

POLICY, PERFORMANCE & PROGRAMMES

Data Sharing Protocol Guidance

Establishing Protocols for the sharing of data between
South Yorkshire Fire and Rescue and its partners

Document Management No.	██████████
Author	██████
Date Written	July 2009
Date Ratified	
Date for Review	July 2010
Version No.	1



South Yorkshire
Fire & Rescue
WORKING FOR A SAFER
SOUTH YORKSHIRE

CONTENTS PAGE

Title	Page No
Introduction	1
Principles to be Adopted in the Sharing of Information.	2
Types of Data	3
Personal Data	3
Sensitive Data	3
Anonymised and Aggregated Data	4
Purpose of the Protocol	4
Roles and Responsibilities	4
Suppliers / Providers	4
Receivers of Data	4
Owner	5
Security	5
Issuing of Data	6
Data Formats	6
Confidentiality of Data	6
Data Quality	6
Data Audit	7
Requests for Personal or Sensitive Data	7
Changes to Protocols	7
Appendix A – SYFR Standard Data Sharing Agreement Form	8

INTRODUCTION

1. The aim of this document is to define how South Yorkshire Fire and Rescue (SYFR) should share data with outside bodies and partners. It will provide the basic principles to ensure SYFR is compliant with relevant legislation as well as its own policies and procedures. It will help to ensure the secure and legal management and processing of any data shared between SYFR and its partners. The principles of this document should be used as guidance where no formal data sharing agreement is in place or until one is agreed. This document is not itself a data sharing protocol as individual projects, initiatives, pieces of work or research should have a bespoke data sharing agreement drawn up between all the relevant parties that suit their requirements. This process can sometimes take a number of months to draw up and ratify as it is often necessary to scope the exact requirements and establish the necessary approval from the relevant responsible officers. Other organisations may draw up a protocol and SYFR may only need to sign up to this or agree it is fit for purpose. In the absence of any protocol or agreement a template document has been supplied in Appendix A.

2. The three main pieces of legislation that govern data sharing are:
 - [Freedom of Information Act 2000 \(FOI\)](#)
 - [Data Protection Act 1998 \(DPA\)](#)
 - [Human Rights Act 1998 \(HRA\)](#)

3. Other useful references and guidance documents are available on the following websites:
 - [The Ministry of Justice](#)
 - [Information Commissioner's Office](#)

4. This guidance sets out the responsibilities for each involved party to ensure all processing of shared data is accurate, necessary, legal and ethical. Any data shared or issued by SYFR employees should be carried out in accordance with existing SYFR policies and procedures, namely;
 - [SYFR Security Policy](#)

- [Data Protection Policy](#)
- [Freedom of Information Guidance](#)
- [Data Quality Strategy](#)

5. These documents are available on the intranet and form the basis on which a SYFR employee should act when dealing with data and any data sharing activities. Where necessary a Data Sharing Protocol (DSP) should be developed and established between all parties that wish to share data and information.

PRINCIPLES TO BE ADOPTED IN THE SHARING OF INFORMATION.

6. The aim of any DSP is to define how data should be treated between organisations. These protocols provide a way to help organisations to understand and comply with their legal obligations; they are often bespoke documents and can become very complicated.

7. The DSP should form an agreement between the parties and should contain the following as a minimum:-

- The types of data to be shared.
- The purpose of the agreement.
- Which organisations formed part of the agreement; their roles and responsibilities.
- The condition of use of the data provided, both before and after it's been initially supplied.
- The security of the data.
- Format of the data.
- Signatories from the partners

8. Other considerations maybe:-

- The length of time the agreement will may remain valid, or how often it should be reviewed.
- Period or time limits on the retention of the data.
- The risks around the use of the data – especially if it is amalgamated with other data.

9. Partners should satisfy themselves that any DSPs are compliant with their statutory duties and legislation. Personal and personally identifiable information will only be disclosed when the purpose of the DSP requires this disclosure and it satisfies the exemptions in the Data Protection Act (Section 33).

TYPES OF DATA

10. For the purpose of this guidance there are essentially three types of data. These are Personal data, Sensitive data, Anonymised and Aggregated Data. Wherever possible anonymised or aggregated data should be used. Explanations of each are given below.

PERSONAL DATA

11. The Data Protection Act 1998 applies only to personal data about a living, identifiable individual. However the definition of personal data is highly complex and for day to day purposes it is best to assume that all information about a living, identifiable individual is personal data.
12. Such personal data might include, but not be limited to:
- Name
 - Address
 - Telephone Number
 - Age
 - A unique reference number if that number can be linked to other information which identifies the data subject, such as a National Insurance Number or Payroll number.
13. The law imposes obligations and restrictions on the way the SYFR and its partners process personal data. The DPA regards 'processing' of data to include collecting, storing, amending and disclosing data. The individual who is the subject of the data (the "data subject") has the right to know who holds their data and how such data will be processed, including how such data is to be or has been shared.

SENSITIVE DATA

14. In the DPA certain types of data is referred to as "sensitive personal data". This is data which relates to the data subject's:
- Racial or ethnic origin
 - Political opinions
 - Religious beliefs, or other beliefs of a similar nature
 - Trade union membership
 - Physical or mental health or condition
 - Sexual life
 - Commission or alleged commission of any offence (the term 'Malicious' for example)
 - Any proceedings for any offence committed, or alleged to have been committed.

Usually more stringent restrictions will apply the use of this sensitive personal data.

ANONYMISED AND AGGREGATED DATA

15. The use of anonymised and aggregated data can be treated in very similar ways. Anonymised data are individual data records from which the personally identifiable fields have been removed.
16. Aggregated data is data which has been processed to produce a generalised result, and from which individuals cannot be identified. However caution needs to be taken when such aggregations could lead to an individual being identified e.g. Groupings with small distribution leading to isolation of individual characteristics.
17. On the basis that anonymised and aggregated data does not identify individuals, the processing of such data is not regulated by the DPA.

PURPOSE OF THE PROTOCOL

18. The purpose of the protocol should be clearly stated and be as simple as possible without being too open or overly restrictive. These statements form the boundaries within which the shared data can be used. All parties should be in agreement before any protocol and agreement is signed. If a partner wishes to change the usage defined in the DSP then ideally a new agreement should be entered into.

ROLES AND RESPONSIBILITIES

19. Each organisation or partner should be clearly identified, and where possible, their roles or parts they play within the protocol, the names of individuals, their section or department and their addresses should be stated.

SUPPLIERS / PROVIDERS

20. Suppliers are any organisation, body or individual that supplies data to another body. These could include, but are not necessarily limited to, SYFR, Local Authorities, Primary Care Trust, the Police, members of the public, private organisation, Universities and educational establishments. Suppliers should establish what the data is to be used for and must agree that it can be used for the purpose defined in any agreement before releasing it.

RECEIVERS OF DATA

21. Any organisations or partner entering into a DSP should be aware of their responsibilities as to the use and security of the data provided to them. They should

be aware that there is a possibility of prosecution if the data is used in any other ways than its intended use. However it should be noted that under section 33 of the DPA, data can be used for purposes other than its original use. The most likely reason for any exemption would be if the data is to be used for research.

OWNER

22. If applicable there may be a need to state who owns the data if it's to be amalgamated with any other data.

SECURITY

23. Regardless of the type of data being processed and stored, the issue of security should be considered as of the utmost importance. Reasonable measures should be taken to reduce the risk of any security issues arising.
24. All data that is held by SYFR should be on secure servers or secure locations, with access restricted to internal use by selected members of staff.
25. It is understood that each provider/suppliers will have differing security needs, however it is important that all reasonable steps are made to ensure data is kept private and confidential at all times.
26. In particular all partners must take appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss, destruction, or damage to personal data.
27. This will include:
- Appropriate technological security measures, having regard to the state of technology available and the cost of implementing such technology, and the nature of the data being protected
 - Secure physical storage, and where possible limitation in the use of portable storage devices or media.
 - Password protected computer systems
 - Restricted access to data and taking reasonable steps to ensure the reliability of employees who have access to data
 - Appropriate security on external routes into the organisation, for example Internet firewalls and secured dial-in facilities.
28. Partners are of course themselves responsible for complying with the DPA, irrespective of the specific terms of stated with any agreement or protocol. Any agreements must be in alignment with SYFR Security Policy.

ISSUING OF DATA

29. Partners should give consideration as to how the data is to be exchanged. This should be assessed against any potential security risks, current policies or legislative requirements. For example, data should only be sent to an individual as set out in the DSP, sending items to group email address is not best practice and sending items to third parties outside the DSP should not take place.

DATA FORMATS

30. To provide a consistent approach when exchanging data an agreed format should be stated. The format will depend on the exactly what the data consists of, but where possible should be a recognised standard.

CONFIDENTIALITY OF DATA

31. All personal data should be treated with the utmost confidentiality, and will only be shared by SYFR with those organisations which can demonstrate a professional or legal requirement for having access. No SYFR data should be used outside the service for commercial gain or advantage without the prior agreement of SYFR.

DATA QUALITY

32. When entering into any data sharing agreement consideration should be given to the quality of the data. The principles of data quality are outlined in SYFR Data Quality Strategy. Data quality means producing information that is 'fit for purpose' on a 'right first time' basis. In order to achieve this there are a number of principles that underpin good quality data that need to be adhered to. Failure to work to these standards introduces the possibility of inaccuracies and poor data quality with the potential knock on effect of flawed decision making. These standards are:
- Validity and Relevance - the correctness and reasonableness of data and ensuring it is appropriate to the purpose of the performance measure it has been selected for;
 - Completeness - there are controls over input, especially that information is input on an ongoing basis rather than being entered at a later date;
 - Consistency and reliability - data should be internally consistent with the aim of being accurate 100% of the time;
 - Accuracy - there are verification procedures in place as close to the point of input as possible.
 - Timeliness - data should be timely and up to date.

- R elevance – Appropriate use o f t he dat a, i s it f it for pur pose and i t's applicable

33. Before entering into any agreement SYFR must be satisfied that the above criteria are met to the highest possible standard. When data is supplied to SYFR it is critical that we have an understanding of the supplier's policies and controls when dealing with data quality.

DATA AUDIT

34. All data stored, processed and/ or passing through SYFR should be tracked and recorded. This provides an audit trail of where data has come from and where it is going. This can be achieved by the use of 'Data Sharing Register'
35. It is expected that providers/suppliers will also be able to provide robust audit trails for all data they hold that is considered personal or sensitive.
36. Any DSP should be logged within SYFR's systems and where possible electronically signed copies should be obtained, a copy of which should forward to the Data Management Section in Policy, Performance & Programmes (CHQ) where a central register has been established.

REQUESTS FOR PERSONAL OR SENSITIVE DATA

37. Sensitive and personal data will not normally be passed to organisations outside SYFR, except where an organisation may have a legal and legitimate reason for access and a requirement for the data in order to carry out its function. For instance, law enforcement, prosecution, child protection.
38. Organisations wishing to have access to named, sensitive or personal data must either offer a suitable DSP which SYFR are willing to sign up to or sign up to SYFR data sharing protocol template before any data is released.

CHANGES TO PROTOCOLS

39. It is recommended that all protocols are reviewed on a regular basis. Each DSP should state when the agreement commences, where possible a duration should be stated and when the agreement is to be reviewed.
40. Should changes be made, each organisation affected will be informed of the changes and be given time to comment before any changes take effect. If necessary a new DSP should be drawn up.

Appendix A - **SOUTH YORKSHIRE FIRE AND RESCUE**

STANDARD DATA SHARING AGREEMENT FORM

- Issue 1.0

Expand sections as necessary.

1. AGREEMENT TYPE	Tick Box	Timescales
A Non Personal Data		Agreement Start Date
B Sensitive Data		Agreement Duration
C Personal Data (with DPA Section 33 exemption)		Review Frequency

2. DATA SHARING PURPOSE STATEMENT

3. DATA OWNERSHIP and Parties to the Agreement
Give names and addresses of legal entities

3.1 Provider of Source Data	3.2 Receiver of Data	3.3 Owner of Resulting Data (If applicable)
-----------------------------	----------------------	--

4. CONDITIONS ON USE OF SUPPLIED DATA
Commercial use is prohibited unless specifically stated here

5. CONDITIONS ON USE OF RESULTING DATA
Commercial use is prohibited unless specifically stated here

6. MEASURES TO ENSURE SECURITY OF SUPPLIED DATA
During transfer, processing and disposal

7. RETENTION PERIOD FOR SUPPLIED DATA:

8. FORMAT OF SUPPLIED DATA

9. OTHER CONDITIONS / RISK IDENTIFIED

10. DECLARATION OF AGREEMENT & PARTICIPATION
We agree to supply and use data in accordance with the conditions listed above to absolve the other party from loss and liability in the event of us being in default of this agreement.

SIGNATURE		
NAME		
POSITION		
ORGANISATION		
DATE		