

Protocol for Sharing Data Internally

Name: Protocol for Sharing Data Internally

Version: 1.5

Issue Date: 16/07/2003



File	Protocol for Sharing Data Internally	Pages	1	Version	1.5
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified

Document Control

This is a CONTROLLED document and updates or changes to this document are authorized and then advised by email to the relevant document holders.

It is UNCONTROLLED when printed. You should verify that you have the most current issue.

DOCUMENT HISTORY

Author(s)

Names	Role
John Pritchard	ICT Enterprise Architecture Manager

Document Log

Version	Status	Date Issued	Description of Change	Pages affected	Review
1.0		16/07/2003	Approved by the IPG	All	
1.1	Final	11/10/2007	Review and Updated	All	October 2008
1.2	Final	20/10/2008	Reviewed	All	October 2009
1.3	Final	11/10/2009	Reviewed	All	October 2010
1.4	Final	11/05/2010	Removed ISO9001 Logo	All	April 2011
1.5	Final	15/06/2011	Reviewed	All	May 2012

File	Protocol for Sharing Data Internally	Pages	2	Version	1.5
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified

Contents

Contents:

Introduction	4
Definitions, as taken from the Data Protection Act (1998):	4
Objectives of the General Protocol	5
The Document	5
Legislation	6
General	6
Data Sharing within Herefordshire Council	8
General and Individual Protocols	8
General Protocol	8
Directorate 'B'	8
Directorate 'A'	8
Responsibilities	9
Individual Protocol	9
Confidentiality	10
Consent for data sharing	11
Disclosing the data to be shared	13
Subject Access Requests	14
Exemptions from S7 and the right of the Data Subject to access to personal or sensitive personal data are:	15
Accountability	16

File	Protocol for Sharing Data Internally	Pages	3	Version	1.5
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified

Data sharing protocol

GENERAL PROTOCOL FOR INTER-DIRECTORATE DATA SHARING WITHIN HEREFORDSHIRE COUNCIL

Introduction

This document is designed to offer detailed guidance on the considerations that each member of staff should apply prior to sharing data within the authority.

Definitions, as taken from the Data Protection Act (1998):

“data” means information that is being processed by means of equipment operating automatically in response to instructions given for that purpose or is recorded as part of a relevant filing system. For the purposes of this protocol, *“data”* refers to both personal and sensitive personal data, unless it is specified as either type.

“data controller” means a person who determines the purposes for which and the manner in which any personal data are processed (in this case Herefordshire Council);

“data processor” means any person who processes the data on behalf of the data controller (in this case employees of Herefordshire Council);

“data subject” means an individual who is the subject of personal data;

“personal data” means data that relate to a living individual who can be identified from those data or from those data and other information that is in the possession of the data controller;

“processing” in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation on the information or data (including referring to it);

“sensitive personal data” means personal data consisting of information as to:

- the racial or ethnic origin of the data subject
- his political opinions
- his religious beliefs or other beliefs or a similar nature
- whether he is a member of a trade union
- his physical or mental health or condition
- his sexual life
- the commission or alleged commission by him of any offence, or

File	Protocol for Sharing Data Internally	Pages	4	Version	1.5
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified

- any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings

Please note that the above is quoted from the Act, and where the word “him” is used the Act refers to both genders.

Objectives of the General Protocol

To provide a robust framework for the lawful, secure and confidential sharing of data between Council Directorates to enable them to meet both their statutory obligations and the needs and expectations of the people they serve.

To support the strategic purposes of:

- The delivery of integrated public sector services in line with government initiatives, public expectations and legislation.
- The facilitation and planning of cost effective and efficient services.
- The ability for Directorates to review, account for, and learn how to improve what they do.

The Document

The General Protocol defines:

- The legislation that underpin the exchange of data.
- The personnel nominated to support the exchange of data.
- The procedures that will ensure that data is shared/disclosed in accordance with statutory obligations and responsibilities.
- The responsibilities of Directorates to implement internal arrangements to meet the requirements of the General Protocol.

File	Protocol for Sharing Data Internally	Pages	5	Version	1.5
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified

Legislation

General

Legislation defines the role, responsibility and power of the Directorate to enable it to carry out a particular function.

The legislation that governs the processing of data in this context is the Data Protection Act (1998), which is “An act to make new provision for the regulation of the processing of information relating to individuals including the obtaining, holding, use or disclosure of such information.” The Act classifies data into *Personal Data* and *Sensitive Personal Data* that can include paper, electronic data and images (photographs and video).

The Data Protection Act (1998) should not prevent the sharing of data. Provided that the necessary conditions are met, sharing, although not obligatory in all cases, is legal.

The eight data protection principles are:

1. Personal data shall be processed fairly and lawfully and not processed unless at least one of the conditions in Schedule 2 of the Act are met and, if the data is sensitive personal data additionally at least one of the conditions in Schedule 3 is also met.
2. Personal data shall only be obtained for one or more specified and lawful purposes and can only be processed in a manner compatible with those purposes.
3. Personal data shall be:
 - (i) adequate
 - (ii) relevant
 - (iii) not excessive
4. Personal data must be accurate and kept up to date.
5. Personal data shall not be kept longer than necessary for the purposes for which it is being processed.
6. Personal data shall only be processed in accordance with the data subject's rights under the Data Protection Act 1998.
7. Appropriate measures (technical and organisational) shall be taken against unauthorised or unlawful processing, accidental loss, destruction or damage to the data.
8. The personal data shall not be transferred to someone outside the European Economic Area unless there are adequate levels of protection for it.

File	Protocol for Sharing Data Internally	Pages	6	Version	1.5
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified

The key legislation governing the collection and use of data are:

- The Data Protection Act 1998
- The Crime and Disorder Act 1998
- Common Law Duty of Confidentiality

In addition to the above-mentioned legislation, consideration may also need to be given to the following when sharing data:

- The Human Rights Act 1998
- The Caldicott Committee Report
- The Regulation of Investigatory Powers Act 2000

File	Protocol for Sharing Data Internally	Pages	7	Version	1.5
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified

Data Sharing within Herefordshire Council

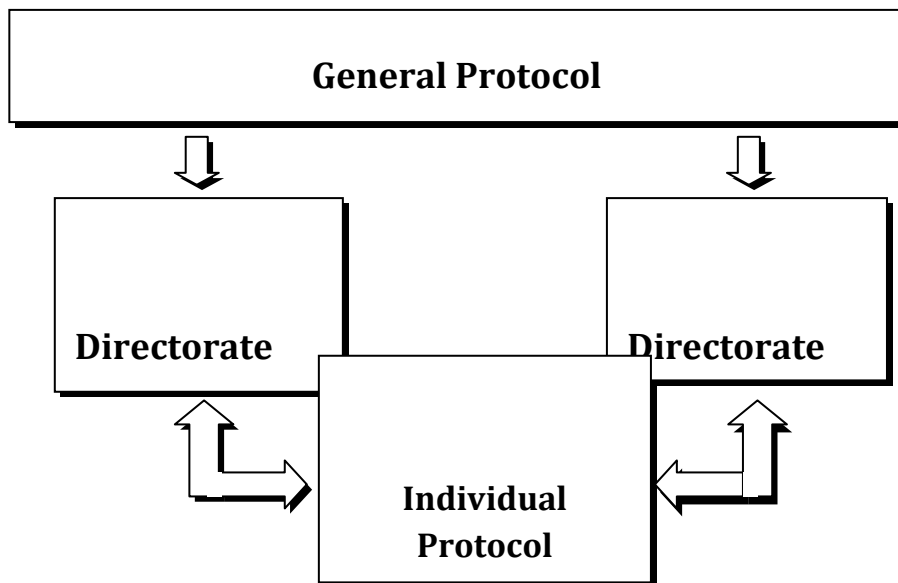
General and Individual Protocols

The General Protocol serves as an overarching regulation to enable the legal and secure exchange of data between Directorates that have common obligations to provide services within the community.

Each Directorate must abide by the General Protocol, the Corporate Information Security Policies and the Retention of Records Policy (currently under review) to in order to share data legally.

In order to facilitate the exchange of data between Directorates, Individual Protocols, as prescribed by the General Protocol, will be agreed and documented between the Directorates that may need to share data about their service user(s). These Individual Protocols will specify the purpose for the exchange of data, the type of the data that may be exchanged, the purpose for which that data may be used and details of who else that data may be shared with.

The diagram below shows how the two types of protocol relate to each other and to Directorates.



File	Protocol for Sharing Data Internally	Pages	8	Version	1.5
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified

Responsibilities

Directorates will nominate a lead person who will be responsible for the day-to-day management of the protocol within their Directorate and the approval of Individual Protocols. The person nominated as 'Lead Person' should have sufficient seniority within the Directorate to influence policies and procedures at executive level.

It is recommended that the 'Lead Person' should be the Data Protection Liaison Officer nominated in each Directorate. Queries about the DPA '98 should be addressed to this person in the first instance.

Responsibility for advice on the Data Sharing Protocol rests with the Information Security Section.

Individual Protocol

In order to maintain a consistent approach, all Directorates will ensure that any Individual Protocol that they develop contains the following data:

- a) The full details of the Directorates, Departments, Services, etc. that are party to the Individual Protocol.
- b) The purpose(s) for the sharing of data.
- c) The type(s) of data that will be shared.
- d) Details of any other Directorates/organisations to whom the data may also be shared by the recipient.
- e) Details of any restrictions on the use of the data.

All Individual Protocols will be approved by the respective Lead Person nominated within each Directorate (see 3.2.2).

A specimen Individual Protocol is given in Appendix A.

Any pre-existing protocols should be read and given effect in accordance with the General Protocol.

Similarly, any subsequent protocols should be read and given effect in accordance with the General Protocol.

File	Protocol for Sharing Data Internally	Pages	9	Version	1.5
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified

Confidentiality

Whilst the leading statute governing data sharing is the Data Protection Act 1998 the Directorates and its staff should remain aware of the common law in relation to confidentiality.

Even if there is no bar on exchange or disclosure under the Data Protection Act 1998 there may be such a bar under the duty of confidentiality, for example where the material supplied was restricted by the data subject for a very specific purpose only.

The Courts in certain circumstances are prepared to accept that an implied duty of confidence exists. For this to exist the data in question must be a) of limited availability and b) of specific character.

If an issue of confidence is suspected to arise the matter should be referred for legal advice as soon as possible.

Directorates are to make use of signed confidentiality agreements with staff as much as possible. This will offer further protection to the Council in the event of a breach of confidentiality by staff arising. The Lead Person should advise their directorate as to which employees should be required to sign a confidentiality agreement.

The Council's disciplinary policy should be implemented if necessary to investigate the inappropriate or unauthorised access to, or use of, data whether intentional or inadvertent.

In the event of shared data being disclosed improperly, whether accidental or intentional, the Directorate making the discovery will without delay:

- Bring the situation to the data subject's attention without delay
- Invite the data subject to make a formal complaint if they so wish
- Tell the data subject what the Council is doing to limit damage and prevent recurrence
- Use the Council's disciplinary procedures if necessary

File	Protocol for Sharing Data Internally	Pages	10	Version	1.5
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified

Consent for data sharing

Unless statutory exemptions are applicable, all Directorates must seek consent from the data subject to share their data in accordance with an agreed Individual Protocol. The DPA '98 defines consent differently in accordance with its classification of Personal and Sensitive Personal Data:

- **Personal:** Non-explicit consent must be obtained. This can either be positive or negative. In the former case consent must be given (e.g. box being ticked). In the latter, consent will be assumed unless contrary indication is made. It is accepted by the Information Commissioner that best drafting practice is to seek positive consent in all cases.
- **Sensitive Personal:** Explicit consent must be obtained after the data subject has been fully informed of the data sharing process. This means that the individual concerned will be made fully aware of the nature of the data that it may be necessary to share, who the data will be shared with, the purposes for which the data will be used and any other relevant details including their right to withhold or withdraw consent.

Consent must be requested at the earliest opportunity.

Consent to disclose data will be limited to the duration of the purpose in question.

Once the purpose for which consent was originally obtained has been completed, that consent will be deemed to have lapsed.

In the event that a similar, or subsequent additional work needs to be undertaken with that data subject, a new consent to disclose will be obtained.

If work is ongoing for a particular purpose, the consent will remain valid.

Where consent is obtained to share Sensitive Personal Data, the data subject should be given a copy of the consent. A copy should be forwarded to the Directorate receiving the data.

Directorates will ensure that a record is made of the details (including any conditions) of any consent, or refused consent.

Any data subject may withdraw or modify their consent. If that relates to any data shared, the relevant Directorate should be notified and the shared ceased immediately unless a legal exemption can be applied.

File	Protocol for Sharing Data Internally	Pages	11	Version	1.5
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified

In some circumstances consent is not required. This is legal provided that at least one of the other conditions contained in the Data Protection Act (1998) Schedule 2 are met (in the case of Personal Data) and one or more conditions in Schedule 2 and Schedule 3 are met (in the case of Sensitive Personal Data). Please refer to the respective Data Protection Liaison officer for clarification if necessary. Even if the required conditions are met, if it is practicable to request consent, such a request should be made.

A decision to share data without the consent of the individual concerned must be authorised by the Lead Person and the reason(s) recorded locally.

On disclosure of the data, the Directorate providing the data will make the receiving Directorate aware that disclosure is being made without consent and the reason(s) why.

Data may be shared when anonymised (e.g. for research or statistical purposes).

File	Protocol for Sharing Data Internally	Pages	12	Version	1.5
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified

Disclosing the data to be shared

Directorates will ensure that, in instances where it is unclear whether data is fact, opinion or a mixture of the two, staff from the providing Directorate to the receiving Directorate make it clear which is which. This is particularly important where such data is likely to be subject to evaluation as to disclosure, for example whether the data falls within the ambit of one of the exemptions.

Directorates will ensure that all data that has been disclosed to them under an agreed Individual Protocol will be recorded accurately.

Directorates will set in place procedures to record not only the details of the data, but also who gave and who received that data.

Directorates will exercise caution when contemplating the disclosure of data relating a deceased person. Although the Data Protection Act (1998) only applies to the data of a living person, a duty of confidentiality may still apply after the person has died and everyone involved should be aware of the sensitive nature of this issue.

In the case of a complaint by a service user with relation to data sharing, the Directorate should refer to the Council's complaints procedure.

All Directorates will provide co-operation and assistance in order to investigate and resolve any complaint.

All Directorates should make their personnel aware of their responsibilities towards confidentiality. Responsibilities to confidentiality are referred to in the Council's Terms and Conditions of Employment given to each employee.

Line management are to ensure that staff are given adequate training and awareness in line with their duties and responsibilities.

All Directorates will follow the regulations in the Corporate Information Security Policies and Records Retention Policy (currently under review) for Security, Storage, Access, Retention and Destruction of Data.

It is recognised that Directorates may fulfil a number of roles. In fulfilling one particular role, they may be given privileged access to data that they may subsequently believe may assist them in another role or be of wider interest to other directorates.

Data shared under this General Protocol will have been disclosed for a specific purpose, as defined in the Individual Protocol, and as such must only be used for that purpose.

File	Protocol for Sharing Data Internally	Pages	13	Version	1.5
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified

Data that has been obtained under an agreed Individual Protocol will not be regarded or used by the receiving Directorate as intelligence for the general use of that organisation.

Directorates wishing to use data given under the General Protocol for any purpose other than that defined in the Individual Protocol, or who may wish to disclose that data to any person other than those authorised to receive that data, must:

- a) inform the originator of the data of their intention to use the data provided for a different purpose, and
- b) Obtain consent from the individual(s) concerned if relevant before processing such data.

Subject Access Requests

A service user making a valid request under section 7 of the DPA '98 for access to his/her record will be fully informed, in accordance with the Act, about the data that is held about them by the Directorate approached.

Directorates must confirm the identity of the Data Subject at the time of request and before the data is supplied. The Data Subject must produce an original form of identification which must be one of the following: birth certificate, marriage certificate, passport, residence permit issued by the Home Office to EU Nationals on sight of own country passport, photo ID driving licence

In the situation of two or more Directorates having a joint (single) record on an Data Subject, that Data Subject may make their subject access request to any of the Directorates. The Directorate receiving the request will be responsible for processing the request for the whole record and not just the part that they may have contributed, subject to the conditions for disclosure.

Once a request has been made under S7 DPA '98 the Directorate must then go on to consider whether disclosure should be made. One of three situations will then be identified, these are:

1. The request is one that the Directorate wishes to accede to and there is no statutory exemption preventing disclosure.
2. The request is one that the Directorate does not wish to accede to but there is no statutory exemption preventing disclosure.
3. The request is one that the Directorate does not wish to accede to and there are one or more statutory exemptions from disclosure that may be relied upon.

File	Protocol for Sharing Data Internally	Pages	14	Version	1.5
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified

Data that has been provided by another Directorate under an agreed Individual Protocol may be disclosed to the data subject without the need for obtaining the provider's consent to disclose, unless the provider has specifically stated that the data supplied must be kept confidential from the data subject user and one or more exemption from disclosure applies.

Exemptions from S7 and the right of the Data Subject to access to personal or sensitive personal data are:

S28 National Security – Absolute

S29 – Crime and Taxation – Qualified – “ Prejudice” test.

S30 – Health education & Social Work – by specific delegated legislation

S31 – Registered Activity – Qualified – “Prejudice” test.

S32 – Journalism – Qualified

S33 – Research History and Statistics – heavily qualified

S34 – Information publicly available by statute – Absolute

Schedule 7 contains additional exemptions:

1. Confidential references- absolute
4. Crown employment – by delegated legislation
5. Management forecasts- qualified by “prejudice” test.
6. Corporate finance-qualified
7. Negotiations with the Data Subject-qualified by “prejudice” test.
8. Legal professional privilege-absolute

There are also specialised regulations dealing with personal data in the fields of

- (a) Health
- (b) Social Services and Social Work
- (c) Education

and the relevant individual protocols will take account of these.

File	Protocol for Sharing Data Internally	Pages	15	Version	1.5
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified

Accountability

Sharing of data must be justifiable on statutory grounds, or a meet the criteria for claiming an exemption under the DPA '98. Without such justification, both the Directorate and the member of staff expose themselves to the risk of prosecution and liability to a compensation order under the Data Protection Act (1998) or damages for a breach of the Human Rights Act. Additionally the Directorate may be subject to an Enforcement Notice by the Information Commissioner.

File	Protocol for Sharing Data Internally	Pages	16	Version	1.5
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified

General Protocol Appendix A - SPECIMEN INDIVIDUAL PROTOCOL

Directorate 'A' (and details of Lead Person)

And

for Inter-Directorate Data Sharing

This Individual Protocol is made under the General Protocol for Inter Directorate Data Sharing between:

Directorate 'B' (and details of Lead Person)

1. Purpose for the sharing of personal data:

Statement defining the purpose(s) for the sharing of personal data.

2. Type of data that may be shared:

List in broad category terms the type of data that may need to be shared e.g.

'Basic' person details = name, address, date of birth etc.

Sensitive data = ethnic origin, criminal offences etc.

Relationships = next of kin, doctor etc.

3. Who else this data may be shared with:

The receiver of the personal data should list details of who else the data may need to be shared with e.g. not party to this Individual Protocol.

4. Restrictions on data shared:

If the provider of the personal data requires to place any additional restriction on the use of the data, this should be indicated here.

File	Protocol for Sharing Data Internally	Pages	17	Version	1.5
Owner	John Pritchard	Distribution	ICT & MRU	Classification	Unclassified