Island Strategic Partnership

Information Sharing Protocol

THIS IS AN ISLAND STRATEGIC PARTNERSHIP INFORMATION SHARING PROTOCOL TO BE USED IN CONJUNCTION WITH COUNCIL POLICIES AND GOVERNMENT LEGISLATION

Phase One Signatories

Partner Organisation	Position Held	Signature	Date
ISLE OF WIGHT COUNCIL	Chief Executive	Steve Beynon	14/10/08
ISLE OF WIGHT NHS PRIMARY CARE TRUST	Chief Executive	Margaret Piatt	29/10/08.
HAMPSHIRE & ISLE OF WIGHT CONSTABULARY	Commander		10.12.12
ISLE OF WIGHT FIRE AUTHORITY	Chief Fire Officer	Paul Thorn.	15/10/08
RURAL COMMUNITY COUNCIL	Chief Executive	M. Burdett	15/10/08
MEDINA HOUSING ASSOCIATION	Chief Executive Officer		20/10/08
SOUTH WIGHT HOUSING ASSOCIATION	Executive Director		29/10/08
ISLE OF WIGHT PROBATION SERVICE	Chief Executive Officer		27/2/09.
ISLE OF WIGHT PRISON SERVICE	Governor Isle of Wight Prisons		28/10/08
VECTIS HOUSING ASSOCIATION	Chief Executive Officer		21/10/08

CONTENT

1. INTRODUCTION

This overarching Protocol sets out the principles for information sharing between Partner Organisations. This Protocol sets out the rules that all people working for or with the Partner Organisations must follow when using and sharing information.

The Protocol applies to the following information:

- All personal information processed by the organisations including electronic (e.g. computer systems, CCTV, Audio etc), or in manual records.
- Aggregated and anonymised data. The considerations, though less stringent, must take into account factors such as commercial or business, sensitive data, and the effect of many data sets being applied.

This Protocol will be further extended to include new members, where applicable, from other public sector, private and voluntary organisations working in Partnership with the ISP to deliver services.

It does this in two ways:

1. Informing the participating organisations of the legal, commercial or practical issues that they must consider when sharing information.
2. Providing a standard process and agreement that organisations can customise to meet the needs of specific information sharing situations or projects.

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.

The legal situation regarding the protection and use of personal information can be unclear. This situation may lead to information not being readily available to those who have a genuine need to know in order for them to do their job properly. See Appendix A for Relevant Legislation.

Regulation of Investigatory Powers Act (RIPA) 2001 is also applicable and allows "any covert information/evidence gathered by a partner agency will comply with the Regulation of Investigatory Powers Act (RIPA) 2001. Covert investigations by a partner agency must be authorised and conducted within the statutory framework. Where there are concerns about the standard of integrity of information/evidence, further information/evidence will be sought."

Unlike other arrangements this protocol is intended to provide a consistent framework and common standard for different organisations to adopt. 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. However, it must be recognised that given the diversity of the partner organisations that each partner will need to temper expectation to organisational realities. Adopting it removes the need to have multiple protocols as it provides the flexibility – through the use of standard agreement forms – to use this one protocol in many different situations and with different partners.

For the purpose of this protocol, the terms data and information are synonymous.

2. PURPOSE

The purpose of this information sharing protocol between the signatory services listed above is to facilitate the sharing of data to develop a robust basis for the Sustainable Community Strategy (Eco Island) whilst protecting vulnerable adults and children.

As signatories we agree that this protocol is an enabling document that ensures that the sharing of information should be made easy and accessible, where appropriate, and as such will be actively encouraged. This document should be the basis for promoting the value of effective partnership working.

3. LEGAL BASIS OF THIS AGREEMENT

This agreement involves the Island Strategic Partnership and therefore each partner's own Data Protection Act registration applies, and ensures that there is a legal basis for the sharing of the agreed information.

Please note for the purposes of this document we have used the legal definition of 'In Confidence and Confidential' information and not the Government Protective Marking Scheme's (GPMS) protective marking definition, which has been introduced by the Cabinet Office.

This agreement is also based on the provisions as set out in the following legislation (Appendix A):

- Civil Contingencies Act 2004
- Common Law Duty of Confidence
- Data Protection Act 1998
- Freedom of Information Act 2000
- Human Rights Act 1998
- Regulation of Investigatory Powers Act (RIPA) 2001
- Rehabilitation of Offenders Act (1974)
- The Crime and Disorder (Prescribed Information) Regulations 2007
- The Housing Acts of 1985, 1988 and 1996
- And all associated guidance documents

The Government's Caldicott Regulations also apply to social and health care. Each partner's Guardian is responsible for the establishment of procedures governing access to and the use of personally identifiable information within the strategic partnership, and where local flexibilities exist, the transfer of such information from the organisation to other bodies. In agreeing local procedures and policies, the Guardian should ensure consistency with any relevant central requirements and guidance.

4. SCOPE & APPLICATION

There are three types of data sharing situations that are covered by this Protocol.

A Non-Personal Data

Non-personal data is data that does not refer to living individuals. There are two types of non-personal data:

1. Data that has never referred to people; for example information on organisations, natural resources and projects.
2. Data about people that has been aggregated or tabulated in ways that make it impossible to identify the details of individuals.

Sharing of non-personal data for any purpose is covered by this Protocol.

B De-Personalised Data

De-personalised data is 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.

Note that although an organisation holding de-personalised data may not be able to identify individuals, there is a risk that a third party with other information may be able to. For this reason care may be needed with the storage and disposal of de-personalised information to comply with legal obligations.

Sharing of de-personalised data for any purpose is covered by this Protocol.

Both non-personal and de-personalised data are outside the scope of the Data Protection Act.

C Personal Data

Personal data is data about living individuals who can be identified from the data, either directly or by pooling with other information available to the organisation.

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, and financial status) and sensitive personal data (e.g. religious & political beliefs, health and sexual behaviour).

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 Sections 29 and 33 of the Act.

5. GENERAL PRINCIPLES

We agree as signatories to this Protocol to undertake to co-operate with each other and to fully and properly use its principles, procedures and supporting forms.

We agree that this Protocol should be automatically considered an appropriate partner by other signatories to this Protocol, provided that the data sharing activity is within the scope of this Protocol.

This Protocol provides an agreed framework for the process of agreeing, recording and actioning data sharing activities.

Complete freedom is given to the parties in deciding the specific circumstances of each data sharing project that takes place between partner organisations. Different data sharing projects may have different detail agreements, even where all parties are signatories to this Protocol.

Responsibility for entering into specific agreements shall be devolved to the level of management responsible for delivering particular projects or activities; e.g. Head of Service or Department.

Specific data sharing agreements shall be recorded using the standard Data Exchange Agreements (See Appendix B).

Data exchange agreements are intended to be binding on all the parties that enter into them.

We agree that any owner of data, even if a signatory to this Protocol, has the right to refuse to share data. However, where the request has come from another signatory to this Protocol, the party refusing the request must provide to the requester a proper explanation of why the request has been refused.

We agree that where a party to an agreement wishes to use a sub-contractor in the data sharing process they are responsible for ensuring that their contractor fully complies with the requirements of this Protocol and the specific data exchange agreement. Good examples are where researchers are employed or where the sanctuary system is in operation.

6. AIMS AND OBJECTIVES

As signatories we agree that the aim of this Protocol is to provide a framework for the Partner Organisations and to establish and regulate working practices between Partner Organisations. The Protocol also provides guidance to ensure the secure transfer of information, and that information shared is for justifiable 'need to know' purposes

These aims include:

- To guide Partner Organisations on how to share personal information fairly.
- To explain the security and confidentiality laws and principles of information sharing.
- To increase awareness and understanding of the key issues.
- To emphasise the need to develop and use Data Exchange Agreements.
- To support a process, this will monitor and review all data flows.
- To encourage flows of data.
- To protect the Partner Organisations from accusations of wrongful use of personal data.
- To identify the lawful basis for information sharing.
- Achieve standards as set out in the Government's Information Governance Toolkit. Guidance can be found at: https://www.igt.connectingforhealth.nhs.uk/

By becoming a Partner to this Protocol, we agree as partner organisations that we are making a commitment to:

- Follow the Information Commissioner's "Framework Code of Practice for Sharing Personal Information;
- Adhere to or demonstrate a commitment to achieving the appropriate compliance with the Data Protection Act 1998
- Develop local Data Exchange Agreements that specify transaction details.

All Partners will be expected to promote staff awareness of the major requirements of Information Sharing. This will be supported by the production of appropriate guidelines where required that will be made available to all staff via the Partners' Intranet sites and/or via other communication media.

7. PURPOSES FOR SHARING INFORMATION

(Please see Appendix C for Information Sharing Guidelines)

As signatories we agree as signatories that:

- Information should only be shared for a specific lawful purpose or where appropriate consent has been obtained.
- Staff should only have access to personal information on a justifiable need to know basis, in order for them to perform their duties in connection with the services they are there to deliver.
- Having this agreement in place does not give license for unrestricted access to information another Partner Organisation may hold. It lays the parameters for the safe and secure sharing of information for a justifiable need to know purpose.
- Every member of staff has an obligation to protect confidentiality and a duty to disclose information only to those who have a right to see it.
- All staff should be trained and be fully aware of their responsibilities to maintain the security and confidentiality of personal information.
- All staff should follow the procedures and standards that have been agreed and incorporated within this Information Sharing Protocol and any associated Data Exchange Agreements.
- Each Partner Organisation will operate lawfully in accordance with the 8 Data Protection Principles
- 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.

8. SECURITY AND DATA MANAGEMENT SECTION

It is our responsibility as signatories to this protocol, to ensure that we have adequate security arrangements in place, in order to protect the integrity and confidentiality of the information we hold.

As signatories we agree that personal information disclosed must;

- Not be emailed over internet links.
- Be protected by back-up rules.
- When stored on a computer system, it must be password protected and we agree this password will be revised regularly.
- When manual, be stored in a secure filling cabinet when not in use.
- Be located in a geographically secure environment.
- Not be inputted or accessed without industry standard security devices in place

All data held by us is subject to a "shelf-life." All personal data disclosed to us will be held until it is no longer needed.

We understand that all these measures need to be taken to ensure the security of our partners and to protect the general public.

We are aware that only the minimum amount of information should be disclosed, in order to get the job done and for the purpose for which it was intended. We agree that all information retained by us and out partners should be kept securely and for not longer than is strictly necessary.

9. RESTRICTIONS ON USE OF INFORMATION SHARED

As signatories we agree that information must only be used for the purpose(s) specified at the time of disclosure(s) as defined in the relevant Data Exchange Agreement. It is a condition of access that it must not be used for any other purpose without the permission of the Data Controller who supplied the data.

Additional Statutory restrictions apply to the disclosure of certain information for example Criminal Records, HIV and AIDS, Assisted Conception and Abortion, Child Protection etc.

10. CONSENT

We agree as signatories that:

- Consent is not the only means by which data can be disclosed. Detailed advice can be provided by each partner organisation's governance leads regarding to the guidance provided under the Data Protection Act.
- Where a Partner Organisation has a statutory obligation to disclose personal information then the consent of the data subject is not required; but the data subject should be informed that such an obligation exists within the Fair Process Notice, where appropriate.
- If a Partner Organisation decides not to disclose some or all of the personal information, the requesting authority must be informed. For example the Partner Organisation may be relying on an exemption or on the inability to obtain consent from the data subject.
- Consent has to be signified by some communication between the organisation and the Data Subject. If the Data Subject does not respond this cannot be assumed as implied consent.
- If consent is used as a form of justification for disclosure, the data subject must have the right to withdraw consent at any time. When using sensitive data, explicit consent must be obtained. In such cases the data subject's consent must be clear and cover items such as the specific details of processing, the data to be processed and the purpose for processing.
- Specific procedures will apply where the data subject is either under the age of 12, or where the data subject does not have the capacity to give informed consent. In these circumstances the relevant policy of the Partner Organisation should be referred to.

11. SECTION 60 OF THE HEALTH AND SOCIAL CARE ACT 2001

As signatories we agree that where information is specifically required from the PCT Section 60 of the Health and Social Care Act disclosure will be implemented as required by the Health and Social Care Act through PIAG (Patient Information Advisory Group). Data Exchange Agreements will need to be approved by PIAG.

Section 60 is for:

- Those wishing to obtain identifiable patient information;
- Data controllers who are asked to supply identifiable patient information;
- Research Ethics Committees who are asked to advise on the ethical disclosure and use of identifiable patient information.

In circumstances where:

- Patient consent has not been obtained, and
- There is no other reliable basis in law to permit the disclosure and use of identifiable patient information

Section 60 approval does not allow the setting aside of obligations under the Data Protection Act 1998 or any other legislation (e.g. Human Rights Act 1998), only obligations under the Common Law of Confidentiality, which is not codified and is established through case law. This can make it difficult to know in advance whether a use of medical records could be a potential breach of confidentiality, and hence whether Section 60 exemption is appropriate to set aside an individual's rights of redress under common law. Clearly, the simplest approach is to consider that any sharing of patient identifiable information other than for the provision of direct care to the patient could lead to a potential breach of confidentiality.

12. RETENTION

As signatories we agree that retention should be for the minimum period required to achieve the objectives of the purpose of the sharing of information after which the information disclosed will be returned to the originator or destroyed as agreed.

Retention of any documents must comply with the Data Protection Act 1998 and/or with the relevant information sharing legislation under which the information is shared.

13. SUBJECT ACCESS

As signatories we agree that if an agency receives a subject access application and personal information is identified as belonging to another agency, it will be the responsibility of the agency receiving the application to contact the information owner to determine whether the latter wishes to claim an exemption under the provisions of the Data Protection Act.

Each partner agency will have their own Access to Information Policy, which will be adhered to when a subject access request has been received including obtaining third party consent procedures.

14. COMPLAINTS AND BREACHES OF CONFIDENTIALITY

As signatories we are responsible for any complaints or appeals process. Any Data Protection or Freedom of Information requests must be responded to only after consultation with the relevant partner organisation which provided the information.

The Principal Designated Officer for each agency must be notified immediately of any of the above. All complaints must be acknowledged in writing within 2 days and, wherever possible, dealt with within 28 days. Any disciplinary proceedings will be implemented according to the partner organisation's policies.

15. ORGANISATIONAL RESPONSIBILITIES

As signatories we agree that:

- Each Partner Organisation is responsible for ensuring that their organisational and security measures protect the lawful use of information shared under this Protocol.
- The supplying organisation identifies any legislative exemptions prior to the sharing of personal information and informs the requesting organisation of the exemptions applied.
- Partner Organisations will accept the security levels on supplied information and handle the information accordingly.
- Partner Organisations accept responsibility for independently or jointly auditing compliance with the Data Exchange Agreements in which they are involved within reasonable time-scales. It is envisaged that this will occur when this document is reviewed by the appropriate governance leads.

- Every organisation should make it a condition of employment that employees will abide by their rules and policies in relation to the protection and use of personal information. This condition should be written into employment contracts and any failure by an individual to follow the policy should be dealt with in accordance with that organisation's disciplinary procedures and any appropriate legal action.
- Every organisation should ensure that their contracts with external service providers abide by their rules and policies in relation to the protection and use of personal information.
- The Partner Organisation originally supplying the information should be notified of any breach of confidentiality or incident involving a risk or breach of the security of information.
- The Partner Organisation also have an obligation to inform the receiving organisation when information changes.
- Partner Organisations should have documented policies for retention, weeding and secure waste destruction.

16. INDIVIDUAL RESPONSIBILITIES

We also agree as signatories that we will ensure that all individuals within our respective organisation are aware of their individual responsibilities as follows:

- Every individual working for the organisations listed in this Partnership Agreement is personally responsible for the safekeeping of any information they obtain, handle, use and disclose.
- Every individual should know how to obtain, use and share information they legitimately need to do their job.
- Every individual has an obligation to request "proof of identity", or takes steps to validate the authorisation of another before disclosing any information.
- Every individual should uphold the general principles of confidentiality follow the rules laid down in this Protocol and seek advice when necessary.
- Every individual should be aware that any violation of privacy or breach of confidentiality is unlawful and a disciplinary matter that could lead to their dismissal.

17. DATA QUALITY

As signatories we agree that each supplying partner organisation will provide the requesting organisation with assurance that the quality of the data supplied is both timely and accurate to the best of their knowledge. Where data quality is not assured the information provided needs to be used with caution as legislation may possibly be breached and an individuals rights infringed under such circumstances.

18. AUDIT SECTION

Audit of Data: we undertake to ensure that we will collect, process, store and disclose all data held by us, within the terms of this protocol and the relevant legislation. We agree to ensure that all information held by us, is accurate, relevant and fit for the purpose for which it is intended.

Audit of Security: we agree to store all held data securely as per the terms of the security and data management section. We will dispose securely of all data held. We also pledge to conduct six-monthly audits of our security arrangements, to ensure they are effective.

Audit of Protocol: we undertake to conduct regular audits of this protocol at yearly fixed periods, in order to amend it and ensure it remains fully effective.

19. DESIGNATED OFFICERS

As signatories we agree that each partner will appoint a Principal Designated Officer (PDO) who is a manager of sufficient standing and has a coordinating and authorising role. The named individuals listed below are designated to assume responsibility for data protection, security and confidentiality and compliance with all relevant legislation.

Partner	Name
Isle of Wight Council	Susanne Holman-Harris
Isle of Wight NHS Primary Care Trust	Phil Dyer
Hampshire & Isle of Wight Constabulary	Dave Gledhill
Rural Community Council	Nigel Parrish
Isle of Wight Fire Authority	Paul Gould
Medina Housing Association	Martyn Pearl
South Wight Housing Association	Margaret Wright
Isle of Wight Probation Service	Nikki Shave
Isle of Wight Prison Service	*To be confirmed*
Vectis Housing	Lynda Purkis or Paul Hann

20. CLOSURE OR TERMINATION OF THIS AGREEMENT

As signatories we agree that any partner may suspend this agreement if they feel that security has been seriously breached.

This agreement may be terminated if there is a serious breach of confidentiality for example, where information provided under the agreement is used for purposes other than set out in this agreement or information is passed to a third party other than with the agreement of the provider.

21. REVIEW OF THIS AGREEMENT

As signatories we agree that this agreement will be reviewed annually from the date of agreement and that all breaches of the policy are to be logged, investigated and the outcome noted and acted upon.

22. PROTECTIVE MARKING

As signatories we agree that no organisation will reduce the marking of data or release preciously marked data. By reducing the marking of data an organisation could become "information leak" and therefore to handle data differently to the primary controlling organisation without any explicit written agreement to the change of marking is prohibited.

As signatories we agree to adhere to the same handling processes as the controlling organisation and not pass protectively marked information onto anyone who does not meet an agreed set standard.

We also agree that, whilst appreciating the diversity of partner organisations, each partner will review its protective marking policy and where applicable work towards implementing the Government Protective Marking Scheme (GPMS).

Appendix A: Relevant Legislation

1. Section 60 - The Health and Social Care Act

Further guidance on Section 60 can be found at:
http://www.advisorybodies.doh.gov.uk/piag/s60guidancenotes.PDF

Further guidance on the Act can be found at: http://www.opsi.gov.uk/Acts/acts2001/

2. The Data Protection Act 1998

Further guidance can be found at: http://www.opsi.gov.uk/Acts/Acts1998/

3. The Freedom of Information Act (FOIA) 2000

Further guidance can be found at http://www.informationcommissioner.gov.uk/

4. The Human Rights Act 1998

Further guidance can be found at: http://www.justice.gov.uk/docs/act-studyguide.pdf

5. The Common Law Duty of Confidentiality

6. The Crime and Disorder (Prescribed Information) Regulations 2007

The National Incident Category List in the National Standards for Incident Recording Instructions for Police Forces in England and Wales for 2007/2008 is available from the Home Office at 2 Marsham Street, London SW1P 4DF; the Home Office Notifiable Offences List is available on the website http://www.homeoffice.gov.uk/rds/countrules.html;

Fire Statistics, United Kingdom 2005 is available on the website
http://www.communities.gov.uk/index.asp?id=1509023;

Best Value Performance Indicators: 2005/06 is available on the website http://www.audit-commission.gov.uk/performance/guidance.asp;

The International Classification of Diseases, Tenth Revision (ICD-10) published by the World Health Organisation is available from the website
http://www.who.int/classifications/apps/icd/icd10online/

Responding to domestic abuse: a handbook for health professionals is available on the website
http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4126161.

7. 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: Example of a Data Exchange Agreement

Data Exchange Agreement

This is a Data Exchange Agreement between the Isle of Wight Council and *(include name of partner service or agency here)* to be used in conjunction with council policies and government legislation

Signatories

Partner Organisation	Name and Position Held	Signature	Date
NAME OF SERVICE OR PARTNER AGENCY	*Name and Position of Signing Officer*		
NAME OF SERVICE OR PARTNER AGENCY	*Name and Position of Signing Officer*		
CALDICOTT GUARDIAN ISLE OF WIGHT COUNCIL			

1. **Purpose of this Data Exchange Agreement**
   This Data Exchange Agreement (DEA) is for the purpose of exchanging information between the signatory services listed above.

   Add a statement here about the purpose of the agreement.....

2. **Legal Basis of this agreement**
   This agreement involves partner services within the Isle of Wight Council and therefore the council's own Data Protection Act registration applies, and ensures that there is a legal basis for the sharing of the agreed information.

   This agreement is also based on the provisions as set out in the *(add a list of legislation that is applicable to this agreement here.....)* For example "Civil Contingencies Act and associated guidance, which provide the Isle of Wight Council with the authority and legal basis to implement this agreement with regard to emergency response."

   The Government's Caldicott Regulations also apply. The Guardian is responsible for the establishment of procedures governing access to and the use of personally identifiable information within the Isle of Wight Council, and where local flexibilities exist, the transfer of such information from the organisation to other bodies. In agreeing local procedures and policies, the Guardian should ensure consistency with any relevant central requirements and guidance.

   2.1 Extent and type of information to be shared
   Add a statement here about the extent and type of information to be shared.....

   For example "The Isle of Wight Council will ensure that the current annual consent review includes notification of this use of their data is included and explained to Service Users."

3. Agreed Information Datasets and Frequency of Reports

3.1 Report

Report Name: *Add name of report(s) here…..*

Include a comprehensive list of information including reports to be share

For example
- Address
- Contact Number
- Vulnerability/Client Category
- Known Hazards
- Carer name and contact details
- Language details

3.2 Frequency

Include details of the frequency that the information will be shared here….

For example "The report for emergency response purposes will run nightly and downloaded daily to the Fire Service's WINGS system, which will only be accessed on the explicit approval of the Caldicott Guardian or their delegated officer in the case of an emergency."

3.3 Approval for Access and Release

This may or may not be relevant but needs to be considered.

The Fire Control Centre will telephone either of the following officers to obtain consent for the access and release of the agreed information to the authorised emergency response officer in charge.

Caldicott Guardian: xxxxxxxxxxxxxxxxxxxxxxx
Caldicott Co-ordinator: xxxxxxxxxxxxxxxxxxxxxxx

3.4 Method of Communication

Include details of the method of communication here….

For example "The report will be run nightly via Business Object XI, which will be stored securely on a central share drive that can be accessed by the relevant officers on the approval of the Caldicott Guardian."

4. Responsibility

Include who will be responsible for developing and providing the information here…….

5. Retention

Include details of the relevant retention policy here…..

For example "The information will be run nightly with the dataset will be overwritten and the information will be stored on a secure network drive with authorised access only with Caldicott Guardian approval to access and release only."

6. Constraints

This agreement must operate within the constraints of the purposes as listed within this document in order for the law sharing of this information to exist.

7. Feedback

7.1 Agreed Feedback Format

Review Meetings to review the reports provided and feedback questionnaires as appropriate

7.2 Frequency of Feedback

Initially monthly and then bi-monthly as necessary

8. How this information may be used

Include details of how the information may be used here….

For example "The information may only be used by the person requesting it to assist the management of Emergency Response for the protection of vulnerable adults and children."

9. Security and Data Management

The security of the information disclosed is the responsibility of the partner service requesting the information and it must not be copied or transferred into any other medium or disclosed to anyone not listed in the agreement or outside the remit of the agreement.

The designated employees of the partner services who will have access to the information will abide by the security and data management restrictions as stated in the Council's Information Disclosure document.

10. Storage of Information

The information will need to be stored securely and where agreed on an encrypted laptop with the information removed once the purpose of the use of this information has been concluded. The laptop when not in use will need to be stored securely within a safe haven location. Authorised access with password protection will be required.

11. Complaints and Breaches of Confidentiality

The partner organisation providing the information is responsible for any complaints or appeals process. Any Data Protection or Freedom of Information requests must be responded to only after consultation with the partner organisation which provided the information.

The Principal Designated Officer for each agency must be notified immediately of any of the above. All complaints must be acknowledged in writing within 2 days and, wherever possible, dealt with within 28 days. Any disciplinary proceedings will be implemented according to the Isle of Wight Council's policies.

12. Data Quality

Please note at the signing of this agreement the quality of the data is currently being reviewed and as such the data quality cannot be assured, and therefore must be used with caution as legislation may possibly be breached and an individual's rights infringed under such circumstances.

13. General Operational Guidance

13.1 Audit

PDO's and PO's must be mindful of the use they make of information specified within this agreement and whether their decision will stand scrutiny at a later stage. This should not, however, be a barrier to the disclosure of information in appropriate circumstances, but will necessitate the keeping of adequate records of disclosure and the reasons for them.

It is the responsibility of the Designated Officers of the partner services to review this agreement annually and it is the responsibility of all the Principal Designated Officers, listed below, to ensure that information is being used and stored in the correct manner and that the list of Designated Officers is up to date.

13.2 Closure or termination of agreement

Any partner service may suspend this agreement if they feel that security has been seriously breached.

This agreement may be terminated if there is a serious breach of confidentiality for example, where information provided under the agreement is used for purposes other than set out in this agreement or information is passed to a third party other than with the agreement of the provider.

14. Designated Officers

Each service must appoint a Principal Designated Officer (PDO) who is a manager of sufficient standing and has a coordinating and authorising role. It is recommended that a Designated Officer (DO) is also appointed within each partner service the details of whom are listed below.

The named individuals listed are designated to assume responsibility for data protection, security and confidentiality and compliance with all relevant legislation. Specific responsibilities of the PDO and DO are as follows but not limited to:

- Ensuring that all sections of this agreement are adhered to.
- Ensuring that all PDO's, DO's and other staff are fully aware of their responsibilities.
- Ensuring the agreement is accurate, up to date and adequate for the purpose for which it is intended.

Department	DEA Role	Position	Telephone No.	Secure Fax No.
Legal Services	Principal Designated Officer	Susanne Holman-Harris Information Governance Manager		
Name of signatory service	*Principal Designated Officer*			
Name of signatory service	*Designated Officer*			

15. Review of this agreement

This agreement will be subject to a formal annual review. All breaches of the policy are to be logged, investigated and the outcome noted and acted upon.

16. Future Development of Information Sharing

Any future development of the type and scope of the information formally shared by partner agencies will require further discussion and formal agreement by the relevant Senior Management Team and Cabinet Members.

Appendix C: Information Guidelines

Sharing personalised information need not be frightening, but we must stick to these guidelines to ensure that we are exchanging it safely.

1. The Forms

A form must be completed to ensure that the process of information exchange can be carefully monitored, this will essentially track the different steps outlined above.

This form is to be completed if the request is:

- From an agency, that is a signatory to the ISP, requesting personalised information about a data subject.
- From an agency or from the data subject he or she, for access to, or correction of, information held about the data subject.

2. Security data

2.1 Exchanging information securely

It is important that we exchange information safely. We have to ensure that we are only exchanging information with those people we think we are! Data can be exchanged in a variety of ways and there are advantages and disadvantages to each method. Ways in which you may choose to exchange information are:

- **Fax**
  This is only secure if the recipient is waiting at the machine to receive the document immediately. Do not assume this will always be the case.
- **E-mail**
  This is only completely secure if the message is encrypted.
- **Paper copies**
  These are only secure when kept under lock and key.
- **Post**
  This is only secure if using a tamper-evident envelope preferably inside another envelope
- **Verbal Exchange**
  This is only secure if it is not repeated to unauthorised Personnel

Always choose the most secure and confidential route of exchange available to you- think through all these methods before you use one.

2.2 Keeping Information Securely

Once we have exchanged the information, we have o be careful how it is stored. Information can be stored in two ways:

i. Manually (paperwork)
ii. Electronically (documents created on a computer, e-mail)

We need to ensure that certain checks are made depending on how the information is stored.

i. Manual (non-electronic) data

You are advised to:

- Regularly **review** the need for keeping the data
- Keep it **secure** (preferably locked)
- Keep it **out of sight**
- Keep it **organised**
- Mark it **'restricted'** or **'confidential'**
- **Dispose** of it wisely
- Take **responsibility** for it

ii. Electronic Data

You are advised to:

- Regularly **review** the need for keeping the data
- Use a password-protected **screen-saver** – activate it when you leave your desk
- Use document **passwords** – but make sure you remember what they are!
- Take **responsibility** for it

This means that we must ensure that we are balancing individual rights against the general interests of the community. Information can, therefore, be exchanged, but we must be careful that our intervention is only proportional to the scale of the problem.

The Data Protection Act 1998 exists to regulate the use of personal data with the purpose of protecting the rights and freedom of the individual.

Sharing personalised information within these guidelines

Current legislation means that we need to be careful when we share personalised information. In order to comply with the guidelines set down for us, you will need to be able to tick every one of these boxes before you share personalised information.

1. There are valid reasons for needing data
2. The exchange represents a "pressing social need" i.e. the threat to the Public is sufficient to warrant interference in the subject's rights
3. The data will only be used for these reasons and not for an unrelated purpose
4. The data is all relevant, appropriate and useful
5. The data is accurate and up-to-date
6. The data will not be kept for longer than necessary
7. The data are kept safe and confidential
8. The data are shared between the correct agencies
9. The data will be kept within the geographical are governed by these rules for data protection

IN OTHER WORDS ... you must be sure that your agency is fully compliant with the Data Protection Act 1998. This involves registration under purpose PO58 (Data Protection Act 1998) or "for the purposes of crime prevention and prosecution of offenders" (Data Protection Act 1998). For further guidance please refer to the " notification handbook – a complete guide to notification", issued by the data protection commissioners office www.dataprotection.gov.uk).