



Data Sharing Protocol

Contents

Introduction	4
Definitions	4
West Norfolk Strategy	5
Data Sharing Vision	5
Aims and Objectives of Data Sharing	5
The 'Dawn' Data Observatory	6
Scope	6
General Principles	8
The Legal Framework	8
Site Administration	8
Partnership Responsibilities	9
Organisational Responsibilities	9
Individual Responsibilities	9
Review Arrangements	10
Appendix A: Relevant Legislation	11
Appendix B: Metadata	14
Appendix C: Dawn data observatory - applications	15
Appendix D: Dawn Technical Support Group	16
Appendix E: Glossary of Terms	17

Introduction

1. This document has been developed by the West Norfolk Partnership to facilitate the sharing of information amongst key organisations through Dawn, data about West Norfolk.
2. The aim of this protocol is to facilitate sharing of information between the public, private and voluntary sectors to strengthen the Partnership's evidence base. This will help ensure that appropriate services are provided and discretionary resources are allocated on the basis of need.
3. This protocol is designed to support the West Norfolk Partnership's move towards evidence-based prioritisation and allocation of resources. This is facilitated by the development of an on-line information service that allows partners in West Norfolk to pool and share data, information and intelligence
4. It is intended to provide a consistent framework and common standard for organisations to sign up to. By accepting this protocol an organisation shows its desire to share information in a lawful and controlled way with other organisations that also accept the protocol.

Definitions

5. Data can be defined as individual measurements; facts, figures, pieces of information, statistics, either historical or derived by calculation, experimentation, surveys, etc.; evidence from which conclusions can be drawn and intelligence gained.
6. There are a number of standards that underpin good quality data. Failure to work to these standards introduces the possibility of inaccuracies and poor data quality. These standards are:
 - **Awareness and Responsibilities:** everyone recognises the need for good data quality and is aware of their responsibilities;
 - **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:** 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.

West Norfolk Strategy

7. The Partnership's sustainable community strategy encapsulates its aspirations for West Norfolk. Central to the shared effort to achieve this vision and improve quality of life in West Norfolk is the work of key public, private, voluntary and community sector organisations. These organisations come together under the auspices of the West Norfolk Partnership to co-ordinate this effort and

"achieve more together than we can on our own through collaboration, co-ordination and commitment - making life better for people in West Norfolk."
8. The Partnership does this through a cycle of:
 - a. developing a shared, long-term vision for the area
 - b. using a robust evidence-base to define the required outcomes
 - c. developing and implementing project / action plans
 - d. using the baseline evidence to track improvements and enable monitoring against outcomes and performance management ('turning the curve')
 - e. structuring and supporting partnership working to achieve its ambitions

Data Sharing Vision

9. The West Norfolk Partnership has established an on-line data observatory, 'Dawn', to facilitate the sharing of information. The partnership's vision for data sharing is that:

"Partners routinely share quality data and information to provide intelligence underpinning the issues facing West Norfolk and to ensure that policy, priorities and decisions are based on clear evidence. Dawn is recognised as the first point of call for any organisation or individual wanting to find out data and information about West Norfolk, and is the primary mechanism through which agencies publish or share data and information about West Norfolk."

Aims and Objectives of Data Sharing

10. Sharing data across and between partner agencies will help the partnership achieve its data-sharing objectives:
 - a. support the provision of quality local evidence at appropriate levels of geography
 - b. support evidence-led policy formulation
 - c. inform the Partnership's lobbying on key issues
 - d. promote the importance of data sharing
11. The aims are to
 - a. improve the quality and robustness of decision-making
 - b. inform the allocation of resources
 - c. inform business planning
 - d. support applications for funding
 - e. inform the promotion and marketing of West Norfolk
 - f. provide public access to nationally-available data

- g. provide a mechanism for sharing locally-available data amongst partners
- h. facilitate the analysis and correlation of different data sets
- i. inform the performance management and benchmarking of partnership activity
- j. promote the use of Dawn in local schools

The 'Dawn' Data Observatory

- 12. The Dawn data observatory is a Partnership resource. It provides interactive access to a wide range of information on the district and its local communities. The system is owned by the West Norfolk Partnership and its development overseen by one of the Partnership's technical support teams. This team reports to and is performance managed by the Partnership's Management Group.
- 13. All partners will be expected to promote Dawn to their staff and encourage data sharing as appropriate. This will be supported by the production of appropriate guidelines where required that will be made available to all staff via the Partnership website.
- 14. Contact details for members of the Partnership's data and information technical support group are provided at Appendix E. For access to the system, visit www.visitdawn.com and contact the named site administrator for log-on details.
- 15. The functionality provided by the Dawn data observatory is summarised in Appendix D. This includes the ability to upload local datasets. These should be provided to the site administrator together with provision of 'meta data' – data about the data which provides users with assurances as to its robustness. See the notes at Appendix C for further information.

Scope

- 16. This overarching protocol sets out the principles that all people working for or with the partner organisations should follow when using and sharing information between organisations.
- 17. The protocol applies to the following three data sharing situations:
 - 17.1 **Non-personal data** (which does not relate to individuals) e.g. information on organisations, performance, natural resources, projects etc. This is the bulk of the information on the Dawn data observatory.
 - 17.2 **Personal data** (data about individuals who can be identified from that data, either directly or through the pooling of other information) e.g. all personal information processed by the organisations including electronic (e.g. computer systems, CCTV etc), or in manual records.

Personal data is specifically covered by the Data Protection Act 1998 (DPA), which imposes a number of obligations and duties on those who hold such data and gives rights to individuals to know what data is held about them. The Act also has different provisions for **personal data** (e.g. address, demographics, education, financial status) and **sensitive**

personal data (e.g. religious & political beliefs, racial / ethnic origin, trade union membership, health and sexual behaviour, offences).

To reiterate, personal data is not held within Dawn.

In relation to this protocol the DPA provides some exemptions for data used for the purpose of research (including statistical or historical purposes). These are given in Section 33 of the Act and allow:

✚ Personal data to be used for research, even if this was not obtained for this purpose.

✚ Personal data used for research to be kept indefinitely.

Only the sharing of personal data for research purposes (i.e. where a DPA Section 33 exemption applies) is covered by this protocol.

17.3 **De-personalised data** is aggregated or anonymised data that describes individuals, but where identification of the individual is not possible by the organisations using the data, either from the data or in conjunction with other data or information they hold or are likely to acquire.

Anonymised data about an individual can be shared without consent (subject to certain restrictions regarding health/social care records), in a form where the identity of the individual cannot be recognised. Anonymising data does not remove the duty of confidence.

18. Both non-personal and de-personalised data are outside the scope of the DPA.
19. This protocol is intended to meet general information sharing needs, where the consequences of parties failing to meet their obligations are not considered excessively damaging. Typically this would be situations where the legal constraints are based primarily on the Data Protection Act 1998 and the Freedom of Information Act 2000 and where the financial or practical risks of non-compliance are manageable. In situations where these conditions are not met the use of specialist protocols or other legal arrangements should be used.
20. This protocol has been designed for situations where the purpose of the information sharing is *not* to make decisions about individuals. These will be covered by specific protocols designed for the purpose.
21. This protocol typically covers data where the subjects are not living individuals, or where the purpose of the data sharing is analysis or decision making about general situations and the facts about any individual in isolation are immaterial.
22. This covers the very large and important activity of analysis of information about individuals for the purpose of policy formulation or management planning, but which is often hampered by misunderstanding of the legal framework and uncertainty about the controls that can be applied to the sharing process.

23. This protocol deals effectively with these concerns and allows all parties involved to have trust and confidence in their partner's ability to give and receive data.

General Principles

24. The principles outlined in this protocol are recommended good standards of practice or legal requirements that should be adhered to by all partner organisations.
25. This protocol sets the core standards applicable to all partner organisations and should form the basis of all data sharing agreements established to secure the flow of information.
26. This protocol should be used in conjunction with local service level agreements, contracts or any other formal agreements that exist between partner organisations.
26. All parties signed up to this protocol are responsible for ensuring that organisational measures are in place to protect the security and integrity of information and that their staff are properly trained to understand their responsibilities and comply with the law.

The Legal Framework

27. The principal legislation concerning the protection and use of personal information is listed below and further explained in Appendix A:
- ✚ Human Rights Act 1998 (Article 8)
 - ✚ The Freedom of Information Act 2000
 - ✚ Data Protection Act 1998
 - ✚ The Common Law Duty of Confidence
28. Other legislation may be relevant when sharing specific information.

Site Administration

29. Dawn contains data at both a national and local level. The partnership is committed to making both types of information as widely available as possible, whilst maintaining suitable controls. Access to the site will be administered via user log in and password and will be available to users as the table below shows.

Users	National Data	Local Data
Public	✓	x
Business	✓	x
Partners	✓	✓
Schools/ Colleges	✓	✓
Media	✓	✓

Partnership Responsibilities

31. All parties signed-up to this protocol:
- + Recognise the importance of sharing information with each-other in line with the aims of the Partnership and in order to achieve the Partnership's stated priorities.
 - + Undertake to co-operate fully with each-other, within the parameters of relevant legislation and any associated guidance.
 - + Pledge that all personal data remains the property of the disclosing agency, and is the responsibility of the data controller, as defined by the Data Protection Act 1998.
 - + Agree that the partner receiving the data will not use it for any purpose other than that set-out in this protocol, nor share it with any other party, without the disclosing partner's written permission.
 - + Will nominate a lead officer to act as a contact within that organisation for the Dawn data observatory technical support group.

Organisational Responsibilities

32. Each partner organisation is responsible for:
- + Ensuring that their organisational and security measures protect the lawful use of information shared under this protocol.
 - + Accepting the security levels on supplied information and handle the information accordingly.
 - + Accepting responsibility for independently or jointly auditing compliance with the data sharing agreements in which they are involved within reasonable time-scales.
 - + Ensuring that their contracts with external service providers abide by their rules and policies in relation to the protection and use of confidential information.
 - + Notifying the partner organisation originally supplying the information of any breach of confidentiality, or incident involving a risk or breach of the security of information.

Individual Responsibilities

33. Every individual working for the organisations listed in this protocol:
- + Is personally responsible for the safekeeping of any information they obtain, handle, use and disclose.
 - + Should know how to obtain, use and share information they legitimately need to do their job.
 - + Has an obligation to request proof of identity, or takes steps to validate the authorisation of another before disclosing any information.

- ✚ Should uphold the general principles of confidentiality, follow the rules laid down in this protocol and seek advice when necessary.
- ✚ Should be aware that any violation of privacy or breach of confidentiality is unlawful

DAWN Disclaimer

The West Norfolk Partnership intend Dawn to be the first point of call for statistics and facts about West Norfolk. By using Dawn you agree to adhere to the standards and guidelines set out in the data sharing protocols [link to doc]. In particular, users are reminded that Dawn only contains aggregated, anonymised data; that Dawn should be referenced whenever data is used or quoted (Source: visitdawn.com); and that care should be taken when interpreting or correlating data – it is always best to refer to the data owner listed in the metadata. Failure to follow these guidelines may result in access to the site being restricted. We would like to hear [email link] how you have used the data from Dawn so that we can continue to build the case for funding and further development of the site. We welcome your feedback and suggestions [email link]. Thank-you for your visit to Dawn.

Review Arrangements

34. This protocol will be formally reviewed bi-annually by the Dawn technical support group and the Partnership's Management Group, unless new or revised legislation or national guidance necessitates an earlier review.
35. Any member of the Management Group can request an extraordinary review at any time where a joint discussion or decision is necessary to address local service developments.

Appendix A: Relevant Legislation

1. Data Protection Act 1998

The Act governs the protection and use of **personal** data. It does not apply to personal data relating to the deceased.

Any organisation processing (obtaining, holding, using, disclosing and disposing) data is a 'Data controller' responsible for abiding by the 8 data protection principles and notifying the Information Commissioner of that processing.

The Act gives seven rights to individuals in respect of their own personal data:

- + Right of subject access;
- + Right to prevent processing likely to cause damage or distress;
- + Right to prevent processing for the purposes of direct marketing;
- + Rights in relation to automated decision taking;
- + Right to take action for compensation if the individual suffers damage or damage and distress (as a result of any breach of the act);
- + Right to take action to rectify, block, erase or destroy inaccurate data;
- + Right to request the Information Commissioner for an assessment to be made as to whether any provision of the Act has been contravened.

The Data Protection Act 1998 – 8 Principles:

1. Personal data shall be processed fairly and lawfully and shall not be processed unless at least 1 of the conditions in Schedule 2 is met, and for 'sensitive personal data' at least 1 of the conditions in Schedule 3 is also met.
2. Personal data shall be obtained for specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose/purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose/purposes for which they are processed.
4. Personal data shall be accurate and, where necessary kept up to date
5. Personal data shall not be kept for longer than is necessary for that purpose/purposes.
6. Personal data shall be processed in accordance with the rights of the data subject under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data, and against accidental loss, destruction or damage to personal data.
8. Personal data shall not be transferred to a country or territory outside the EEA without an adequate level of protection for the rights and freedoms of the data subject in relation to the processing of personal data.

Schedule 2 and Schedule 3 Conditions	
<p>Conditions for processing personal data:</p> <ul style="list-style-type: none"> ✚ one condition in Schedule 2 should be met. 	<p>Conditions for processing sensitive personal data:</p> <ul style="list-style-type: none"> ✚ one condition in Schedule 2 and one condition in Schedule 3 should also be met.
<p>Schedule 2: Personal data</p> <p>The data subject has given consent, or the processing is necessary for:</p> <ul style="list-style-type: none"> ✚ A contract ✚ Legal obligation ✚ Protection of the vital ✚ Interests of the data subject ✚ Public function ✚ In the public interest ✚ A statutory obligation ✚ Legitimate interests of the Data controller 	<p>Schedule 3: Sensitive personal data</p> <p>The data subject has given explicit consent, or the processing is necessary for:</p> <ul style="list-style-type: none"> ✚ Employment related purposes ✚ The purpose of, or in connection with legal proceedings ✚ Protection of vital interests of the individual (where consent cannot be obtained) ✚ Made public by the data subject ✚ Substantial public interest ✚ Prevention or detection of an unlawful act ✚ Legitimate interests of a non profit making organisation ✚ Medical purposes

2. The Human Rights Act 1998

The Human Rights Act 1998 incorporates into our domestic law certain articles of the European Convention on Human Rights (ECHR). The Act requires all domestic law to be read compatibly with the Convention Articles. It also places a legal obligation on all public authorities to act in a manner compatible with the Convention.

The sharing of information between agencies has the potential to infringe a number of Convention Rights. In particular:

- ✚ Article 3 (Freedom from torture or inhuman or degrading treatment)
- ✚ Article 8 (Right to respect for private and family life)

Article 8.1 provides that “everyone has the right to respect for his private and family life, his home and his correspondence”.

Article 8.2 provides “there shall be no interference by a public authority with the exercise of this right except as in accordance with the law and is necessary in a democratic society in the interest of national security, public

safety or the economic well-being of the country for the prevention of crime and disorder, for the protection of health and morals or for the protection of the rights and freedoms of others”.

Article 1 of Protocol 1 (Protection of Property).

In addition, all Convention Rights must be secured without discrimination on a wide variety of grounds under Article 14.

3. The Freedom of Information Act (FOIA) 2000

The Freedom of Information Act 2000 applies to all public authorities, creating a new right of access to information (rights of access to personal information will remain under the Data Protection Act) and revising and strengthening the Public Records Act 1958 & 1967 by re-enforcing records management standards of practice.

The Lord Chancellor has issued a code of practice on the management of records under FOIA. The principle is that *“any freedom of information legislation is only as good as the quality of the records to which it provides access. Such rights are of little use if reliable records are not created in the first place”*. Further information and guidance can be found at the following website:

<http://www.informationcommissioner.gov.uk/>

4. The Common Law Duty of Confidentiality

The Common Law Duty of Confidentiality requires that unless there is a statutory requirement to use information that has been provided in confidence, it should only be used for purposes that the subject has been informed about and consented to. In certain circumstances, this also applies to the deceased. The duty is not absolute but should only be overridden if the holder of the information can justify disclosure as being in the public interest i.e. to protect others from harm.

5. Other Legislation

Other Acts apply to further specify these exceptions, e.g. **Prevention of Terrorism Act 2002, Health & Social Care Act 2000, Regulation of Investigatory Powers Act (RIPA) 2000**. Further information about these or any other relevant legislation can be found at the HMSO website <http://www.hmso.gov.uk/>

Appendix B: Metadata

It is essential to provide the metadata for any dataset that is to be posted on the Dawn data observatory. Metadata is the 'data about data' that provides users with reassurances that the information on the site is valid. This is particularly important to promote ownership of local data that is uploaded onto the site; naming individuals helps provide accountability and assurances of data quality. Examples can be found for any of the indicators available on the Dawn data observatory at www.visitdawn.com

INDICATOR NAME: e.g. birth Rate per '000 total population (2005)		
Title	Description	Value
Coverage: Spatial	The geographical coverage of the data	
Coverage: Temporal	The time period for which the data relates	
Coverage: Unit	The geographical unit at which the data is held	
Date: Issued	The date for which the data was made available (format - Year-Month-Day; U = Unknown).	
Date: Update	The date at which the data will next be updated (format - Year-Month-Day; U = Unknown).	
Date: Update Frequency	The frequency with which the data is updated.	
Description: Definition	A detailed, non-jargonised definition, explaining the data	
Description: How Calculated	How calculated	
Description: Quality of Data	The quality or confidence that can be attributed to the data	
Notes	Extra information	
Publisher	An organisation / individual responsible for making the data available plus contact details	
Rights: Copyright	Specifies the legal ownership of the data	
Source	The resource/ dataset from which this data is acquired. State if local data and ensure contact details are completed under 'Publisher' above.	
Subject: Thematic classification	Thematic classification	
Subject: Theme	Theme	
Type: Data	The value label of the data.	

Appendix C: Dawn data observatory - applications

The Dawn data observatory has a range of applications for analysing the performance of the area compared to other regions, localities, and between wards and super output areas. They are designed to help users generate a better understanding of the area - economically, socially and environmentally.

Map

The Dawn data observatory allows you to create thematic maps to compare performance at a range of geographical levels. Maps provide a powerful means of connecting local concerns more broadly with those at a regional and national level. They also provide a means of identifying the geography and character of local communities.

Profile

The Dawn data observatory allows the creation of local area profiles, bringing together a range of indicators to benchmark the performance of a specific area. Up to eight indicators can be selected and a radar chart created to display the results. The higher the score on the chart, the better the performance based on national rankings. Users also have the option of identifying 'nearest neighbours' - other areas with a similar profile.

Rank

The Dawn data observatory allows you to rank regional and local area performance. League tables or lists can be created to show the areas with the best and worst performance - nationally, regionally or locally. The rankings can be created quickly and easily and the outputs can be downloaded into spreadsheets for further analysis.

Compare

The Dawn data observatory allows you to compare local areas on a wide range of indicators. An area can be quickly compared with its neighbouring areas, or with other parts of the country. The outputs are displayed in bar-chart format, providing a graphic representation of the results.

Table

The Dawn data observatory allows you to compare performance on a range of different indicators. Having created a table your selected areas (e.g. wards) can be ranked on any one of the available indicators. Outputs can then be downloaded to an Excel spreadsheet for further analysis. The table application provides a powerful means of exploring the relationships between variables and quickly summarising the characteristics of an area(s).

Change

The Dawn data observatory allows you to compare performance over time. The West Norfolk Partnership has adopted an approach to data analysis and performance management called 'turning the curve'. It looks at performance trends and designs interventions designed to 'turn the curve' – i.e. positively influence future performance. Through Local Knowledge the task of considering the impact of these interventions is greatly simplified.

Appendix D: Dawn Technical Support Group

The development of an effective information sharing approach will be overseen by a small technical support group involving a representative from key partner agencies (see below), with responsibility to ensure that data is provided in the appropriate format, at the agreed time and also be the primary contact for consultation when issues of disclosure or data protection need to be discussed.

The management group will consist of King's Lynn and West Norfolk Borough Council, Norfolk County Council, Norfolk Constabulary, West Norfolk Primary Care Trust, West Norfolk Voluntary and Community Action, West Norfolk Partnership, College of West Anglia, Freebridge Community Housing and Jobcentre Plus. They will have a role in supplying information and also requesting ad hoc interpretations or commissioning relevant research, reporting to the West Norfolk Partnership Board.

The responsibilities of the management group are:

- ✚ To oversee the development of the data observatory.
- ✚ To ensure that information collected meets the requirements of the West Norfolk Partnership and meets the needs of the partners in identifying and tackling local priorities and to review the process regularly.
- ✚ To review the development of The Dawn data observatory locally and to ensure partners have staff trained to input, access and produce reports.
- ✚ To look at standardising the format of data collected including a high level of quality assurance.
- ✚ To work with partner agencies in ensuring that each one is fully committed to the process, and has an agreed plan of action towards a joint goal of information exchange.
- ✚ To ensure that all partner agencies abide by the terms set out in the protocol and agree a suitable course of action if this does not occur.
- ✚ To develop a strategy for including other agencies and organisations within the information sharing process.
- ✚ To ensure data protection principles are met and continue to be met as systems develop.
- ✚ To monitor the operation of the protocol, ensure compliance and agree amendments as necessary.

Organisation	Contact	Email
Borough Council	Martin Slater	
Police	Ian Hudson	
Health		
WNVCA		
NCC – Adult Services		
NCC – Children's Services		
Norfolk Fire Service		
etc		

Appendix E: Glossary of Terms

Aggregated – collated information in a tabular format.

Anonymous data – anonymous data is where an organisation does not have the means to identify an individual from the data they hold. If the data controller has information which allows the data subject to be identified, regardless of whether or not they intend to identify the individual, is immaterial - in the eyes of the Information Commissioner this is not anonymous data. The data controller must be able to justify why and how the data is no longer personal.

Consent – The Information Commissioner's legal guidance to the Data Protection Act 1998 is to refer to the Directive, which defines consent as "...any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed" (3.1.5).

Data – can be defined as individual measurements; facts, figures, pieces of information, statistics, either historical or derived by calculation, experimentation, surveys, etc.; evidence from which conclusions can be drawn and intelligence gained:

- a) Information being processed by means of equipment operating automatically; or
- b) Information recorded with the intention it be processed by such equipment; or
- c) Recorded as part of a relevant filing system; or
- d) Not in a or b or c, but forming part of an accessible record.

Data Controller – a person or a legal body such as a business or public authority, who jointly or alone determines the purposes for which personal data is processed.

Data Exchange Agreement – the local information sharing agreement based on the attached template Appendix D.

Data Processing – any operation performed on data. The main examples are collection, retention, deletion, use and disclose.

Data Set – a defined group of information

Data Subject – an individual who is the subject of personal information.

Disclosure – the passing of information from the Data controller to another organisation / individual

Duty of Confidentiality – everyone has a duty under common law to safeguard personal information.

Health Professional – In the Data Protection Act 1998 "health professional" means any of the following who is registered as:

- ✚ A medical practitioner, dentist, optician, pharmaceutical chemist, nurse, midwife or health visitor, and osteopaths.

and

- ✚ Any person who is registered as a member of a profession to which the Professions Supplementary to Medicine Act 1960 currently extends to, clinical

psychologists, child psychotherapists and speech therapist, music therapist employed by a health service body, and scientist employed by such a body as head of department.

Health Record – any information relating to health, produced by a health professional.

Need to know – to access and supply the minimum amount of information required for the defined purpose.

Personal Data – means data relating to a living individual who can be identified from those data (including opinion and expression of intention).

Processing – any operation performed on data. Main examples are collect, retain, use, disclosure and deletion.

Purpose – the use or reason for which information is stored or processed.

Recipient – anyone who receives personal information except statutory bodies for the purpose of specific inquiries

Sensitive Personal Data – data concerning racial origin, politics, Trade Union activity, health, sexuality, offending, religion, etc.

Subject Access – the individual's right to obtain a copy of information held about themselves.

Third Party – any person who is not the data subject, the data controller, the data processor (includes Health, Housing, Education, Carers, Voluntary Sector etc. as well as members of the public).