Data Sharing Agreement

Agreement for Sharing Data Between Partners of the Warwickshire Direct Partnership

Version 0.4
August 2008

Contents

1 Introduction and Overview

The aim of this agreement is to define how personal and sensitive data will be provided to the Warwickshire Direct Partnership (WDP) and the methods used by the WDP for the secure and legal management, accessing and processing of that data.

This document is one of a number of documents that combine to provide guidelines and rules covering all aspects of data sharing and management between the WDP and its partners.

In writing this agreement due attention has been paid to the views of partners where possible, and all the guidance has been written taking into account relevant legislation where applicable, including:

- Data Protection Act 1998
- Human Rights Act 1998
- Disability Discrimination Act 1995

and the local Warwickshire Information Charter agreed by the Public Service Board of the Local Area Agreement.

Disclosure of information is also subject to the Freedom of Information Act 2000.

A Data Sharing Guidance note and Confidentiality Guidelines also exist, which have been included in Appendices of this document. Together these documents form the basis on which all partners access and share data with the WDP. It also sets out the responsibilities for partners on how the WDP will manage the access and processing of data, to ensure that accessing and / or processing of shared data is accurate, necessary, legal and ethical.

Questions relating to any of these documents may be directed to any of the partner authorities listed in the Contacts Section in Appendix A.

1.1 Warwickshire Direct Partnership

The existence of the WDP is to:

Provide services to its citizens and customers in the most effective and efficient way. In order to do this the WDP collects data from customers and businesses, and use this data for a variety of information and service delivery functions including planning and research activities.

The data collected by the WDP, as defined by the Data Protection Act 1998 (DPA), contains both personal and sensitive data. The WDP therefore has developed guidance and agreements for partners that access the data which it holds, to ensure that they acknowledge their legal responsibilities in using and processing such data.

The WDP have identified that the categories of both personal and sensitive data as defined in the DPA fall into a number of classifications in terms of use by the partnership, and that the risks surrounding the different uses of the data requires further clarification of the DPA definitions.

2 Types of Data

For the purposes of this set of documents there are essentially three classes of data as defined by the Act itself listed below:

2.1 Anonymised and Aggregated Data

Anonymised data are individual data records from which the personally identifiable fields have been removed. It should be noted that where the WDP removes name and address information, fields such as date-of-birth, post code and qualifications are not removed, due to the nature of research undertaken, but such data will still be "anonymised" ensuring that the data subject's identity is not discernable from such data.

Aggregated data are data which are processed to produce a generalised result, and from which individuals cannot be identified. This might include data brought together to give a broad understanding of e.g., ethnicity distribution.

There is sometimes a slight risk that aggregated data might still allow an individual to be identified, for example by the results producing a very small group of results, from which other data may be used in identifying an individual, even though personal data has been removed.

2.2 Personal Data

In the DPA personal data are defined as:

"…data which relate to a living individual who can be identified

a) from those data, or

b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual."

Such personal data might include, but not be limited to:

- Name
- Address
- Telephone Number
- Date of Birth / Age
- Case history
- A unique reference number if that number can be linked to other information which identifies the data subject.

The law imposes obligations and restrictions on the way the WDP and its partners process personal data (in this context processing includes collecting, storing, amending and disclosing data), and 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 are or will be processed, including how such data are to be shared.

2.3 Sensitive Data

In the DPA certain types of data are referred to as “sensitive personal data”. These are data which relate 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
- Any proceedings for any offence committed, or alleged to have been committed.

Additional and more stringent obligations and restrictions apply to the WDP and its partners whenever we process sensitive personal data.

3 Data Management

3.1 Uses of Data

Whilst the DPA has defined these three classes of data, some categories within these classifications will have different levels of risk associated with them and WDP has therefore, defined sub-categories of the classes based on intended use and the risk associated with those sub-categories.

3.1.1 Unrestricted Data

This category relates to provision of information or services that do not require partners to know anything about the individual making the contact.

This category also includes anonymised and aggregated data that may be used for segmentation or research purposes. To safeguard data subjects and to manage the risk associated with this type of data, **aggregated data which comprise less than five individual records should not be used or disclosed without senior management approval**, unless such aggregated data can in no way be matched to identify individual data subjects.

On the basis that anonymised and aggregated data do not identify individual data subjects, the processing of such data is not regulated by the DPA. The WDP takes the view however, that controls over the processing and disclosure of non-identifying data should be implemented nevertheless.

3.1.2 Restricted Data

This category covers both personal and sensitive data and seeks to clarify which sub-categories of data require additional measure or controls in their use.

WDP’s approach is that some sub-categories of Personal data can be used by the partnership with a low risk of injury to the data subject, and significant benefits in terms of service delivery.

The sub-categories of this data would include:

- name
- address
- telephone number
- email addresses
- Case history (do we mean high level history of all services and not case detail?)
- A unique reference number if that number can be linked to other information which identifies the data subject.

Access and processing of this data carries little risk where good information management practices are upheld and may be used widely for access and processing.

The sub-categories where additional measures will be required are:

- Date of Birth / Age
- Racial or ethnic origin
- Political opinions
- Religious beliefs, or other beliefs of a similar nature
- Trade union membership

This information may be required for individual services or for aggregating in surveys or segmentation exercises. However, there is an increased potential risk of injury to the data subject with these subcategories and less obvious benefits. If this data is to be held in the CRM system, permission for this should be obtained from the data subject.

The remaining sub-categories have a high level of risk attached to them and accessing or processing of this information will be restricted to only those with the required permissions. Accordingly, the WDP attaches even greater than normal importance to these sensitive personal data and any processing of sensitive personal data may only take place in an anonymised format or by persons duly authorised to access such data. These final sub-categories include:

- Physical or mental health or condition
- Sexual life
- Commission or alleged commission of any offence
- Any proceedings for any offence committed, or alleged to have been committed

3.2 Data Control

Under the DPA, any organisation which "determines the purposes for which and manner in which any personal data are, or are to be, processed" is called a "data controller". All data controllers are required to comply with the DPA whenever they process personal data (bearing in mind, as stated above, that "processing" includes collecting, storing, amending and disclosing data). At all times, when providing data to partners, the partner responsible for delivering a service will be considered the data controller, as opposed to the partner who may be the first point of contact. Partner organisations which receive data from that responsible delivery authority are considered to be "data processors" i.e., processing those data "on behalf of" the delivery partner. As a data processor, partners must at all times process data solely in accordance with the WDP's instructions and comply with the security obligations set out in section 4.

3.3 Data Protection Registration/Notification

All organisations that manage, access, process and/or share personal data must be registered with the Information Commissioner's Office (ICO).

Any partner recording personal data for the WDP must be registered with the ICO. It is a criminal offence to process (which includes sharing) personal data in a manner which is inconsistent with your registration. Details of the categories of information partners have signed up for are explained below.

The notification section of the Information Commissioner's website:

http://www.informationcommissioner.gov.uk contains more information on how to notify, including a downloadable handbook, which covers all the requirements of notification.

Registration should be done directly with the Information Commissioner via the above website address, and not through an agent, which may incorrectly register a client, and which will likely charge in excess of the Information Commissioner's registration fee (currently £35).

A telephone help line is available from the Information Commissioner's Office for any queries relating to the notification process. This number is 01625 545740.

Again it is up to the Partners when registering to ensure that all purposes, classes and sub-sections are correctly notified.

The processing of personal data in a manner which is inconsistent with your registration is a criminal offence.

4 Security

Regardless of the type of data being accessed, processed and stored, security is considered of paramount importance.

All data that are held by the WDP are held on secure servers, with access restricted to internal use by appropriate members of staff.

As data controllers for the data they collect, all Partners are expected to treat named data in accordance with the DPA, and ensure that security is in place sufficient to protect the data from unauthorised access.

This includes physical security, such as adequate protection for premises when unattended, to IT related security such as passwords and secure IDs.

It is understood that each partner may 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. Each partner is expected to comply with its Information Security Policy and to make staff aware of their obligations in this respect. All partners are also expected to comply with the standard requirements in the Code of Conduct for Government Connect.

In particular all partners must take appropriate technical and organisational measures against unauthorised or unlawful accessing and / or processing of personal data and against accidental loss or destruction of, or damage to, personal data.

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 management of non-electronic data
- Password protected computer systems
- Restricted access to data and taking reasonable steps to ensure the reliability of employees who have access to sensitive data
- Ensuring data is only held as long as is necessary, in line with Data Protection principles
- Appropriate security on external routes into the organisation, for example Internet firewalls and secure dial-in facilities.

Partners are themselves responsible for complying with security in respect of the DPA, irrespective of the specific terms of this agreement.

If there is a requirement for WDP to supply data to any external body, full records will be kept of when data is supplied by the WDP to external and other governmental organisations.

4.1 Issuing of Data

Partners are expected to issue data only to data subjects who comply with the required procedure or those organisations which have a legitimate right to view and process that data. In accordance with the standard declaration (Appendix C), the WDP will not make named data available for commercial use.

4.2 Storage of Data

Data recorded by Partners are stored in a secure, purpose built database, access to the raw data is on a restricted basis, and all processing done on the data within the WDP requires authorisation from the team responsible for managing the data.

4.3 Confidentiality of Data

All personal data is treated with the utmost confidentiality, and shared by the WDP only with those organisations which can demonstrate a professional or legal requirement for having access.

5 Data Audit

5.1 Audit

All data stored, processed and/or passing through the WDP, is tracked and recorded. This provides an audit trail of where data has come from and where it is going.

It is expected that Partners will also be able to provide robust audit trails for all data they hold that is considered personal or sensitive.

6 Requests about Personal or Sensitive Data held

6.1 Subject Access Requests

Under the Data Protection and Freedom of Information Acts, customers can ask to see the information that is held on computer and in some paper records about them. This is called a Subject Access Request. If customers wish to know what information is held about them, requests must be put in writing to the organisation processing the data. Further contact information on the appropriate officers can be found in the Fair Processing Notice.

6.2 Complaints

Complaints about personal or sensitive information held by the partnership must be made in writing to the person or organisation holding this information, detailing the reasons for the complaint. Further contact information on the appropriate officers can be found in the Fair Processing Notice.

6.3 External organisations

Sensitive and personal data are not passed to organisations outside the WDP, 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.

Organisations wishing to have access to named data must first sign up to the WDP's data sharing agreement for personal and sensitive data, submit a request as to which data elements are required and justify their request for access.

This request will then be considered by the WDP, and access to the data either granted or denied.

Personal and sensitive data are not shared unless the need is totally justified, the WDP believes the requesting organisation to be fully aware of their obligations under all relevant legislation, and the organisation has agreed to be bound by the agreement for the sharing of such data.

7 Changes to Agreements

This agreement will be reviewed periodically and consequently it may be subject to change. This agreement will be available on-line and in the public domain. On changing an agreement, the new publication will be provided on the WDP partner web sites.

Appendix A - Data Sharing Guidance for Staff

Warwickshire Direct Partnership
Data Sharing Guidance

This document is intended to ensure that personnel working for and on behalf of the Warwickshire Direct Partnership (WDP) understand the importance of good practice when dealing with personal and sensitive personal data held in customer records, and appreciate the rules by which individuals' data may be accessed and processed.

Whilst the guidelines are written for internal use, they will be available for viewing by the public on the WDP partners' web sites.

The following items represent the Data Sharing Guidelines of the WDP, with respect to personal and sensitive personal data:

1. Data held by the WDP will be treated as confidential at all times.
2. Data held by the WDP will be processed in accordance with the DPA, and internally produced agreements.
3. Individuals have the right of access to information about them. (Refer to Data Protection section for more details).
4. Personal data will be made available to the data subject provided the data subject satisfies the request requirements of the DPA.
5. Data will only be held that are needed in order for the WDP to perform and fulfil its statutory and business obligations.
6. The uses, to which personal and sensitive data may be put, are detailed in the Data Sharing Agreement and can be found in the data sharing agreement on partner websites.
7. Data will not be made available to third parties for commercial or marketing purposes. Data will only be shared with organisations that have a legal requirement to access such data in order to fulfil their statutory requirements. Organisations using any type of data held by the WDP will have to sign up to a data sharing agreement and be bound by the requirements of that agreement.
8. Data used for surveys will be subject to processing agreements.
9. All documentation that relates to the management of data will be made publicly available.

Periodically, this policy will be subject to review and change. Any changes to this policy will be published on the WDP partners' web sites, and up-to-date copies of the policy will be available via the Data Protection Officers.

Appendix C - Confidentiality and Release Guidelines

Warwickshire Direct Partnership
Confidentiality and Release Guidelines for
Personal and Sensitive Data

Introduction

This document provides advice on the release of personal data to third party organisations, and guidelines for the process by which the decision whether or not to disclose will be made.

Data is collected about customers and businesses. The data is brought together to form a single database of information, which is used by the Warwickshire Direct Partnership (WDP) and may also be shared with other government and statutory bodies.

Data Protection Act 1998

The WDP has notified the Information Commissioner's Office of the purposes for which it intends to process personal data.

Under the terms of the DPA, individuals have a right of access to any information held about them. Requests by individuals, of this nature should be directed to the Data Protection Officer of one of the partner authorities.

Principles of Confidentiality

There are a number of principles that apply to the confidentiality and release of data, and which should always be adhered to:

- Data identifying individuals, whosoever they may be, are regarded as confidential.
- Data of any kind will only be shared with organisations which have equivalent data protection policies and guidelines, or who have signed up to the relevant WDP data sharing agreement.
- Personal data will only be shared in accordance with these guidelines.
- Anonymised or aggregated data, which produces publishable results of less than five individuals, will only be published with the agreement of senior WDP management and legal teams.
- An individual has the right to request copies of data that are held by the WDP, and the WDP partners will endeavour to supply this information at the earliest opportunity.

Release Guidelines

Personal and Sensitive Data

Personal data held by the WDP may be released to individuals and other organisations under certain conditions. These include:

- Internal staff who require access to the data, in order to perform their duties

- External staff, working within the WDP partner offices, such as consultants who are working under contract to the WDP or its partners and require access to personal or sensitive personal data in order to perform their duties.
- External Organisations contracted by the WDP, including consultants and researchers that need access to personal and sensitive personal data in order to carry out their contracted obligations, subject to their acceptance and agreement of all relevant WDP data sharing agreements.
- Governmental and statutory organisations that require access to such data in order to perform statutory or public functions. Agreement to the WDP's data sharing agreements may be a requirement under certain conditions.
- Whilst aggregated data are provided to organisations that have agreed to be bound by certain data sharing conditions, the WDP will not release any aggregated data that contains groups of fewer than five individuals **without senior management approval**. In any event the WDP expects external organisations performing analysis on data to refer back to the WDP if their analysis produces aggregated data containing groups of less than five individuals.

Crime Prevention

The WDP partners are registered individually with the ICO for the purposes of crime prevention. If required the WDP will allow data matching processes across its database in order to detect fraud, or identify other criminal activities.

This authority will only be used where the WDP believes it has reasonable grounds for taking such action, or a third party can provide reasonable grounds for justifying such action by the WDP.

External Organisations Working on Behalf of WDP

Occasionally the WDP or its partners will employ an external agency to do research or analysis work on its behalf. In these cases, information supplied to the third party will be supplied subject to a processing agreement, and the relevant data sharing agreement if appropriate.

Summary

At all times data that are held by the WDP will be treated in accordance with these guidelines, the data agreement and guidelines published by the WDP, and the DPA.

Appendix D – Declaration of Acceptance and Participation (for Partners)

On behalf of the organisation specified below, I agree to the provision and management of data in accordance with the conditions laid out in the “Agreement for the Sharing of Data between Partners of the Warwickshire Direct Partnership”.

I declare that we have given notification to the Information Commissioner and registered the purposes for which the organisation may process and manage data, and that the registration is up-to-date and complete.

Signed…….. Date …….

Name…….

Position…….

Organisation …….

Address…….

…….

…….

Postcode……

Telephone……

Data Protection Registration No.*…….

Please send this page to your local Data Protection Officer.