SCRUTINY REVIEW OF DATA SHARING

MARCH 2017

Scrutiny Working Group:
Councillors Tranter, Spence and Hogarth

Facilitated by:-   Strategic Hub

Scrutiny Review of Data Sharing

1. Introduction

As part of the Scrutiny Committee Work programme for 2015/16 a review of data sharing was agreed. The scope for the review was agreed by Scrutiny Committee Members to be part of the Scrutiny Committee work programme for 2015/16 and 2016/17.

The review was identified following the review of partnership working. In addition, it was an appropriate response to concerns raised by the Director Service Delivery as Serious Case Reviews and higher level investigations have stated that data sharing remains a consistent blockage for effective partnership working and is often a contributory factor to poor service. In general terms data sharing is still problematic with restrictions on information from partners being most prevalent across the health sector, a partner who is recognised as being critical in West Midlands Fire Services (WMFS) ongoing journey towards excellence.

The purpose of the review was to:-

- Provide a clear picture of the level and effectiveness of data sharing between WMFS and partner agencies.

- Identify if there are lessons to be learned from other agencies and sectors.

- What improvements can be recommended and determine how fire authority members can support data sharing activities.

In discharging the scope of the review a Members working group was established made up of Councillors Tranter, Spence and Hogarth. However, during the review it became apparent that although data sharing was taking place, there was no formal structure in place. The proposals contained in this report address some areas that need addressing before members can assist in supporting data sharing activities.

2. Matters Arising

2.1   Governance of Data Sharing Policy

The review has highlighted that there is no Organisational policy in place to enable for the effective sharing of data in a way that ensures compliance with both legislative and Organisational requirements. Similarly, there is no policy in place outlining the Organisation's expectations as to what its data sharing priorities are and the principles of operation to enable for the high quality delivery of these expectations.

A Standing Order is in place for the Data Protection Act 1998 which refers to the treatment of personal information, however this reads as personal employee information and provides no specific mention to 'data sharing'.

Data sharing is part of the Data Protection Act 1998, however, for the purpose of this report the following definitions clarify the difference.

Data Protection

The Data Protection Act 1998 defines the way in which information about living people may be legally used and handled. The main intent is to protect individuals against misuse or abuse of information about them.

Data Sharing

Although Data Sharing is linked to The Data Protection Act, for the purpose of this review, it has been defined as:-

The disclosure of data from one organisation to a third party organisation to assist in identifying and supporting the most vulnerable people within the community.

There is evidence that data sharing is taking place across WMFS with the intention of supporting the progressive targeting of vulnerable individuals to enable the achievement of organisational priorities in delivering services to local communities. This occurs at many levels with some data sharing arrangements existing as part of a formalised approach through 'agreements' made during the establishment of relationships.

It is known that data sharing is taking place on a more informal basic across local command areas and may exist either with or without agreements in place.

To date it has not been possible to evidence the existence of a policy detailing the Organisation's intent and expectations with regard to data sharing. The normal Organisational approach to communicating key information is by Standing Orders.

The development of a policy with regard to data sharing will provide the platform against which a wider framework of guidance or procedural information to support the excellence in delivery of Organisational priorities. The main benefit of communicating policy will be that it will provide absolute clarity as to what the Organisation's expectations are in respect of the sharing of data. This is important because it appears that the approach to data sharing is inconsistent.

It is not intended that policy should be prescriptive. The Organisation is committed to encouraging personal accountability through an effective contribution. As part of this, innovation and flexibility in the pursuit of excellence, as opposed to a set of rules to be followed (as was previously the case with the production of policy through Standing Orders), is central to the delivery of effective data sharing partnerships and agreements. The policy should outline the Organisational expectations and principles of operation to be followed in meeting these operations.

The existence of a policy will protect both the Organisation and its employees through ensuring that employees clearly understand the Organisation's expectations and their part in how these will be delivered. In outlining the principles of operation (and in implementing an appropriate supporting procedural framework) to enable

individuals to develop their understanding, meet their specific accountabilities and deliver the organisation's expectations in this area, the Organisation will mitigate against any potential risk in this area. The policy should be designed to enable for legal compliance, best practice standards to be met and reduce the opportunity for employees to unintentionally get things wrong by setting out broadly who does what.

The production of a policy and supporting framework of information as well as providing clarity, will also help to build confidence in delivery through effective data sharing. This is because employees will be sure that they are using the appropriate approach to delivering their responsibilities, potentially increasing performance and improving outcomes. The existence of a policy and wider framework also provides a consistent reference and checkpoint to which the Organisation or its employees can refer.

From an assurance perspective, the existence of a policy and supporting procedures will help in measuring Organisational performance in achieving its strategic expectations. Policy, is seen as a first point of call when seeking to test or assure performance. The absence of policy setting out expectations is a weakness for the Organisation. Should this area be the focus of external audit or inspection, the failure to provide clarity through a policy as to the expectations of delivering regulatory or legal responsibilities could be seen as a significant failure leaving the Organisation's leadership team open to criticism.

Communicating the policy via Standing Orders will also ensure that any change in strategic direction or the legislative landscape governing data sharing can be considered and approved at the right strategic level. This is because of the requirement of a 'Strategic Enabler' to 'sign off' any subsequent changes to the Standing Order. This approach provides for an effective and auditable system of governance and decision making. It also enables for changing expectations to be communicated and achieved through an embedded and accepted communication approach.

There are no statutory guidelines in place for data sharing. Guidance is provided from a best practice perspective from the Home Office. There is also a Centre of Excellence for information sharing, this is a government body that provides helpful guidance in what should be included when establishing a data sharing agreement. It was not possible during this review to establish if the organisation is using any of this guidance, or others to support the approach to data sharing.

In moving forward, it has been recognised that WMFS is currently developing a 'Governance Partnerships Framework' to include Data Sharing which will be linked to a toolkit for staff to use. This will seek to address the policy gap highlighted above.

Proposal 1

A data sharing policy and supporting principles of operation are required to guide the organisation. Members of the Community Safety team and the Data Management team are key stakeholders in Data Sharing as are staff in

Commands and partners. Stakeholder engagement is paramount when establishing the policy and principles of operation.

2.2   Central Governance of Data Sharing

Due to the lack of governance, which could be enabled through a policy, it cannot be determined as to the level that data sharing is taking place across the organisation, indicating a lack of cross organisational awareness of what data is being shared externally and internally. There was not a clear picture across the organisation of the level and type of data which is being shared both internally and externally and subsequently limited evidence to demonstrate a coordinated approach to data sharing.

In determining a way forward, a strategic decision needs to be made with regard to how to effectively govern and manage the data sharing activity and partnerships. Currently, there is no central control in place to routinely identify and provide assurance of:-

- Data sharing partnerships in place
- Whether such partnerships are aligned to the delivery of Organisational priorities
- What data is being shared
- Whether such data is being shared in a secure and 'safe' manner
- Whether there is an appropriate data sharing agreement in place and
- Whether the data sharing agreements are being applied effectively

The introduction of effective governance arrangements will provide assurance to the Organisation as to the quality of data sharing arrangements through an effective system of control. It will also enable for the ongoing evaluation and improvement of data sharing partnerships. This will promote a high quality and consistent level of delivery, the sharing of good practice which should provide the opportunity for improve outcomes across the West Midlands community.

Furthermore, effective governance arrangements will protect both the Organisation and its delivery teams through providing a transparent and auditable system, ensuring that data sharing is undertaken in a way which is legally compliant. This will, for example, reduce the risk of inappropriate data sharing agreements being put in place or data being incorrectly shared. This is important because significant financial penalties have been levied against Organisation's for the inappropriate sharing of data as a consequence of ineffective governance arrangements.

Proposal 2

A strategic decision should be made as to the structure and system requirements to enable for the effective governance of data sharing. Following this a complete audit throughout the organisation needs to be undertaken to determine the amount, type and purpose of the data that is being shared internally and externally. The audit would in addition need to determine the data sharing agreements that are currently in place.

2.3 Data Sharing Agreements

There are some data sharing agreements in place with external partners which ought to be shared with the Data Management function for review. Currently, it is the Organisational expectation that the Data Management department will approve data sharing agreements. This does not appear to be taking place as the norm. Anecdotal evidence exists that on occasion data sharing agreements have been signed off without the full involvement of Data Management.

Data Management hold a limited number of agreements, all of which are different in format and approach. Organisation's such as the '*Centre of Excellence for Information Sharing'* can provide a checklist of items to include in an agreement to simplify them. From discussions with stakeholders, it can take a considerable amount of time for Data Management to review these agreements as they are often lengthy. This is cited as a reason as to why this review and assurance function is not regularly used.

The Data Management function provides support in the formulation and/or review of agreements prior to the organisation signing up. This is a critical role given the potential impacts of data protection and management of information policies which are in place. Through not involving Data Management, there is a critical loss of internal expertise in developing or considering suitable data sharing agreements. Without a policy in place to guide data sharing the under use of the Data Management function even from an advisory perspective presents a risk to the organisation, as there is no control or consistency to the approach.

Proposal 3

A review of the template for the WMFS Data Sharing agreement needs to take place with a view to it being simplified.

2.4   Data being shared between WMFS and other agencies

Data sharing exists with a wide range of partner organisations, examples discussed with stakeholders are listed below:-

- Seven Local Authorities on social care
- Mental Health Trusts
- Hospitals – acute care
- GPs, District Nurses – primary care
- Third sector such as Age UK, Diabetes UK, Alzheimer's Society

The above examples demonstrate a wide range of organisations engaged in data sharing and potentially a wide range of data and information being shared. However, the ability to understand the full breadth of organisations engaged in data sharing and the types of agreements entered into and types of data being shared, is not facilitated through a policy or systematic approach to recording this information. It was acknowledged during the review that data sharing will exist at a local level which may not be part of a formal agreement or agreements entered into, without

clear steer regarding organisational expectations. Without a policy in place guiding staff in this activity, this presents an unclear picture of what information and data is currently being shared internally and externally. This presents a risk to the organisation and its partners. If WMFS are not aware of the full breadth of data being shared and the partners involved, it may not be able to put in place the measures to manage these effectively (management of information), It could also be entering agreements which do not align to organisational strategy and could present issues in the security of data.

Evidence suggests that data sharing takes place across other functions outside of Service Delivery, this is being managed at a local level without any coordination around the purpose of the sharing and how it is managed.

There is also anecdotal evidence to suggest that information around vulnerable individuals is shared verbally through meeting forums across partner agencies. This indicates a lack of awareness around guidelines for data sharing, data protection and the management of information for individuals. It could also be perceived to be a potential breach of data security. This is to be expected as a consequence of having no policy in place.

From the evidence set out in section *'2.1 Governance of data sharing',* highlighting the lack of an established policy and the unclear picture presented around the data being shared with other organisations, it can be assumed that data sharing is taking place in other areas outside of the above, of which WMFS are not centrally aware of, or coordinating using a policy.

Proposal 4

WMFS should identify a suitable approach for effectively managing and controlling data that is shared with partners. As part of this the role and responsibilities in respect of managing shared data should be determined.

2.5   Barriers to effective data sharing, internally and externally

At this point in time, the key barriers that have been identified relate to the requirement of an Organisational policy and operating principles. As part of this, the way partnerships are managed and identified through the effective provision of a suitable system needs to be established. This would be aligned to organisational expectations and be legally compliant.

More detailed barriers will become apparent when the policy and operating principles are developed and fully operational.

At this stage of the review it is not possible to determine what the external barriers are until a full picture is established on the level of data that is currently being shared.

3.6   ICT Systems supporting data sharing

There is no central ICT system in place aligned to a policy which supports the organisation and its staff in the management of data sharing approaches and agreements. From discussions which took place as part of this review it was established that there are currently different approaches to the management of data sharing across the organisation. Information is received and most likely sent out in different ways. For example, data shared by email, this is not always secured through password protection or has clear labelling or handling instructions. Clearly the communication of an effective policy and principles of operation would be helpful in identifying the critical factors in data sharing. The approach is too variable to provide a consistent and secure approach.

It became apparent that information is stored locally on spreadsheets, again it cannot be established if these are always password protected.

Due to the sporadic approach to storing data and the lack of a central approach there is a lack of appropriate access for individuals to enable them to carry out their roles effectively. An example of this is where the Commands each use different 'drives' to store data locally.

This also provides risks as to the security of the data of vulnerable individuals as it is not currently known who has access to this data. It may be the case that individuals are printing off information and carrying it around in paper format.

The ICT Systems supporting data sharing link into 'Proposal 4' as stated above.

3.7   Notable Good Practice Examples

During the review it became apparent that other Fire and Rescue Services have carried out immense work on the sharing of data.
- Avon Fire & Rescue Service
- Cheshire Fire & Rescue Service
- Dorset Fire & Rescue Service
- Merseyside Fire & Rescue Service
- Nottinghamshire Fire & Rescue Service
- South Yorkshire Fire & Rescue Service

Whilst there are no statutory guidelines around data sharing, there are several guiding documents issued through the Home Office and other government associations. These would support a simple approach to data sharing. There are also several good examples of data sharing across the public sector which would support WMFS in creating a governance structure for data sharing aligned to policies around data protection and management of information. For example, South Yorkshire Fire and Rescue have a detailed section on their website on how data will be shared. It also includes information on how to be removed from data that is held.

With the implementation of a policy and operating principles, the evaluation of Data Sharing could take place after the governance arrangements has been established.

Proposal 5

In developing the approach to data sharing, consideration to best practice should be considered and adopted if it is regarded to be appropriate to WMFS.

3.8   Impact on Corporate Risk

With the lack of a policy or operating principles there could be an impact on WMFS corporate risk, the brand and image of the organisation. The failure not to share data in accordance with organisational expectations and legislation could potentially expose the organisation to risk, specifically these are:-

Corporate Risk 3, Delivery of Services, Prevention
Risk 3.2

The Fire Authority is unable to establish effective partnership arrangements and deliver community outcomes, resulting in a significant impact upon the organisation's financial standing, reputation and ability to deliver key objectives.

Corporate Risk 7, Information, Communication and Technology
Risk 7.2

The Fire Authority is unable to provide effective management and security of organisational information and documentation including the receipt, storage, sharing and transfer of information and data, resulting in reputational damage, litigation, substantial fines and external scrutiny.

However, through addressing the proposals raised in this report, the organisation will be able to evidence that it has strengthened its control around these particular risks.

Subject to the approval of the Scrutiny Committee, the responsible officer, the Director for Service Delivery, will facilitate the production of a suitable timeline for the proposals set out in Appendix 3. An update on the accomplishment of the proposals will be periodically provided to the Scrutiny Committee.