Jersey Child Protection Committee

PROTOCOL FOR INFORMATION EXCHANGE BETWEEN STATES DEPARTMENTS

1. Parties/Signatories

Chief Officers	States of Jersey Police
	Health and Social Services
	Education, Sport and Culture
	Probation and After Care Service
	Housing
Governor	HM Prison La Moye
Chief Executive Officer	Family Nursing and Home Care

Other States departments and voluntary agencies may also become signatories to the protocol where this is necessary or expedient to the purpose set out in 2. The Jersey Child Protection Committee, though not a legally constituted body and therefore not a signatory, has a role is monitoring inter-agency child protection work and is recognised as having an interest in the protocol and proposed amendments.

It will be the responsibility of these signatories to ensure that:

- realistic expectations prevail from the outset;
- ethical standards are maintained;
- a mechanism exists by which the flow of information can be controlled;
- appropriate training is provided;
- adequate arrangements exist to test adherence to the protocol.

2. Purpose

The purpose of this protocol is to facilitate the exchange of information in order to safeguard the welfare of children or vulnerable adults, including victims of Domestic Violence.

This protocol will also provide the basis to facilitate information exchange relating to the role of the Serious Cases Sub-Committee. In this respect each signatory to this protocol will undertake to protect the confidentiality and security of all shared information by adopting best practice principles and ensuring compliance with Data Protection and Human Rights legislation.

3. Introduction

The signatories subscribe to the following for this protocol:

- the agreed standards must provide safeguards and an appropriate framework for the controlled exchange of relevant information;
- the Data Protection principles must be upheld (The principles are outlined at **Appendix A**);
- this protocol to be reviewed annually or following any change requested to the protocol;
- any partner may request any change to the protocol at any time by submitting to the protocol holder a suggested revision; any changes to be discussed and agreed by the JCPC;
- the nominated holder of this protocol is the Information Compliance and Security Manager, States of Jersey Police.

4. Definitions

For the purpose of this protocol:

“Personal data” is information that relates to a living individual that can be identified from those data, or from those data and other information which is likely to come into the possession of the data controller. It includes any expression of opinion or intentions in respect of the individual.

“De-personalised data” means information where an individual cannot be identified, for example by using information such as the first group and only the 1st character of second group of a post code such as BS20 9--.

“Data controller” means a person who (either alone or jointly or in common with other persons) determines the purpose for which and the manner in which any personal data are, or are to be, processed.

“Child” means a person who has not yet attained the age of majority (18yrs) (and includes young adults who were looked after and continue to receive a service).

“Vulnerable Adult” includes elderly people and adults with a physical or learning disability, or who have mental health problems.

"Victim of Domestic Violence" means a person who has come to the attention of any of the partners to the protocol following any incident of threatening behaviour, violence or abuse (psychological, physical, sexual, financial or emotional) between adults, aged 18yrs or over, who are or have been intimate partners or family members, regardless of gender and sexuality.

5. Information Exchange

Disclosure of any personal data must be bound to both common and statute law and professional ethics and codes of conduct.

The data protection principles require that such information is obtained and processed fairly and lawfully; is only disclosed in appropriate circumstances and for the purpose(s) it was obtained; is accurate, relevant, and not held longer than necessary; and is kept securely.

The European Convention on Human Rights (ECHR) requires all domestic law to 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. Should a public authority fail to do this then it may be subject of a legal action under section 7. This obligation should not solely be seen in terms of an obligation not to violate Convention Rights but also as a positive obligation to uphold these rights.

The sharing of information between agencies has the potential to infringe a number of Convention Rights, in particular, Article 8 (Right to private and family life), and 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 (Prohibition of Discrimination).

The Convention does allow limited interference with certain Convention rights by public authorities under broadly defined circumstances known as legitimate aims. However, mere reliance on a legal power may not alone provide sufficient justification and the following principles should be considered:

- Is there a legal basis for the action being taken?
- Does it pursue a legitimate aim (as outlined in the particular Convention article)?
- Is the action taken proportionate and the least intrusive method of achieving that aim?

A brief summary of the Articles of the Human Rights Act 1998 is attached at **Appendix B.** Article 8 is covered in more detail at 5.2 (d) but other articles may apply in specific circumstances.

5.1 De-personalised Data

De-personalised data should be used unless the purpose could not be achieved by this means alone.

Any personal data exchanged should be protected and secured, by all parties, in accordance with this protocol.

5.2 Personal Data - Power to Disclose and Conditions for Processing (Appendix C)

If failure to share personal information means that the purpose of this protocol could not be achieved, each party must carefully consider each of the following prior to making any decision:

a) Consent

Many of the data protection issues surrounding the disclosure can be avoided if the informed consent of the individual has been sought and obtained. Consent must be freely given after the alternatives and consequences are made clear to the person from whom permission is being sought. If the data is classified as sensitive data the consent must be explicit.

In any case the specific detail of the processing should be explained to the individual. This should include:

- precisely who is processing the data;
- the particular types of data to be processed;
- the purpose of the processing;
- any special aspects of the processing which may affect the individual, e.g. disclosures;
- the persons/agencies to whom the information will be made available

In the absence of consent, the nominated officer must balance the duty of care and the public duty of confidentiality against the need to prevent and detect crime and disorder, and serve the public interest, in order to make a positive decision whether or not to release the information.

b) Vital Interests

i. The processing is necessary in order to protect the vital interests of the data subject or another person, in a case where consent cannot be given by or on behalf of the data subject, or the data controller cannot reasonably be expected to obtain the consent of the data subject; or

ii. in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.

c) Public Functions

If informed consent has not been sought, or sought and withheld, the partner must consider if there is any other overriding factor for the justification for the disclosure. In making this decision the following should be considered:

- Is the disclosure necessary for the prevention or detection of crime, prevention of disorder, to protect public safety, or to protect the freedoms of others?
- Is the disclosure necessary for the protection of a child or young person or a vulnerable adult?
- What risk to others is posed by this individual?
- What is the vulnerability of those who may be at risk?
- What will be the impact of the disclosure on the subject and on others?
- Is the disclosure proportionate to the intended aim?
- Is there an equally effective but less intrusive alternative means of achieving that aim?

d) Human Rights - Article 8

Article 8 of the Human Rights Act 1998 states that everyone has the right to respect for his private and family life, his home and his correspondence and that there shall be no interference by a public authority with this right except as in accordance with the law, in particular: -

- public safety;
- the prevention of crime or disorder;
- the protection of health or morals;
- the protection of the rights or freedoms of others.

e) The professional codes of ethics of the person proposing to disclose the information

If consent is not sought, or sought and not obtained, or only partially obtained, the reasons for not seeking consent or otherwise breaching confidentiality must be recorded and explained to the subject as soon as this can be done without negating the purpose for which consent was originally not sought originally.

5.3 Extent of Personal Data Disclosed

Disclosure of personal data must be relevant and the minimum amount required for the purpose.

The identity of the originator must be recorded against the relevant data. No secondary use or other use may be made unless the consent of the disclosing party to that secondary use is sought and granted. Disclosure must be compatible with the second data protection principle: 'Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes'.

5.3.1 Proportionality

The principle of 'proportionality' is a common theme running through both the Convention rights and judgements of the European Court. It is explicitly expressed in the limitations contained in Articles 8 - 11 where it is stated that any interference or restriction of those rights must be lawful and 'necessary in a democratic society'. Any restriction of rights must, therefore, be justified in that a fair balance must be achieved between the protection of an individual's rights with the general interests of society. In the context of information exchange, any disclosure of information should be restricted to a minimum and be the least damaging that is required in achieving the objective.

5.4 Review and Weeding of Data

One of the principles within the data protection legislation states that excessive data must not be retained for longer than is necessary to fulfil the purpose for which is was originally obtained. It follows that information must be removed as soon as it is no longer required for the original purpose for which it was supplied or collected.

Therefore, retention should be for the minimum period required to achieve the objectives of the disclosure after which the data will be returned to the originator or destroyed as agreed.

5.5 Data Quality

Information discovered to be inaccurate or inadequate for the purpose will be notified to the data owner who will be responsible for correcting the data and notifying all other recipients of the data who must ensure that the correction is made.

5.6 Designated Officers

Each partner (signatories) to this protocol must designate someone within their organisation to assume responsibility for data protection (including notification if appropriate); security and confidentiality; and compliance with legislation, e.g. by undertaking audits, point of contact for Subject Access Requests.

5.7 Requesting /disclosing personal information

Each partner shall complete (and thereafter maintain) **Appendix D** and submit to the nominated protocol holder for circulation to all other partners, a list of key staff:

- to whom requests for information should be sent;
- to whom disclosures should be made;

- with whom contact should be made in relation to this protocol;
- who are responsible for data protection and security.

Requests from unauthorised organisations/staff will be declined.

This information will provide evidence if the disclosure is challenged or formal complaint is made. Clear records of the evidence provided by various partners will be required to justify any challenges of the proportionality of the action taken. Care should be taken when any request for disclosure emanates from private, commercial or unprecedented sources, in which, case reference must be made to designated Data Protection Officers.

5.7.1 Case Conferences

Child Protection or adult protection conferences and professionals' meetings may be held when deemed necessary by all partners, following *Working Together* and other protocols in use by States employees. Information exchanged at such a meeting will be minuted and given in accordance with the confidentiality agreement at **Appendix E**, which must be noted by all present prior to the commencement of the meeting. Personal data should not be made available unless the consent of the subject has been obtained, or the reasons why this is not possible or not appropriate (see 5.2 and 5.3) are recorded and explained to the conference/meeting.

6. Security

All partners must ensure that a baseline level of security is in place to ensure compliance with principle 7 of the Data Protection Law 2005 and should be proportionate to the data held.

7. Complaints and Breaches

Any complaint made will be brought to the attention of the nominated officer of the relevant partner(s), and they will be dealt with in accordance with their own policies and procedures. Partners will keep each other informed of developments following a complaint received, where relevant. Complaints about inappropriate disclosure of confidential information within multi-agency child protection processes monitored by the Jersey Child Protection Committee should be considered initially by the Serious Cases sub-committee of the JCPC, and a decision taken as to whether the complaint should be investigated by that sub-committee or by the agency of the professional alleged to have acted contrary to this Protocol.

8. Requests for Information

8.1 Subject Access Requests

All requests for information under the subject access provisions of the Data Protection Law 2005 will be dealt with by the person responsible for Data Protection within the organisation. If personal data is identified as belonging to another partner, it will be the responsibility of the receiving partner to contact the Data Protection Officer for the originating partner to determine whether the latter wishes to claim an exemption under the provisions of the Data Protection Law.

Where a data controller cannot comply with the request without disclosing information relating to a named individual who can be identified from that information, he is not obliged to comply with the request unless:

a) any named individual has consented to the disclosure of the information to the person making the request, or

b) it is reasonable in all the circumstances to comply with the request without the consent of a specified individual. In determining whether it is reasonable, regard shall be had, in particular, to:

    - any duty of confidentiality owed to the specified individuals;
    - any steps taken by the data controller with a view to seeking the consent of the specified individuals;
    - whether the specified individual/s is/are capable of giving consent;
    - any express refusal of consent by the other individual.

- *The request should not be declined simply if consent from a third party is not forthcoming. It may be possible to anonymised data or still provide other information requested provided the individual is protected.*

8.2 Freedom of Information

Requests for personal information under the Code of Practice on Public Access to Official Information will be dealt with under code.

9. Training

Each partner is responsible for ensuring that appropriate members of staff are adequately trained in respect of all matters covered in this protocol.

10. Indemnity

Each partner shall be fully indemnified by the other partners in accordance with the indemnity contained in **Appendix F**.

11. Confidentiality

Each partner shall at all times keep confidential all personal data supplied pursuant to this agreement. This clause shall survive termination of the agreement or the withdrawal of or removal of any partner. This means that no publication of data supplied pursuant to this agreement will identify any individual.

12. Signatures

By signing this document the participants accept and will adopt the statements included in this protocol and the indemnity, and agree to maintain the specified standards. In addition, the partners will not use, release or otherwise disclose any information whatsoever:

- for any other secondary use not specified by the document
- to any organisation which is not a signatory to this protocol.

Signed on behalf of: -

Name of organisation and address:
States Of Jersey Police
Police Headquarters
Rouge Bouillon
St Helier
JERSEY
JE2 3ZA

Name/Position/Job title:
David Warcup
Chief Police Officer

Signature:

Dated this [ ] day of [ ] 2009

Signed on behalf of: -

Name of organisation and address:
Health and Social Services
Peter Crill House
Gloucester Street
St Helier
Jersey JE1 3QS

Name/Position/Job title:
Mike Pollard
Chief Executive

Signature:

Dated this [ ] day of [ ] 2009

Signed on behalf of: -

Name of organisation and address:
Education, Sport and Culture
Highlands Campus
Jersey
JE4 8QJ

Name/Position/Job title:
Mario Lundy
Chief Executive

Signature:

Dated this [ ] day of [ ] 2009

Signed on behalf of: -

Name of organisation and address:
Probation and After Care Service
1 Lemprière Street
St Helier
Jersey
JE4 8YT

Name/Position/Job title:
Brian Heath
Chief Probation Officer

Signature:

Dated this [ ] day of [ ] 2009

Signed on behalf of: -

Name of organisation and address:
Housing
Jubilee Wharf
24 Esplanade
St Helier
Jersey
JE4 8XT

Name/Position/Job title:
Ian Gallichan
Chief Officer

Signature:

Dated this [ ] day of [ ] 2009

Signed on behalf of: -

Name of organisation and address:
HM Prison La Moye
La Rue Baal
St. Brelade
Jersey
JE3 8HQ

Name/Position/Job title:
Bill Millar
Governor

Signature:

Dated this [ ] day of [ ] 2009

Signed on behalf of: -

Name of organisation and address:
Family Nursing & Home Care
Le Bas Centre
St Saviour's Road
St Helier
JE2 4RP

Name/Position/Job title:
Pamela Massey
Chief Executive

Signature:

Dated this [ ] day of [ ] 2009

Signed on behalf of: -

Name of organisation and address:
Jersey Child Protection Committee

Name/Position/Job title:
Mike Taylor
Independent Chair

Signature:

Dated this [ ] day of [ ] 2009

Appendix A

DATA PROTECTION LAW 2005

SCHEDULE 1 (Article 4(1))

PART 1

THE DATA PROTECTION PRINCIPLES

1. First principle

Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –

a) in every case – at least one of the conditions set out in paragraphs 1-6 of Schedule 2 is met; and

b) in the case of sensitive personal data – at least one of the conditions in paragraphs 1-10 of Schedule 3 is also met.

2. Second principle

Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Third principle

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Fourth principle

Personal data shall be accurate and, where necessary, kept up to date.

5. Fifth principle

Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Sixth principle

Personal data shall be processed in accordance with the rights of data subjects under this Law.

7. Seventh principle

Appropriate technical and organisational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Eighth principle

Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Appendix B

HUMAN RIGHTS

Article 2 - Right to Life

Everyone's right to life shall be protected by law

Article 3 - Prohibition of Torture, Inhuman or Degrading Treatment

No one shall be subjected to torture or to inhuman or degrading treatment or punishment.

Article 4 - Prohibition of Slavery and Forced Labour

No one shall be held in slavery or servitude.

No one shall be required to perform forced or compulsory labour.

Article 5 - Right to Liberty and Security

Everyone has the right to liberty and security of person.

Article 6 - Right to a Fair Trial

In the determination of his civil rights and obligations or of any criminal charge against him, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law.

Article 7 - No Punishment Without Law

No one shall be held guilty of any criminal offence on account of any act or omission which did not constitute a criminal offence under national or international law at the time when it was committed.

Article 8 - Right to Respect for Private and Family Life

Everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law.

Article 9 - Freedom of Thought, Conscience and Religion

Everyone has the right to freedom of thought, conscience and religion.

Article 10 - Freedom of Expression

Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.

Article 11 - Freedom of Assembly

Everyone has the right to freedom of association with others, including the right to form and to join trade unions for the protection of his interests.

Article 12 - Right to Marry

Men and Women of marriageable age have the right to marry and to found a family, according to their national laws governing the exercise of this right.

Article 14 - Prohibition of Discrimination

The enjoyment of the rights and freedoms set forth in this Convention shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status.

Article 16 - Restriction on the Political Activity of Aliens

Nothing in articles 10, 11 and 14 shall be regarded as preventing the High Contracting Parties from imposing restrictions on the political activity of aliens.

Article 17 - Prohibition of Abuse of Rights

Nothing in this Convention may be interpreted as implying for any State, group or person any right to engage in any activity or perform any act aimed at the destruction of any of the rights and freedoms set forth herein or at their limitation to a greater extent than is provided for in the Convention.

Article 18 - Limitation on use of Restrictions on Rights

The restrictions permitted render this Convention to tire-said rights and freedoms shall not be applied for any purpose other than those for which they have been prescribed.

The First Protocol

Article 1 - Protection of Property

Every natural or legal person is entitled to the peaceful enjoyment of his possessions.

Article 2 - Right to Education (subject to UK reservation)

No person shall be denied the right to education.

Article 3 - Right to Free Elections

The High Contracting Parties undertake to hold free elections at reasonable intervals by secret ballot

The Sixth Protocol

Article 1 - Abolition of Death Penalty

The death penalty shall be abolished. No one shall be condemned to such penalty or executed.

Article 2 - Death penalty in Time of War

A State may make provision in its law for the death penalty in respect of acts committed in time of war or imminent threat of war.

Appendix C

DATA PROTECTION LAW 2005

SCHEDULE 2

(Article 4(3) and Schedule 1 Part 1, paragraph 1(a))

FIRST PRINCIPLE: CONDITIONS FOR PROCESSING OF ANY PERSONAL DATA

1. Consent

The data subject has consented to the processing.

2. Processing necessary for contract

The processing is necessary for –

a) the performance of a contract to which the data subject is a party; or

b) the taking of steps at the request of the data subject with a view to entering into a contract.

3. Processing under legal obligation

The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.

4. Processing to protect vital interests

The processing is necessary in order to protect the vital interests of the data subject.

5. Processing necessary for exercise of public functions

The processing is necessary for –

a) the administration of justice;

b) the exercise of any functions conferred on any person by or under any enactment;

c) the exercise of any functions of the Crown, the States or any public authority; or

d) the exercise of any other functions of a public nature exercised in the public interest by any person.

6. Processing for legitimate interests

The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except if the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

7. Regulations about legitimate interests

The States may by Regulations specify particular circumstances in which the condition set out in paragraph 6 is, or is not, to be taken to be satisfied.

SCHEDULE 3

(Article 4(3) and Schedule 1 Part 1, paragraph 1(b))

FIRST PRINCIPLE: CONDITIONS FOR PROCESSING OF SENSITIVE PERSONAL DATA

1. Consent

The data subject has given explicit consent to the processing of the personal data.

2. Employment

The processing is necessary for the purposes of exercising or performing any right, or obligation, conferred or imposed by law on the data controller in connection with employment.

3. Vital interests

The processing is necessary –

a) in order to protect the vital interests of the data subject or another person, in a case where consent cannot be given by or on behalf of the data subject, or the data controller cannot reasonably be expected to obtain the consent of the data subject; or

b) in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.

4. Non-profit associations

The processing –

a) is carried out in the course of its legitimate activities by any body, or association, that is not established or conducted for profit, and exists for political, philosophical, religious or trade-union purposes;

b) is carried out with appropriate safeguards for the rights and freedoms of data subjects;

c) relates only to individuals who are members of the body or association or have regular contact with it in connection with its purposes; and

d) does not involve disclosure of the personal data to a third party without the consent of the data subject.

5. Data subject has made information public

The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.

6. Legal proceedings etc.

The processing –

a) is necessary for the purpose of, or in connection with, any legal proceedings;

b) is necessary for the purpose of obtaining legal advice; or

c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

7. Public functions

The processing is necessary for –

a) the administration of justice;

b) the exercise of any functions conferred on any person by or under an enactment; or

c) the exercise of any functions of the Crown, the States, any administration of the States or any public authority.

8. Medical purposes

1) The processing is necessary for medical purposes and is undertaken by –

   a) a health professional; or

   b) a person who in the circumstances owes a duty of confidentiality equivalent to that which would arise if that person were a health professional.

2) In this paragraph "medical purposes" includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment, and the management of healthcare services.

9. Equal opportunity research

The processing –

a) is of sensitive personal data consisting of information as to racial or ethnic origin;

b) is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained; and

c) is carried out with appropriate safeguards for the rights and freedoms of data subjects.

10. Circumstances prescribed by Regulations

The personal data are processed in such circumstances as may be prescribed by Regulations.

11. Regulations about paragraph 2, 7 or 9

1) The States may by Regulations –

   a) exclude the application of paragraph 2 or 7 in such cases as may be specified; or

   b) provide that, in such cases as may be specified, the condition in paragraph 2 or 7 is not to be regarded as satisfied unless such further conditions as may be specified in the Regulations are also satisfied.

2) The States may by Regulations specify circumstances in which processing falling within paragraph 9(a) and (b) is, or is not, to be taken for the purposes of paragraph 9(c) to be carried out with appropriate safeguards for the rights and freedoms of data subjects.

Appendix D

Name of Signatory:

Protocol for Data Sharing

The Signatory:	

Requests documents to be sent to: (Note: Specify individual departments if necessary)	**Disclosures to be made to:**	**Responsibility for Data Protection and Security**

.

1. Disclosure will be actioned by staff listed on the above list in response to requests in writing.

2. Disclosure via fax to a secure listed fax number will be the preferred method of the delivery of the requested information. This will ensure that accurate information is passed direct to the person requesting information, and that an audit trail is established. Alternatively disclosure may be may be by telephone in the first instance, but must be followed up by a confirmation fax.

3. Due to the insecure nature of the internet no personal data to be shared under this protocol is to be supplied via e-mail. Secure fax [a fax in the office of the contact person] must be used.

4. The Signatories should respond to formal requests for Disclosure of Personal Data within forty-eight [48] hours of receipt of the request. However, it is acknowledged that there may be occasions when the Disclosure is required more urgently.

Appendix E

Confidentiality Statement

To enable the exchange of information between attendees at this meeting to be carried out in accordance with the Data Protection Law 2005, the European Convention on Human Rights and the common law duty of confidentiality, all attendees are asked to agree to the following.

This agreement will be recorded in the minutes.

1. Information can be exchanged within this meeting for the purpose of identifying any action that can be taken by any of the agencies or departments attending this meeting to resolve the problem under discussion.

2. A disclosure of information outside the meeting, beyond that agreed at the meeting, will be considered a breach of the individuals' confidentiality and a breach of the confidentiality of the partners involved.

3. All documents exchanged should be marked 'confidential – not to be disclosed without consent'. All minutes, documents and notes of disclosed information should be kept in a secure location to prevent unauthorised access.

4. Personal data should not be made available unless the consent of the subject has been obtained, or the reasons why this is not possible or not appropriate are recorded and explained to the conference (see paragraph 5.2 of Protocol for Information Exchange for issues to be considered when deciding that data subject consent need not be obtained/ can be dispensed with).

Appendix F

FORM OF INDEMNITY

1. In consideration of the provision of information in accordance with (insert details of agreement or arrangement under which information is to be supported, and insert name of authority granting indemnity) undertakes to indemnify any of the signatories against any liability which may be incurred by such person or authority as a result of the provision of such information.

Provided that this indemnity shall not apply:

a) where the liability arises from information supplied which is shown to have been incomplete or incorrect, unless the person or authority claiming the benefit of this indemnity establishes that the error did not result from any wilful wrongdoing or negligence on its part or on the part of any other signatory.

b) unless the person claiming the benefit of this indemnity notifies (insert name of authority granting indemnity) as soon as possible of any action, claim or demand to which this indemnity applies, permits (insert name or authority granting indemnity) to deal with the action, claim or demand by settlement or otherwise and renders (insert name of authority granting indemnity) all reasonable assistance in so dealing.

c) to the extent that the person or authority claiming the benefit of the indemnity makes any admission which may be prejudicial to the defence of the action, claim or demand.