

**GENERAL PROTOCOL
FOR SHARING INFORMATION
BETWEEN AGENCIES**

IN

**KINGSTON UPON HULL
AND
THE EAST RIDING OF
YORKSHIRE**

2008

CONTENTS

1. INTRODUCTION	
Purpose of this document	1-6
2. KEY LEGISLATION AND GUIDANCE	
The Data Protection Act 1998 – Introduction	7
The Data Protection Act Principles	8
The Lawful Use of Information	9-14
Individuals’ Rights under the Act	15
Individuals’ Rights of Access to Information	16
The Common Law Duty of Confidentiality	17-18
The Human Rights Act 1998	19-20
The Crime & Disorder Act 1998	21
Learning and Skills Act	22-23
The Childrens Act 2004	24-26
The Mental Capacity Act 2005	27-30
3. PRINCIPLES GOVERNING THE SHARING OF INFORMATION	31-45
4. PROCEDURES FOR THE DISCLOSURE OF PERSONAL INFORMATION	
Obtaining Consent	46-53
Lack of Capacity to Consent	54-57
Lasting Power of Attorney and Deputies appointed by the Court of Protection	58-59
Independent Mental Capacity Advocate	60
Children	61
Disclosure without Consent	62-65
5. ACCESS AND SECURITY PROCEDURES	66-68
6. MONITORING AND REVIEWING PROCEDURES	69-75
7. PARTNERSHIP UNDERTAKING	76-78
APPENDIX A	
Parties to the Protocol	
APPENDIX B	
Operation Procedures for Information Sharing Template	

SECTION ONE: INTRODUCTION

Purpose of this document

- 1 This document is the information sharing protocol for public agencies working in Kingston upon Hull and the East Riding of Yorkshire. It provides guidance for sharing personalised information between these agencies, which are listed at in Appendix A.
- 2 The protocol has three main aims:
 - To provide and establish the principles of information sharing between public organisations and other agencies with whom there are SLAs or contracts in place
 - To form a base line for the development of detailed protocols referred to as operational procedures required for specific projects, initiatives or issues
 - To commit parties to an agreed set of minimum standards for information sharing
- 6 It is accepted from practice, experience and research that the sharing of information between professionals helps to ensure that adults and children receive the care, services, protection and support they need. Sharing personal information between partner agencies is vital to the provision of co-ordinated and seamless care and services to individuals. In addition the sharing of information can help achieve statutory and local initiatives for example those designed to prevent crime and disorder. Legislation does not prevent the sharing of information between agencies delivering services, although there are important rules and safeguards to be observed.
- 4 All professionals who are party to this agreement accept their continuing obligation to comply with their professional codes of conduct.
- 5 All agencies must be clear about what information they are required to share and in what circumstances and to assist in this it is expected operational procedures specific to particular purposes or initiatives are created using the template provided in appendix B as a guide. However, all agencies that are party to this general protocol agree to ensure that individual protocols are compliant and consistent with this document.
- 6 Public organisations may work in partnership with non public organisations

such as private, charity or voluntary, and these arrangements will be documented by further signed written agreements (SLA, contracts or protocols).



SECTION TWO: KEY LEGISLATION AND GUIDANCE

The Data Protection Act 1998 - Introduction

- 7 The key legislation governing the obtaining, protection and use of identifiable personal information is the Data Protection Act 1998 (The DPA). The DPA does not apply to information relating to the deceased, however the parties to the protocol will seek to apply the principles to all personal information they hold.

The Data Protection Act Principles

- 8 The DPA sets out eight principles which must be complied with when obtaining and using personal data. These principles are as follows:

First Principle

Obtain and process personal data fairly and lawfully.

Second Principle

Hold data only for the lawful and specified purposes.

Third Principle

Personal data shall be adequate, relevant and not excessive in relation to the purposes for which it is processed.

Fourth Principle

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

Fifth Principle

Hold data for no longer than necessary.

Sixth Principle

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

Seventh Principle

Measures should be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction or damage to personal data.

Eighth Principle

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

The use of personal information by agencies must therefore comply with these principles.

The Lawful Use of Information

- 9 When sharing information, compliance with the first DPA principle is crucial to ensuring the sharing of information is carried out lawfully.
- 10 To ensure personal information is processed in a lawful manner, one of several specified conditions, which are set out in Schedule 2 of the DPA , must be complied with. These conditions are as follows:
 - The individual has given his/her consent to the processing;
 - The processing is necessary to comply with a legal obligation;
 - The processing is necessary to carry out public functions;
 - The processing is necessary in order to protect the vital interest of the individual (this is envisaged to be a life and death scenario);
 - The processing is necessary in order to pursue the legitimate interest of the organisation or certain third parties (unless prejudicial to the interests of the individual);
 - The processing is necessary for the entering into a contract at the request of the individual or performance of a contract to which the individual is a party.
- 11 Therefore, as a general rule, if one of the above conditions is satisfied, the processing of information is likely to be lawful. However, if the information to be processed is what is described as “sensitive personal data”, then there are extra conditions that must be satisfied before the processing of information is lawful.
- 12 Sensitive personal data is information as to:
 - The racial or ethnic origin of the individual;
 - Their political opinions;
 - Their religious beliefs or beliefs of a similar nature;
 - Whether they are a member of a trade union;
 - Their physical or mental health or condition;

- Their sexual life;
- The commission or alleged commission by them of any offence;
- Any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any Court in such proceedings.

13 Should the information processed contain sensitive personal data, then one of the following conditions contained in Schedule 3 of The DPA, must be satisfied (as well as a condition from schedule 2 above) before processing that information. The main conditions are as follows:

- That the individual has given their explicit consent to the processing of the personal information;
- That the processing is necessary to perform any legal right or obligations imposed on the organisation in connection with employment;
- The processing is necessary to protect the vital interests of the individual or another person, where consent cannot be given by the individual, or the organisation cannot be reasonably expected to obtain consent or consent is being unreasonably withheld where it is necessary to protect the vital interests of another;
- The information contained in the personal information has been made public as a result of steps deliberately taken by the individual;
- The processing is necessary in connection with legal proceedings, dealings with legal rights or taking legal advice;
- The processing is necessary for the administration of justice or carrying out legal or public functions;
- The processing is necessary for medical purposes;

14 Where information is given to professionals in confidence, then in addition the common law duty of confidentiality must also be considered. This is summarised at paragraph 16 below.

Individuals' Rights under the Act

15 The DPA gives seven rights to individuals in respect of their own personal data held by others. They are:

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

Individuals' Rights of Access to Information

- 16 Subject to certain exceptions, any living person who is the subject of information held and processed by an organisation has a right of access to that information. Where access is refused, the individual may appeal. There are certain statutory exemptions which may limit access rights. These include for example where access would prejudice the prevention or detection of crime.

The Common Law Duty of Confidentiality

- 17 Information has a necessary quality of confidence when it is of a confidential character. This does not mean that the information need be particularly sensitive, but simply that it must not be publicly or generally available. Information is not confidential if it is in the public domain. To decide whether an obligation of confidence exists, the following must be considered:
- Whether the information has a necessary quality of confidence;
 - Whether the circumstances of the disclosure have imposed an obligation on the confidant to respect the confidence. This usually means considering whether the information was imparted for a limited purpose.
- 18 As a general rule confidential information should not be disclosed without the consent of the subject. However, the law permits the disclosure of confidential information where there is an overriding public interest or justification for doing so. Examples of this might be child protection or the protection of vulnerable adults or the prevention and detection of crime or public safety.

The Human Rights Act 1998

- 19 Article 8(1) provides that:

Everyone has the right to respect for his private and family life, his home and his correspondence.

However, this is a qualified right and Article 8 (2) states that:

There should be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interest of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and

freedoms of others.

- 20 Therefore, disclosure of information will need to take Article 8 into consideration. The sharing of information may be necessary, for example, for the protection of health or morals, for the prevention of the rights and freedoms of others or for the prevention of disorder or crime.

The Crime and Disorder Act 1998

- 21 This Act was introduced to provide measures to prevent crime and disorder and anti-social behaviour in the community. Section 115 of the Act provides that any person can lawfully disclose information, where necessary or expedient for the purposes of any provision of the Act, to a chief officer of police, a police authority, a local authority, a probation service or a health authority, even if they do not otherwise have this power. This power also covers disclosure to people acting on behalf of any of the named bodies. The “purposes” of the Act include a range of measures such as local crime audits, youth offending teams, anti-social behaviour orders, sex offender orders and local child curfew schemes. However, the use of Section 115 must be considered on a case by case basis, and must still be compliant with the principles of the DPA.

Section 17 Duty to consider crime and disorder implications

- (1) Without prejudice to any other obligation imposed on it, it shall be the duty of each authority to which this section applies to exercise its various functions with due regard to the likely effect of the exercise of those functions on, and the need to do all that it reasonably can to prevent, crime and disorder in its area.
- (2) This section applies to a local authority, a joint authority, a police authority, a National Park authority and the Broads Authority.

The Learning and Skills Act 2000

22 Section 114

- (1) The Secretary of State may provide or secure the provision of services which he thinks will encourage, enable or assist (directly or indirectly) effective participation by young persons (13 – 19 year olds) in education or training.

23 Section 120

- (1) For the purpose of the provision of services in pursuance of section

114(1), any of the persons or bodies mentioned in subsection (2) may supply information about a young person:

- (a) to the Secretary of State,
- (b) to any other person or body involved in the provision of those services.

(2) Those persons and bodies are:

- (a) a local authority,
- (b) a Health Authority,
- (c) the Learning and Skills Council for England,
- (d) a chief officer of police,
- (e) a probation committee,
- (f) a youth offending team, and
- (g) a Primary Care Trust.

The Childrens Act 2004

(This is the legislation under which the Contact Point database is to be established.)

24 Section 10 Co-operation to improve well-being

(1) Each children's services authority in England must make arrangements to promote co-operation between

- (a) the authority;
- (b) each of the authority's relevant partners; and
- (c) such other persons or bodies as the authority consider appropriate, being persons or bodies of any nature who exercise functions or are engaged in activities in relation to children in the authority's area.

(2) The arrangements are to be made with a view to improving the well-being of children in the authority's area so far as relating to—

- (a) physical and mental health and emotional well-being;
- (b) protection from harm and neglect;
- (c) education, training and recreation;
- (d) the contribution made by them to society;
- (e) social and economic well-being.

25 Section 11 Arrangements to safeguard and promote welfare

(1) This section applies to each of the following—

- (a) a children's services authority in England;
 - (b) a district council which is not such an authority;
 - (c) a Strategic Health Authority;
 - (d) a Special Health Authority, so far as exercising functions in relation to England, designated by order made by the Secretary of State for the purposes of this section;
 - (e) a Primary Care Trust;
 - (f) an NHS trust all or most of whose hospitals, establishments and facilities are situated in England;
 - (g) an NHS foundation trust;
 - (h) the police authority and chief officer of police for a police area in England;
 - (i) the British Transport Police Authority, so far as exercising functions in relation to England;
 - (j) a local probation board for an area in England;
 - (k) a youth offending team for an area in England;
 - (l) the governor of a prison or secure training centre in England (or, in the case of a contracted out prison or secure training centre, its director);
 - (m) any person to the extent that he is providing services under section 114 of the Learning and Skills Act 2000.
- (2) Each person and body to whom this section applies must make arrangements for ensuring that—
- (a) their functions are discharged having regard to the need to safeguard and promote the welfare of children; and
 - (b) any services provided by another person pursuant to arrangements made by the person or body in the discharge of their functions are provided having regard to that need.

26 Section 12 Information databases

- (1) The Secretary of State may for the purpose of arrangements under section 10 or 11 above or under section 175 of the Education Act 2002—
- (a) by regulations require children's services authorities in England to establish and operate databases containing information in respect of persons to whom such arrangements relate;
- (4) The information referred to in subsection (3) is information of the following descriptions in relation to a person—
- (a) his name, address, gender and date of birth;
 - (b) a number identifying him;

(c) the name and contact details of any person with parental responsibility for him (within the meaning of section 3 of the Children Act 1989)or who has care of him at any time;

(d) details of any education being received by him (including the name and contact details of any educational institution attended by him);

(e) the name and contact details of any person providing primary medical services in relation to him under Part 1 of the National Health Service Act 1977 (c. 49);

(f) the name and contact details of any person providing to him services of such description as the Secretary of State may by regulations specify;

(g) information as to the existence of any cause for concern in relation to him;

(h) information of such other description, not including medical records or other personal records, as the Secretary of State may by regulations specify.

The Mental Capacity Act 2005

Chapter 9

- 27 The Mental Capacity Act 2005 provides a statutory framework to empower and protect vulnerable people who may not be able to make their own decisions. It makes it clear who can take decisions in which situations and how they should go about this. It enables people to plan ahead for a time when they may lose capacity.
- 28 The Act replaces existing common law governing the treatment of people without capacity and covers a range of choices from day-to day decisions such as what to wear or eat, through to decisions about where to live, medical treatment, finances and property.
- 29 The Act makes provision for the appointment of Lasting Power of Attorney, a Deputy appointed by the Court of Protection or an Independent Mental Capacity Advocate.
- 30 This Act is supported by the 'Mental Capacity Act 2005 Code of Practice'. Which those working in a professional or any paid role have a legal duty 'to have regard' to. You must explain any non-compliance with this Code and record the reasons at the same time as you make the decision not to follow the Code

SECTION THREE: PRINCIPLES GOVERNING THE SHARING OF INFORMATION

- 31 The agencies who are party to this document recognise that they work in a multi-agency environment and initiatives cannot be achieved without the exchange of information about individual service users, levels of activity, the level and nature of resources and about their approach to addressing the issues. Their adoption of a multi-agency approach to address the issues therefore, includes a commitment to ensure such information is shared, albeit in a manner which is compliant with their statutory responsibilities.
- 32 Information provided by service users is likely to be confidential in nature. All agencies therefore accept that this information will not be disclosed without the consent of the individual concerned, unless there are statutory grounds and, in the case of confidential personal information, an overriding public interest or justification to disclose.
- 33 When seeking information from other parties to this agreement, staff in all agencies will respect the responsibility of confidentiality and will not seek to override the procedures which each agency has in place to ensure information is not disclosed illegally or inappropriately.
- 34 Each agency accepts that information received under this protocol is only to be used for a specified purpose(s). The secondary use of personal information is not permitted unless the consent of the disclosing party to that secondary use is sought and granted, but having regard to the provisions of paragraph 30.
- 35 Each agency agrees always to give consideration as to whether it is possible to use depersonalised information (namely information presented in such a way that individuals cannot be identified) to achieve the purpose.
- 36 Each agency agrees to ensure that the information shared is purposeful, justified and specifically geared to the task it is intended to serve. The information should be sufficient and sharing should exclude unnecessary material.
- 37 All agencies agree that they will each comply with the various statutory timescales relating to how long particular types of information are retained. Internal procedures will be put into place to ensure compliance with this. Where there are no statutory guidelines, information will be held in accordance with the fourth and fifth principles of the DPA.
- 38 Subject to certain exemptions, each agency is obliged to notify the Data Protection Commissioner of all purposes for which they process personal

data by automated means.

- 39 The parties agree to ensure compliance with the notification requirements of the DPA and ensure that their notification is accurate and kept up to date.
- 40 Each agency agrees to make every reasonable effort to ensure that the information they hold is accurate and up to date. Any errors identified in the information held will be corrected or erased as soon as reasonably practicable.
- 41 Each agency agrees to make reasonable efforts to ensure that the recipients of personal information are kept informed of changes in the personal information which they have received, so that records can be kept up to date.
- 42 Each agency will ensure efficient and effective procedures are put in place to address complaints relating to the disclosure of information.
- 43 Each agency agrees that appropriate training will be given to staff to ensure they are aware of their responsibilities in relation to the handling and sharing of personal information to ensure information is shared lawfully and in accordance with this protocol.
- 44 Should information be disclosed without legal justification, each agency agrees to ensure that a manager at the appropriate level of the organisation reviews the incident and considers ways in which the repetition of the error can be avoided in the future, and take other such action as may be appropriate in the circumstances.
- 45 In accordance with The Information Commissioners' Guidance, Privacy Impact Assessments should be considered when collecting personal information as a means of ensuring that information sharing will not cause real unfairness or unwarranted detriment to individuals.

SECTION FOUR: PROCEDURE FOR THE DISCLOSURE OF PERSONAL INFORMATION

PRINCIPLES GOVERNING THE SHARING OF INFORMATION

Obtaining Consent

- 46 The general principle is that service users should be as fully informed as possible. Therefore, as a general rule, in every practical circumstance, the individual's consent should be obtained for sharing identifiable information. When seeking consent, the information provided must allow for disabilities, illiteracy, diverse cultural conditions and language differences
- 47 In most cases the consent to share information will be sought at the first contact with an individual. The member of staff should inform the service user who their employer is, what purpose the information will be used for, why the information being sought is to be shared, and which agencies the information might be shared with. This would usually form the basis of what is commonly termed a Fair Processing Notice. If, in the professional judgement of the staff member concerned, it would be detrimental to the person concerned to address these issues at the time of first contact, then the reason for not doing so should be recorded and arrangements agreed to complete this task at the first available opportunity.
- 48 Should it become necessary to share information with other agencies other than as originally agreed with the service user, or to share information for other purposes other than originally agreed, then the renewed consent of the individual will be obtained unless disclosure can otherwise be justified as being in the public interest where the information is of a confidential nature, and within the conditions permitted in Schedule 2 and Schedule 3 of the DPA.
- 49 Each agency agrees to work towards a situation whereby in most cases, where practically possible, especially in the case of sensitive information, the consent of the individual is given in writing. If consent can only be taken verbally, then the details of this consent should be recorded on an individual's file. An individual should be given a copy of any written consent given by them, and a further copy placed on the individuals file. Any refusal of consent or limited consent should also be recorded on the file.
- 50 Where it is necessary to seek the renewed consent of the service user, for example, because the purpose for which the information is to be shared has changed, or information is to be given to different agencies other than originally agreed with the service user, then the agencies agree to work towards obtaining a fresh written consent of the service user, where practical to do so.

- 51 Service users should be made aware that use of information is necessary to enable the organisation to meet its statutory obligations in relation to the particular service and the individual, to ensure the individual is not misled.
- 52 Reasonable steps should also be taken to ensure that service users are informed of their right to seek access to the information held about them. It is therefore important that staff having direct contact with service users ensure that the information they gather is accurate, coherent and as comprehensive as is needed, and properly recorded.
- 53 When considering the need to share confidential information in the public interest e.g. to prevent or detect a serious crime or prevent serious harm to the individual or others, decisions must be clearly recorded detailing the circumstances and reasoning behind the decision to disclose or not disclose. The decision must be documented in the individual's record.

Lack of Capacity to Consent

- 54 Where an individual is unable or not competent to provide consent then this should be recorded. A person is unable to make a decision if he/she is unable: -
- a) to understand the information relevant to the decision,
 - b) to retain that information
 - c) to use or weigh that information as part of the process of making the decision, or
 - d) to communicate his decision (whether by talking, using sign language or any other means).
- 55 A person is not to be regarded as unable to understand the information relevant to a decision if he is able to understand an explanation of it given to him in a way that is appropriate to his circumstances (using simple language, visual aids or any other means).
- 56 The fact that a person is able to retain the information relevant to a decision for a short period only does not prevent him from being regarded as able to make the decision.
- 57 In such circumstances, information may be shared if it is in the person's best interests, informed by any previously expressed wishes and feelings of the individuals and in consultation with: -
- anyone previously named by the person as someone to be consulted on either the decision in question or on similar issues

- anyone engaged in caring for the person
- close relatives, friends or others who take an interest in the person's welfare
- any attorney appointed under a Lasting Power of Attorney or Enduring Power of Attorney made by the person
- any deputy appointed by the Court of Protection to make decisions for the person.

Guidance on assessing capacity and establishing best interests can be found in the Mental Capacity Act Code of Practice published by the Department for Constitutional Affairs, see www.dca.gov.uk/menincap/legis.htm

Lasting Power of Attorney and Deputies appointed by the Court of Protection

- 58 Individuals who lack capacity may have a Lasting Power of Attorney or a Deputy appointed by the Court of Protection. A Lasting Power of Attorney or Deputy may make an information sharing decision on behalf of the person, if it is within the scope of their authority. Such decisions must be in the person's best interests. In such cases the purpose of the information sharing, the type of information to be shared and who it is to be shared with must be explained to the Legal Power of Attorney or Deputy.
- 59 Any objections must be noted in the subject's record. The Legal Power of Attorney or Deputy will be kept informed of any subsequent disclosures and any objections raised will be noted in the individual's record.

Independent Mental Capacity Advocate

- 60 Individuals who lack capacity and do not have a Last Power of Attorney or Deputies may have an Independent Mental Capacity Advocate appointed. Such an advocate would be used when making decisions about serious medical treatment or changes of residence.

Children

- 61 Children under the age of 16 who have the capacity and understanding to make decisions about the use and disclosure of information may consent to the disclosure of information about themselves. The consent process described above should be followed. For children under the age of 16 who are unable to consent, consent should be sought from the person with parental responsibility

Disclosure without consent

62 Although it is regarded as good practice to seek the consent of service users, disclosure without the consent of the individual is lawful where one of the conditions set out in Schedule 2 of the DPA is met, and, where the data is sensitive, where one of the conditions set out in Schedule 3 is also met. Disclosure of confidential information, without consent, should only be made however, where it is in the public interest to do so. The information may, for example, need to be shared to ensure the performance of public functions or a legal obligation. Organisations will need to ensure that anyone who is given access to personal information is aware of the need to treat the information as confidential.

63 In other cases, consent should not be sought, at least initially, to the obtaining and sharing of information, provided the criteria under Schedules 2 and 3 are met, where it would be against the public interest to seek consent at that point. “Working Together to Safeguard Children” at paragraph 5.6 for example, indicates that:

“While professionals should seek, in general, to discuss any concerns with the family and, where possible, seek their agreement to make a referral to Social Services, **this should only be done where such discussion and agreement seeking will not place a child at increased risk of significant harm**”.

“No Secrets”, produced by the Department of Health in relation to adult protection states at Section 3.6 that the interagency framework must:

“... balance the requirements of confidentiality with the consideration that, to protect vulnerable adults, it may be necessary to share information” At Section 5.6, it goes on to say:

“Confidentiality must not be confused with secrecy; informed consent should be obtained but if this is not possible and vulnerable adults are at risk, it may be necessary to override this requirement”.

In other cases, disclosure might prejudice permitted objectives, such as the prevention or detection of crime or the apprehension or prosecution of offenders. Legal advice should be taken in cases of uncertainty.

64 In certain cases, the consent of an individual may be sought to disclose the information, but that consent is refused. That refusal of consent can be overridden provided the requirements of the DPA are met, and in the case of confidential information, where it is in the public interest to disclose. Taking into account the Human Rights Act, a balancing exercise needs to be carried out between the individual’s right to confidentiality, and the public interest in

disclosure. The refusal of consent and the reasons for overriding that refusal should be recorded on the client's or customer's file.

- 65 Each organisation should ensure that staff are trained or know where to obtain advice on the need to seek consent, how to seek consent, recording consent and the circumstances under which information may be disclosed without consent.

SECTION FIVE: ACCESS AND SECURITY PROCEDURES

- 66 Each agency who is a party to this agreement will ensure procedures are prepared to enable service users to be given access to personal information held about them. In the case of joint records, either organisation can provide access to the joint record, provided the individual is informed that the information is held jointly. Agencies in joint record holding arrangements therefore agree to ensure they have in place procedures to enable the individual to be made aware that he/she is not obliged to apply to all of the agencies for access, and to ensure that each agency is informed that access has been given.
- 67 Where information relating to an individual is shared between the agencies, each agency shall take all reasonable steps to ensure this information is transferred and shared in a secure manner.
- 68 Agencies shall ensure that appropriate security measures are taken to ensure that data is stored and held in a secure manner. These measures will ensure that access to the information can only be obtained by those with the need and the right to know.

SECTION SIX: MONITORING AND REVIEWING PROCEDURES

- 69 This protocol will be subject to a review every year by the agencies who are parties to this agreement.
- 70 Each agency should have an allocated person to respond to queries regarding the protocol, and take comments on the operation of the protocol. It is assumed that the allocated person responsible for dealing with queries regarding the protocol will be the allocated Data Protection Officer within each agency.
- 71 The review will be coordinated by The Information Governance Team, Hull City Council on behalf of all agencies and maintain a list of contact officers responsible for the protocol for each agency. Proposed changes to the protocol will be issued to contacts for approval prior to adoption.
- 72 This protocol will be agreed by each signatory agency through its own appropriate mechanism for dealing with data protection and information sharing issues.
- 73 Copies of this protocol will be held by the allocated Officer for each agency.
- 74 The agencies are responsible for ensuring that Service Level Agreements or contracts with voluntary, charitable and private partners with whom they share personal information include requirements to comply with this protocol.
- 75 The parties to the protocol are responsible for publicising and promoting this agreement to the public and staff within their own organisations.

**SECTION SEVEN:
PARTNERSHIP UNDERTAKING**

76 The parties to the protocol accept that the principles laid down in this document will provide a secure framework for the sharing of information between their agencies in a manner compliant with their statutory and professional responsibilities.

77 As such they undertake to:

- Implement and adhere to the principles set out in this protocol;
- Ensure that all operational procedures established between their agencies for the sharing of information relating to the population of Hull and East Riding are consistent with this General protocol;
- Ensure that where these procedures are adopted then no restrictions will be placed on the sharing of information other than those specified within operational procedures.

78. Signatory

Name

Title

Organisation

Address

.....

.....

Signature

Original, agency signed copies of the protocol will be held by Hull City Council and may be viewed on request by contacting:

Information Governance Team

Hull City Council

The Guildhall

Alfred Gelder Street

Hull

HU1 2AA

Tel 300300

APPENDIX A PARTIES TO THE PROTOCOL

Hull & East Yorkshire Hospitals NHS Trust
Hull Teaching Primary Care Trust
East Riding of Yorkshire Primary Care Trust
Humber Mental Health NHS Teaching Trust (HMHTT)
Yorkshire Ambulance Service
Humberside Police
Humberside Police Authority
National Probation Service - Humberside
HM Prison Everthorpe
HM Prison Full Sutton
HM Prison Hull
HM Prison Wold
HM Coroner for Hull & the East Riding of Yorkshire
Humberside Crown Prosecution Service,
CAFCASS Children and Families Court Advisory Service - Yorkshire & Humberside
Hull City Council
East Riding of Yorkshire Council
Humberside Fire and Rescue Service
Connexions Humber
East Riding Primary Schools
East Riding Secondary Schools
East Riding Special Schools
East Riding Nurseries
Hull Primary Schools
Hull Secondary Schools
Hull Special Schools
Hull Nurseries
East Riding Youth Offending Team
Hull Youth Offending Team

APPENDIX B OPERATIONAL PROCEDURES FOR INFORMATION SHARING TEMPLATE

The main headings for the framework were agreed as follows:

Introduction / Objectives

- Why a procedure is required and what is its purpose?
- Who is involved?

Principles of Information Sharing

- Refer to Hull and East Riding General Protocol.

Client Consent

- Details of how each organisation will gain consent and apply Fair Processing Notices where necessary.

Parameters

- Validation procedures, eg: verbal.
- 'Lead Officer' for specific functions.
- Responsibilities including sub organisations.

Defined Purposes

- Reference to the principles of the Act.
- Why? (Justification - refer to other relevant documents.)
- What information is covered and what is it used for?
- How will it be obtained?
- Who will see it? (based on role / task.)
- Specific restrictions, eg: 3rd Party.

Access and Security

- Physical / organisational.
- Procedure for dealing with requests.

General

- Review process (annual).
- Procedure for handling disputes and complaints (refer to general Protocol).
- Signature (level necessary to meeting each organisation's compliance).