6 - no answer**

**Q7 –**

Questions 5 helps with this answer. There are restrictions on sharing Council Tax and Elections data internally, with the result that we do not proactively explore inconsistencies which may indicate either fraud, or more fundamental demographic changes (eg immigration) which can impact on the authority's overall service delivery.

**Q8 –**

We have recently undertaken a security audit, and we do not consider that we are in the situation where data is being shared which shouldn't be. However, in some databases, we identified concerns about the data being shared without proper checks or adequate security of transmission, which we are now addressing.

**Q9 –**

As indicated above, the DPA, together with other legal constraints, may have the effect within the authority of discouraging data matching and data mining, to support data cleansing, to identify demographic trends and changes across services, and to identify fraud, as well as ensuring that out citizens get all the help they need. For example, if Council Tax data could be shared with Social Services then Social Workers would be aware their client are having issues paying Council Tax (or overpaying as does happen), and could proactively assist. Similarly, Environmental Health data on Houses in Multiple Occupation, or the residents' parking data base, could provide useful points of reference against which the electoral registration database could be checked for accuracy.

We would like to see exceptions for government bodies to share data to allow them to combat fraud as well as being able to be more proactive in helping society. However, we would not wish to see the private sector given this right, as it could lead to a monopoly situation and we would not necessary benefit from it.

We would draw your attention to the current legal confusion being caused by the National Fraud Initiative, and the Audit Commission's desire to access and match Council Tax and Electoral Registration databases to identify fraud. This appears to be incompatible with election law. Different legislation is facing in different directions, and there is a need for more consistent and joined up thinking by the Government.

**Q10 –**

We consider that public bodies adhere to the second principle of the DPA, but it can cause operational problems and can sometimes have the potential to put lives at risk through discouraging disclosure to partners - which is the opposite of what local authorities are there to do, in particular in relation to vulnerable clients.

**Q11 –**

We don't think there are technical barriers (apart from funding), but we would like to see a more formal (and enforced) secure connection for sharing data between all public sector bodies. There can be cultural issues of officers focusing on DPA compliance rather than the needs of a vulnerable client. There is also the issue of society being unable to understand why Police/Health etc didn't share data to stop someone from being killed (which inevitably attracts critical press comment).

**Q12 –**

More clarification (whether in the Act or supportive [legal] documents) - making it very clear that if we have a duty to share data under other legislation (eg Children's Act) then this will take precedence over the DPA principle of whether we should share.

Also, more focus on the security of data transmission – but in terms of good practice rather than statutory prescription.

**Q13 –**

This is a continuation of point 9. There are too many references to sharing data in numerous acts with regard to public sector working and this make it very hard to understand what we can share and when. As indicated in 9, some pieces of legislation work against each other. Standardising data sharing this across all relevant legislation would make it much clearer and easier to manage, and would lead to fewer mistakes.

**Q14 –**

We would welcome the development by central government of a secure network for local authorities (like the Police and Health have) for the sharing of data. Police and health staff sometimes assume that all public sector bodies have secure e-mail and thus they can e-mail us data which in reality goes unencrypted over the public internet.

**Q15 –**

See 9 and 13 above

**Q16 –**

More clarity over this would be welcomed, especially in the Social Care arena. Care should be taken to avoid undue bureaucracy, especially where his can work against MPs and Councillors in representing the interests of their electors.

**Q17 –**

People may have some medication condition which stops them from consenting, or fail to understand the significance of consent.

Some people will inevitably refuse to consent over concerns with "Big Brother", and may not always understand why consent is needed.

As indicated above, MPs and Councillors may feel constrained if they are required to ask their constituents to give them formal consent to represent them. This may act against their proactively and helpfully seeking to identify local people who are causing problems, or who may require care and attention (or indeed who may be a potential danger either to other residents or to Council property), with a view to helping them. It may also discourage constituents from approaching their democratic representatives in the first place.

I have been dealing only this week with a case where a ward Councillor, in trying to draw the Housing and Community Care services' attention to a vulnerable local resident (and Council tenant) who appeared to be a risk both to herself and to neighbours, was annoyed and frustrated to receive an unhelpful officer response citing the DPA as a reason for not giving him any information on the case [and possibly even not taking any action].

Formal consent requirements should be proportionate, and related to vulnerability. We already recognise this through local data sharing protocols applying to Children's services, Community Care and Crime and Disorder. These service areas raise issues that are of a different order from complaints about refuse bin collection.

There may be sense in the Information Commissioner setting out a generic data sharing protocol to apply as a basic level to all persona data records, and which organisations could supplement with more prescriptive local protocols as appropriate.

**Q18 –**

The DPA already gives individuals strong subject access rights.

**Q19 –**

There is a need to strike the balance between transparency, and operational efficiency: the sharing of personal data between partners should not be discouraged by time-consuming administrative procedures. The approach should as be proportionate: the more vulnerable the client, the more control processes may be justified.

As mentioned above, a generic data sharing protocol for all personal databases might prove helpful, as general guidance.

**Q20 –**

E-mail has made data sharing much easier – but it has also made the unintentional disclosure of personal data easier, and has opened the door for more interception due to unencrypted emails. Cheap CDs and ease of production again make it easy to share data (and as shown recently, easy to lose!). This also applies to laptops, and PDAs.

The risk is poor user understanding of the capacity of the technology they are operating. People may assume that everyone has compatible technology: this could put at risk the secure exchange of data between parties who are not on the same secure network (i.e. Health -> Local Authority).

**Q21 –**

Yes, there is sense in working to agreed standards of electronic data security, which should also cover when encryption should be used, i.e. PDAs, Laptops etc taken off site. Ideally, e-mail should either be encrypted or sent via closed networks. However for this to work the government will have to fund the public sector to ensure its all done at the same time, as if only 80% have a secure e-mail system, there will still be a requirement to communicate electronically with the remaining 20%.

**Q22 –**

Possibly – but as a local authority, the bulk of our day-to-day business is about processing personal data, and as mentioned above, care needs to be taken to avoid imposing more administration on already over-stretched authorities which are under Government pressure to deliver efficiency savings year-on-year, increasingly through making more joined-up use of electronic data processing. Anonymisation may be more appropriate for some personal data bases than others, dependant on levels of vulnerability, and should better be addressed through local (service-based) data sharing protocols.

**Q23 – 28: No comments**

15 February 2008.