

County Durham and Darlington

A JOINT PROTOCOL

FOR

INFORMATION EXCHANGE

For

Multi Agency Risk Assessment

Conferences

February 2008

Contents

Page

1. INTRODUCTION.....	5
1.9 Legislation.....	5
2. MULTI-AGENCY RISK ASSESSMENT CONFERENCES.....	6
3. REQUIREMENTS FOR INFORMATION EXCHANGE.....	7
3.1 Personal Data.....	7
3.2 Power to Disclose.....	7
3.3 Consent.....	7
3.4 Capacity to give consent.....	8
3.5 Disclosure without Consent.....	8
3.6 Extent of Personal Data Disclosed.....	10
3.7 Clinical Confidentiality.....	10
3.8 Proportionality.....	10
DOCUMENTS CIRCULATED FOR SIGNATURE TO:.....	2
4. SECURITY.....	11
4.1 Security, Retention, Destruction of Data.....	11
4.2 Data Quality.....	11
4.3 E-Mail.....	11
4.4 Caldicott Guardians.....	12
4.5 Indemnity.....	12
5. COMPLAINTS AND BREACHES.....	12
6. SUBJECT RIGHT OF ACCESS.....	12
6.2 Third Party Information.....	13
6.3 Freedom Of Information.....	13
7. MONITORING AND REVIEW.....	13
7.1 Policy management.....	13
7.2 Specific Procedures.....	14
8. SIGNATURES.....	15
APPENDIX A.....	19
Further Guidance to Key Legislation Underpinning the Protocol.....	19
APPENDIX B.....	27
Form of Indemnity.....	27
APPENDIX C.....	30
Guidance for Computer Based Systems.....	30
APPENDIX D.....	32
Contact Officers.....	32
APPENDIX E.....	33
Letter informing victim of MARAC.....	33
DOCUMENTS CIRCULATED FOR SIGNATURE TO:	

Chief Constable
Durham Constabulary

Chief Executive
Durham County Council

Chief Officer
Durham Tees Valley Probation Service

Chief Executive
Darlington Borough Council

Chief Executive
County Durham and Darlington
Strategic Health Authority

Chief Executive
Tees, Esk and Wear Valley NHS Trust

Chief Executive
County Durham and Darlington NHS
Trust

Chief Executive
County Durham and Darlington Foundation
Trust

Manager
Derwentside Domestic Abuse Service

Domestic Abuse Coordinator
East Durham Domestic Violence Forum

Director
Barnardo's North East

Director
Wear Valley Women's Aid (Refuge)

Director
Harbour

Regional Director
Victim Support

Manager
Terentia House (Derwentside Refuge)

Director
DISC

Team Leader
Durham Women's Refuge

Manager
Darlington Women's Aid (Refuge)

Director
East Durham Homes

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

- Notification of business purposes under the Data Protection Act 1998 has been given to the Governance Officer;
- realistic expectations prevail from the outset, with a balance between all of the statutory powers, including Human Rights Act 1998, Freedom of Information Act 2000, Race Relations (Amendment) Act 2000, Section 115 of the Crime and Disorder Act 1998, Computer Misuse Act 1990, case law and the requirements of the Data Protection principles and other Acts;
- ethical standards are maintained;
- appropriate security, retention, review, quality assurance and destruction policies are maintained;
- organisations providing commissioned services must sign up to and comply with a specific protocol and indemnity between those participating organisations;
- appropriate training or awareness raising is provided;
- adequate arrangements exist to test adherence to this protocol; and
- this document shall be reviewed every two years unless significant new legislation or guidance from central government makes it necessary to have an earlier review.

1. INTRODUCTION

- 1.1 The purpose of this Protocol is to facilitate the sharing of information between agencies/organisations, who are/may be involved in the Multi Agency Risk Assessment Conferences (MARAC), whilst safeguarding the confidential nature of that information. The information held by agencies relates to people of all ages, their carers, children, young people and families.
- 1.2 The purpose of MARAC is to combine in a single meeting relevant up to date risk information with a comprehensive assessment of the victim's needs and links those directly to the provision of appropriate services for high risk cases of domestic abuse: victim, children and perpetrator.
- 1.3 The Protocol recognises the benefits of joint/partnership work thereby ensuring a more effective service delivery. It also recognises that there have been occasions where the lack of information sharing has been to the detriment of individuals and commented upon in subsequent enquiries.
- 1.4 The Protocol provides a framework, relating to the sharing of information and the safeguarding of confidentiality. Each agency will have their own procedures for sharing information and confidentiality. It is important to note that this protocol does not supersede these; it is an interagency agreement on common issues of good practice in order to work together more effectively in the MARAC process.
- 1.5 All participating organisations/agencies must recognise and fulfil their individual and collective responsibilities under this agreement. Compliance will ensure that those participating organisations/agencies will satisfy all legal and ethical requirements and those of any professional regulatory body.
- 1.6 The sharing of information shall adhere to the principles contained within case law i.e. the "Common Law Duty of Confidentiality" and the following legislation. It will cover only that which is relevant in pursuance of the provisions of the legislation (see 1.10).
- 1.7 All personal information will be collected, processed, disclosed and shared in accordance with statutory requirements for the safeguarding of information.
- 1.8 All agencies that are signatories to this protocol will agree to share information and treat all personal information confidentially.

1.9 Legislation

- Data Protection Act 1998
- Human Rights Act 1998
- Crime and Disorder Act 1998
- Freedom of Information Act 2000

- Mental Health Act 1983
- Health & Social Care Act 2001
- NHS & Community Care Act 1990
- Independent Safeguarding Act 2006
- Children Act 2004
- Police reform Act 2002
- Race Relations (Amendment) Act 2000
- Regulation of Investigatory Powers Act 2000
- Housing Act 1996
- Children Act 1989
- Education Act 1996
- Computer Misuse Act 1990
- Adoption Act 2002
- Victim and Witnesses Act 2004
- Mental Health Act 1983
- Police and Justice Act 2006
- Children and Young People Act 2006
- Mental Capacity Act 2005

2. MULTI-AGENCY RISK ASSESSMENT CONFERENCES

2.1 The MARAC aims to:

- Share information to increase the safety, health and well-being of adult victims and their children.
- Determine whether the perpetrator poses a significant risk to any particular individual or to the general community.
- Develop and implement a multi agency risk management plan to reduce the risk of harm.
- Reduce repeat victimisation.
- Improve agency accountability.
- Improve support for staff involved in high risk domestic abuse cases.

2.2 The responsibility to take appropriate actions rests with individual agencies, it is not transferred to the MARAC.

2.3 The role of the MARAC is to facilitate, monitor and evaluate effective information sharing to enable appropriate actions to be taken to increase public safety.

3. REQUIREMENTS FOR INFORMATION EXCHANGE

3.1 Personal Data

- 3.1.1 Any disclosure of personal data must have regard to both common and statute law, for example: defamation, the common law duty of confidence, the principles of the Data Protection Act 1998, the Human Rights Act 1998 Freedom of Information Act 2000 and the 6 Caldicott general principles, to ensure that confidential information may be exchanged, as defined within operating procedures, of each agency.
- 3.1.2 The data protection principles require that such information is obtained and processed fairly and lawfully; is only disclosed in appropriate circumstances; is accurate, relevant, and not held for longer than necessary; and is kept securely in accordance with the current organisational policies and procedures.

3.2 Power to Disclose

- 3.2.1 In relation to “crime reduction”, Section 115 of Crime & Disorder Act 1998 ensures all agencies have a power to disclose; it does not impose a requirement on them to exchange information, control remains with the agency which holds the data.

3.3 Consent

- 3.3.1 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 this case the specific detail of the processing should be explained, the particular types of data to be processed, the purposes of the processing and any special aspects of the processing which may affect the individual, e.g. disclosures.
- 3.3.2 Wherever possible the person’s explicit consent must be obtained when their personal information is to be shared and they should be as fully informed as possible regarding this. Individuals should be informed that information will not be shared without their consent, unless there is a statutory duty to do so in preventing harm to someone else, to protect them or prevent or detect crime. In all cases, this consent should be in writing.
- 3.3.3 No details of victims, witnesses, informants or complainants should be disclosed without their written consent (Swinney v Chief Constable of Northumbria).
- 3.3.4 Circumstances may arise where consent cannot be obtained e.g. a medical emergency. In these cases, there is a requirement to pass information promptly to those providing the individual’s care. With this and other types of emergencies, the reasons justifying disclosure should be documented.

Non-Offenders at risk of offending

3.3.5 The agencies involved should obtain the explicit consent of the individual (or the parent or guardian, in the case of a minor).

3.4 Capacity to give consent

3.4.1 Where a person is unable to give consent because they are unconscious or otherwise incapable, for example due to immaturity, illness or mental incapacity, the decision should be made on the person's behalf in their best interests by those responsible for providing care. Staff should ascertain any views the person can express and those of their carer or advocate wherever possible.

3.4.2 Children who are judged to be able to understand what they are consenting to (Gillick v Norfolk Health Authority 1986) may provide consent. Where a person under the age of 18 is not judged competent to consent on their own behalf, then consent may be given, by a person with parental responsibility for the child or young person. All children or young persons are entitled to the same duty of confidence as an adult and disclosure of confidential information to their parents/person with parental responsibility must satisfy the same common law requirements:

- legal responsibilities
- duty of confidence
- public interest
- any disclosure - staff must ensure reasons are recorded and agreed by the team involved in the decision making process.

3.5 Disclosure without Consent

Starting Principle - Article 8 Human Rights Act

3.5.1 Article 8 of the European Convention on Human Rights 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 the interests of national security
- Public safety
- Economic well being of the country
- The prevention of crime and disorder
- The protection of health and morals
- The protection of the rights and freedoms of others

3.5.2 This principle is reflected in Data Protection Act, 1998. The non-disclosure provisions are the first five data protection principles and exemptions from these

provisions are allowed in situations where the Act recognises that disclosure would in fact be in a public interest when consent has not been sought or has been withheld.

This includes:

- prevention of crime including;
- prevention of disorder
- protection of public safety
- protection of rights and freedoms of all
- protection of young or other vulnerable people

3.5.3 If informed consent has not been sought, or has been sought and withheld, the agency must consider if there is an overriding public interest of justification for the disclosure. Decisions must be made on a case by case basis to determine whether a failure to disclose would be likely to prejudice this objective, and the advice of the appropriate Caldicott Guardian or Data Protection Officer should be sought in any case of doubt. There is further guidance on Data Protection exemptions in Appendix A.

3.5.4 When making the decision if disclosure is necessary, the following questions should be considered:

- Is the question of disclosure necessary for the prevention or detection of serious crime?
- Is the disclosure necessary for the protection of young or other vulnerable people?
- 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 individual?
- Is the disclosure proportionate to the intended aim?
- Is there an equally effective but less intrusive alternative means of achieving that aim?

3.5.5 Any request for information should specify, as clearly as possible:

- why the disclosure is necessary
- and in the example of crime prevention, why it is envisaged that a successful action would prevent crime, e.g. what is the projected effect of successful proceedings

Authority for Disclosure

3.5.6 In R v Chief Constable of North Wales ex parte AB & Another, a decision to disclose information without consent was subject to judicial review. The decision to disclose can be justified if the risk assessment test, details the considerations and safeguards that must be taken into account before disclosure takes place in relation to the police's performance of its public duty.

These are:

- There must be an honest belief that the disclosure is necessary for the protection of specific persons who might otherwise become a victim of crime. It is not acceptable to argue that because an offender has committed a certain type of offence disclosure is inevitable
- Potentially damaging information should not be disclosed unless it is necessary for the performance of public duty. Public duty is not a data protection issue but a matter of general principle.

Consideration must be given to the extent and nature of the disclosure.

3.6 Extent of Personal Data Disclosed

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

3.6.2 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.'

3.7 Clinical Confidentiality

3.7.1 In the context of health services, particular consideration will need to be given as to the possible harm which could result from the disclosure of a patient's personal information. The risk of possible damage to the patient/clinician relationship of trust and the likelihood that the individual concerned may disassociate themselves from a necessary programme of health care intervention must be balanced against the positive benefits of diverting the individual from criminal activity or protecting other members of society.

3.7.2 Any such disclosure should be clearly recorded.

3.8 Proportionality

3.8.1 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 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.

3.9 Refusal to Disclose

3.9.1 Any refusal should be recorded and must include the reasons for that decision. There must be an in-built procedure for a senior member of the organisation to review this decision that could include liaison with the Data Protection Officer and/or Caldicott Guardian.

4. SECURITY

4.1 Security, Retention, Destruction of Data

4.1.1 Security Partners (signatories) should ensure that they have appropriate security arrangements in place for information stored, or the organisation is working towards this aim.

4.1.2 As a general principle, information should only be retained for the minimum period required to achieve its objective(s) and will be returned to the originator or destroyed. Criteria for the review of retention and destruction will be agreed in accordance with existing organisational policies and procedures.

4.2 Data Quality

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

4.3 E-Mail

4.3.1 Sharing of data between organisations using e-mail should be strictly controlled in accordance with organisational policy of each agency, with encryption used wherever possible. (Further guidance on computerised systems is contained in Appendix C). This will not be the usual method of sharing MARAC case information. Recorded delivery will be the preferred method, however it is noted that this is not a 'secure' delivery method.

4.4 Caldicott Guardians

- 4.4.1 All NHS and Councils with Social Services responsibilities have a Caldicott Guardian to oversee access to patient/service user information. The Guardian is responsible for agreeing and reviewing protocols for governing the disclosure of patient/service user identifiable information across organisational boundaries. The Guardian offers advice regarding the handling of patient/service user identifiable information.

4.5 Indemnity

- 4.5.1 An indemnity has been signed by each partner (signatories) and is attached in Appendix B.
- 4.5.2 Disclosures and requests for disclosures must be in writing and retained for the minimum period defined in organisational procedures.
- 4.5.3 Decisions on disclosures reached at meetings must be minuted. Staff must be especially careful when releasing or discussing personal information.

5. COMPLAINTS AND BREACHES

- 5.1 Complaints about the use, or disclosure, of information must be referred to the organisation from which the information originated, and will be investigated in accordance with the relevant organisational procedures.
- 5.2 Complaints about the use or disclosure of information from police databases or manual records must be referred to a police officer of Inspector rank.
- 5.3 Any complaint relating to a policy or procedure should be considered when the policy is reviewed.

6. SUBJECT RIGHT OF ACCESS

- 6.1 Service users have a right of access to information held about them subject to current legislation. The Data Protection Act 1998, however, identifies limited circumstances in which access may be denied, these circumstances relate to specific situations, for example, safeguarding national security, crime and taxation, health, education and social work. The Freedom of Information Act 2000 makes some changes and is about a culture change from a 'need to know, to a right to know.' For public authorities it represents a balance between openness and transparency of decision making on the one hand and the need to protect information where disclosure would cause harm or otherwise be contrary to the public interest on the other (see Appendix A).

6.2 Third Party Information

6.2.1 When a request is received to access records, the records will need to be checked in order to obtain the consent of any persons identifiable from these records. If consent cannot be obtained, staff should refer to their own organisational procedures, which will state who to contact in these circumstances. They will then need to liaise with this named person to consider whether it is reasonable in all the circumstances to comply with the request without consent.

6.2.2 In determining this, staff will need to consider:

- any duty of confidentiality owed to the third party;
- any steps taken by the data controller with a view to seeking the consent of the third party;
- whether the third party is capable of giving consent;
- any express refusal of consent by the third party; and
- whether the third party information is exempt under Section 40 of the Freedom of Information Act 2000.

6.2.3 Where an individual specifically requests information about a 'third party', or where responding to a request would involve the disclosure of personal information about a third party, the request falls within the remit of the Freedom of Information Act (although Data Protection Principles must still be applied). An organisation must not release information about a third party, if doing so would breach one of the Principles.

6.3 Freedom Of Information

6.3.1 Requests under the Freedom of Information Act that may involve access to policy documents and the decision-making processes should be dealt with as above. The Freedom of Information Act 2000 also identifies some circumstances in which access may be denied, such as information provided in confidence, commercial interests, law enforcement and health and safety. A full list is included as an Appendix A.

6.3.2 Agencies are reminded that these agreements should be publicly available.

7. MONITORING AND REVIEW

7.1 Policy management

7.1.1 This Protocol will be reviewed and re- issued biannually by the County Durham Domestic Abuse Forum Executive Group.

7.2 Specific Procedures

- 7.2.1 All procedures devised as a result of this protocol should state who is responsible for the monitoring and review process in relation to them.
- 7.2.2 Specific Guidance on the day to day operation of the procedures including the posts responsible for producing information, content and format of data, means of exchanging data, etc. should be included in the specific procedures.

8. SIGNATURES

This protocol must be signed by a Chief Officer from each of the agencies in the Parties/Signatories Section in the following format.

Signed _____ Position _____ Date _____

Signed _____ Position _____ Date _____

Signed _____ Position _____ Date _____

Signed _____ Position _____ Date _____

Signed _____ Position _____ Date _____

Signed _____ Position _____ Date _____

Signed _____ Position _____ Date _____

Signed _____ Position _____ Date _____

Signed _____ Position _____ Date _____

Signed _____ Position _____ Date _____

Signed _____ Position _____ Date _____

Signed _____ Position _____ Date _____

Signed _____ Position _____ Date _____

Signed _____ **Position** _____ **Date** _____

Signed _____ **Position** _____ **Date** _____

Signed _____ **Position** _____ **Date** _____

Signed _____ **Position** _____ **Date** _____

Signed _____ **Position** _____ **Date** _____

Signed _____ **Position** _____ **Date** _____

Signed _____ **Position** _____ **Date** _____

Signed _____ **Position** _____ **Date** _____

Signed _____ **Position** _____ **Date** _____

Signed _____ **Position** _____ **Date** _____

Signed _____ **Position** _____ **Date** _____

Signed _____ **Position** _____ **Date** _____

Signed _____ **Position** _____ **Date** _____

Signed _____ **Position** _____ **Date** _____

Signed _____ **Position** _____ **Date** _____

Signed _____ **Position** _____ **Date** _____

Signed _____ **Position** _____ **Date** _____

Signed _____ **Position** _____ **Date** _____

Signed _____ **Position** _____ **Date** _____

Signed _____ **Position** _____ **Date** _____

Signed _____ **Position** _____ **Date** _____

Signed _____ **Position** _____ **Date** _____

Signed _____ **Position** _____ **Date** _____

Signed _____ **Position** _____ **Date** _____

Signed _____ **Position** _____ **Date** _____

Signed _____ **Position** _____ **Date** _____

Signed _____ **Position** _____ **Date** _____

Signed _____ **Position** _____ **Date** _____

Signed _____ **Position** _____ **Date** _____

Appendices

APPENDIX A

Further Guidance to Key Legislation Underpinning the Protocol

1. Data Protection Act 1998

The Data Protection Act 1998, provides the statutory basis for organisations to share information for an approved purpose. The Act does not apply to the deceased or anonymised information i.e. information does not identify the individual.

The Act provides in Schedules 2 and 3, conditions that must be met before personal information can be processed fairly and lawfully. Schedule 2 is for all personal information; Schedule 3 is an additional test for sensitive information. Processing the information (for example, how it is collected, held and disclosed) must satisfy one of the conditions in Schedule 2 and where it also involves sensitive information (which most inter-agency work does) at least one of the conditions in Schedule 3 must also be met. Please refer to Data Protection Act 1998 for detailed information.

For example, where a service user gives their explicit consent to share information then the conditions relating to having given consent are met in both Schedules 2 and 3 and therefore, no other conditions are required to be met in either of these Schedules.

Staff should consider what common law or other legislation they are sharing information under, for example, is it for the purpose of an assessment of a child under the Children Act 1989.

The first 8 principles of the Data Protection Act relate to Personal information as follows:

1. *Personal data must be processed fairly and lawfully and in particular, shall not be processed unless at least one of the conditions in Schedule 2 and in the case of sensitive data, at least one of the conditions in Schedule 3 of the Data Protection Act, 1998.*
2. *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.*

Information given or obtained for one purpose should not be used for a different purpose without the consent of the person who provided the information. Staff should ensure they always record who provided the personal information, as no secondary or other use may be made of the information

3. *Personal data must be adequate, relevant and not excessive in relation to the purpose/s for which they are processed.*

This allows for an individual's personal information to be protected and assists in controlling the amount of personal information flowing between agencies and organisations.

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

Where staff responsible for a case discover any inaccuracies or inadequacies in personal information they should notify the owner of the information and request they correct it. They should also notify others involved in the case of the corrections and request these are made to their records.

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

All agencies and organisations should ensure they have policies and procedures in place for the retention and destruction of personal information.

6. *Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act, 1998.*

There are seven rights, which are:

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

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

8. *Personal data shall not be transferred to a country or territory outside the European Union 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*

Data Protection Act 1998 – Part IV – Exemptions

The act contains a number of exemptions to the requirement that personal data be processed in accordance with the act. Unfortunately this cannot be easily categorized into situations where types of information enjoy the same exemptions

and most of them apply to narrowly defined situations that need to be considered on a case-by-case basis.

Depending on the purpose for which the data are processed the processing function may be exempt from either the “subject information provisions” or the “non-disclosure provisions” of the Act.

The former are those requiring data controllers to inform data subjects of various matters and give them access to their data. The latter are, essentially, first five data protection principles and exemptions are allowed where it is recognized that it would be in the public interest to allow disclosure.

Generally, exemptions are available when data is procured for the following purposes:

1. national security;
2. the prevention and detection of crime and assessment or collection of taxes;
3. health, education and social work;
4. regulatory activities;
5. research, history and statistics;
6. making information available to the public under statutory requirements;
7. disclosure required by law or in connection with legal proceedings;
8. domestic purposes.

Other miscellaneous exemptions may apply in certain circumstances relating to other matters, including confidential references given by the data controller and the armed forces. This is not exhaustive.

Due to the complexity of the exemption provisions the above list should not be relied upon, nor seen as definitive. Specific advice should be sought if it is felt that a certain situation may fall within an exemption category and the particular statutory instrument referred to where appropriate.

2. Human Rights Act 1998

When sharing information staff should also consider the requirements of the Human Rights Act 1998. It places a legal obligation on all public authorities to act in a manner compatible with the Convention. 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 3 (Freedom from torture or inhuman or degrading treatment), 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.

The Convention does allow limited interference with certain Convention rights by public authorities under broadly defined circumstances known as legitimate aims. Before pursuing an action of this type, staff should consider the following questions:

- is there a legal basis for the action being taken?
- does it pursue a legitimate aim (as outlined in a particular Convention article)? – see Article 8
- is the action taken proportionate and the least intrusive method of achieving that aim?

The principle of ‘proportionality’ is a common theme running through the Convention rights. 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 interest of society. In the context of sharing information, it should be restricted to a minimum and be the least damaging that is required in achieving the objective. A fair balanced judgement needs to be made by staff to ensure they give the minimum but also the necessary information in order, for example, to contribute effectively to a risk assessment about possible abuse in relation to a child or a vulnerable adult.

ARTICLES

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 that did not constitute a criminal offence under national or international law at the time the offence 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 from 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 join trade unions for the protection of his interests.

Article 12 – Right To Marry

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

Article 14 – Prohibition Of Discrimination

The enjoyment of 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 activities 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 The Use Of Restrictions On Rights

Restrictions permitted under this Convention to the said rights and freedoms shall not be applied for any purpose other than those for which they have been prescribed.

PROTOCOLS

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 Free 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 The Death Penalty

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

Article 2 – Death Penalty In Time Of War

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

3. Common Law Duty of Confidentiality

Although provided by case law rather than legislation, it is important that all staff working in agencies whether a statutory or voluntary agency or in the independent sector are aware that they are legally subject to a common law duty of confidentiality and must abide by this.

The duty of confidentiality requires that unless there is a statutory requirement to use information that has been provided in confidence, it should only be used for purposes that the service user has been informed about and has consented to. The duty is not absolute but should only be overridden if the holder of the information can justify disclosure as being in the public interest (e.g. to protect others from harm).

Whilst it is not entirely clear under law whether or not a common law duty of confidence extends to the deceased, ethically it is considered good practice to accept that this is the case.

It is generally accepted that most (if not all) information provided by service users is confidential in nature.

4. Freedom of Information Act 2000

The Data Protection Act, 1998, gives individuals the right of access to personal information held about them. The Freedom of Information Act extends this right of access to include 'non personal' information. This may include information about a third party. The two laws come together at the point where personal information is considered for disclosure.

Requests for information made by individuals about themselves will be exempt under the Freedom of Information Act, and will continue to be handled as Subject Access Requests under the Data Protection Act.

Where an individual specifically requests information about a third party, or where responding to a request would involve the disclosure of personal information about a third party, the request falls within the remit of the Freedom of Information Act (although Data Protection Principles must still be applied). An authority must not release information about a third party, if doing so would breach one of the Principles.

Exemptions

There are a number of exemptions to the general right of access contained in the Act. These are listed below:

- information accessible to the applicant by other means (Section 21)
- information intended for future publication (Section 22)
- information supplied by or relating to bodies dealing with security matters (Section 23)
- national security (Section 24)
- certificates under ss.23 and 24: supplementary provisions (Section 25)
- information likely to prejudice national defence or the armed forces (Section 26)
- information likely to prejudice the UK's international relations or interests (Section 27)
- information likely to prejudice relations within the United Kingdom (Section 28)
- information likely to prejudice the economic interests of the UK or part of the UK (Section 29)
- investigations and proceedings conducted by public authorities (Section 30)
- law enforcement (Section 31)
- court records (Section 32)
- information held by public authorities which have functions relating to audit (Section 33)
- parliamentary privilege (Section 34)
- formulation of government policy (Section 35)
- prejudice to the effective conduct of public affairs (Section 36)

- information that relates to communications with Her Majesty, a member of the Royal Family or Royal Household, or to the conferring of honours (Section 37)
- health and safety (Section 38)
- environmental information (Section 39)
- personal information (Section 40)
- information provided in confidence (Section 41)
- legal professional privilege (Section 42)
- commercial interests (Section 43)
- legal prohibitions on disclosure (Section 44)

Amendments to the Data Protection Act 1998

Currently under the Data Protection Act 1998, manual data is considered to be data under the Act only where it forms part of a “relevant filing system” (i.e. where the manual data forms part of a set and is structured in such a way that specific information relating to a particular individual is readily accessible). This definition of data is extended under the Freedom of Information Act 2000 to include manual records held by public authorities (or by other parties on behalf of public authorities), which do not fall within the definition of a “relevant filing system”. This unstructured manual data will be considered to be personal data where it can lead to a living individual being identified.

Section 40 of the Freedom of Information Act 2000 states that information is exempt from disclosure:

- where the applicant is the subject of the data. Such requests will be treated as Subject Access Requests under the Data Protection Act;
- where the applicant is not the subject of the personal data but where disclosure of this third party data would breach any of the eight Data Protection Principles; or
- where the applicant is not the subject of the personal data but where disclosure of this third party data would be exempted under the Data Protection Act 1998 (i.e. where the data subject themselves would not be entitled to see this data under the Data Protection Act).

5. Crime and Disorder Act 1998

Section 115 of the Crime and Disorder Act allows agencies to share information held in respect of individuals in order to prevent crime and disorder in their area.

APPENDIX B

Form of Indemnity

1. In consideration of the provision of information in accordance with the attached MARAC Joint Protocol on Information Exchange, undertakes to indemnify any of the persons or any authority referred to in Paragraph 2 below against any liability that 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 incomplete or incorrect, and the error or omission was due to the wilful wrongdoing or negligence of the person providing the information;
- b. unless the person or authority claiming the benefit of this indemnity notifies as soon as possible of any action, claim or demand to which this indemnity applies, permits to deal with the action, claim or demand by settlement or otherwise and renders 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.

2. Organisations/persons who may claim the benefit of this indemnity are as follows:

Chester- le-Street District Council; any serving or former officer or currently elected or former elected member thereof;

City of Durham Council; any serving or former officer or currently elected or former elected member thereof;

County Durham Primary Care Trust; any serving or former officer or currently elected or former elected member thereof;

County Durham Probation Area; any serving or former member thereof;

County Durham and Darlington Foundation Trust; any serving or former member thereof;

Darlington Primary Care Trust; any serving or former officer or currently elected or former elected member thereof;

Darlington Borough Council; any serving or former officer or currently elected or former elected member thereof;

Darlington Women's Aid; any serving or former officer or currently elected or former elected member thereof;

Derwentside Domestic Abuse Service; any serving or former officer or currently elected or former elected member thereof;

Derwentside District Council; any serving or former officer or currently elected or former elected member thereof;

District of Easington Council; any serving or former officer or currently elected or former elected member thereof;

Durham Constabulary; any serving or former officer/employee thereof;

Durham County Council; any serving or former officer or currently elected or former elected member thereof;

Durham Women's Refuge; any serving or former officer or currently elected or former elected member thereof;

East Durham Domestic Violence Forum; any serving or former officer or currently elected or former elected member thereof;

Peterlee Refuge any serving or former officer or currently elected or former elected member thereof;

Sedgefield Borough Council; any serving or former officer or currently elected or former elected member thereof;

Tees, Esk and Wear Valley NHS Trust t; any serving or former officer or currently elected or former elected member thereof;

Teesdale District Council; any serving or former officer or currently elected or former elected member thereof;

Victim Support; any serving or former officer or currently elected or former elected member thereof;

Wear Valley District Council; serving or former officer or currently elected or former elected member thereof;

Wear Valley Women's Aid; serving or former officer or currently elected or former elected member thereof;

This indemnity shall apply to former officers/employees or members provided at the time when the act or omission occurred, that the person was a member or officer/employee of the relevant organisation.

3. Certificate of Acceptance

In order to fulfil the requirements of information exchange under the provisions of the Crime and Disorder Act 1998:

I, _____

on behalf of _____ hereby

accept and agree to the provision of this protocol.

Signed: _____ Date: _____

APPENDIX C

Guidance for Computer Based Systems

1. The sharing of personal information derived from computer systems must be considered very carefully by staff from any agency, which is a signatory to this protocol.
2. All agencies that are signatories to this protocol should have a computer security policy and procedures in place.
3. Agencies, which are signatories to the protocol will at regular intervals, update each other on the security standards within their respective networks and aspire to nationally recognised security standards such as ISO 27001.
4. All personal data held on systems should be protected through the use of system user identity (User IDs) and password protection. Members of staff should not divulge their personal password to anyone.
5. Work is underway at present to develop at National Government level an “e-Government Inter-operation Framework” (e-GIF). This framework will describe the technical standards and policies to be used by government agencies to “allow information to flow seamlessly across the public sector and provide citizens and business with better access to government services”. Compliance with CESG (Communications – Electronic Security Group, the information Assurance arm of GCHQ)
6. It is envisaged by Government that the e-GIF will enable agencies to share data electronically.
7. The e-GIF guidance states “standards are mandated on all new systems. Legacy systems which need to link to the Government Secure Intranet (GSI) Government Portal, the Knowledge Network or other systems which are part of electronic service delivery, will need to comply with these standards”.
8. At present there is no countrywide inter-operability policy. It is possible to arrange connection of networks with the National Health Service through the NHS code of connection; however, a significant amount of work may be required from respective agencies to meet these standards. In the interim, staff will only be allowed access to computer records of other agencies on the basis that they use PCs or terminal on the respective networks of the agencies concerned, i.e. there will be no connection of networks.
9. This does not prevent for example, staff in integrated teams being granted access to computer systems operated by agencies. However, no data other than that which it has been agreed to be shared must flow from one network to another.

10. Any arrangements to grant access to computer systems will only be granted if access to data is appropriate in accordance with the policy and specific procedures.
11. Agencies that are signatories to the policy will need to consider the e-GIF's requirements in the development and deployment of their electronic information systems.
12. Agencies that are signatories to this policy need to work towards inter-operability in line with the e-GIF bearing in mind the experience brought about through the establishment of integrated teams and other developments such as the Electronic Health Record (EHR).
13. Where agencies allow personal information to be e- mailed it should not be exchanged using e- mail outside of an agency's internal secure network (i.e. Internal E- mail). Any correspondence about clients exchanged using external e-mail i.e. between secure networks must be anonymised, i.e. the client should not be identifiable, and for example use of initials only, would be used.

APPENDIX D

Contact Officers

The following are designated posts that are responsible for data protection (including notification if appropriate), security and confidentiality and compliance with legislation. Their role should include the provision of suitable advice and guidance to staff.

Although the Designated Officers assume overall responsibility for ensuring adherence to the principles and requirements of this protocol, this shall not preclude specified individuals, roles or ranks within an organisation to authorise the routine disclosure of relevant information in accordance with operating practices/procedures.

<u>Post</u>	<u>Organisation</u>
Community Safety Incidents Officer	Chester- le-Street District Council
Head of Human Resource Management	Darlington Borough Council
Caldicott Guardian	Darlington Social Services Department
Data Protection Officer	Derwentside District Council
Data Protection Officer	Durham Constabulary
Chief Probation Officer	County Durham Probation Service
Principal Assistant (Systems Development)	Sedgefield Borough Council
Head of Information Technology	Teesdale District Council
Data Protection (I.T.) Information Technology	Wear Valley District Council City of Durham Council
Development Manager	
Freedom of Information and Data Protection Coordinator	Durham County Council
Caldicott Guardian ACS and CYPS	Durham County Council
Head of Personnel & Payroll	Easington District Council
Caldicott Guardian	Tees, Esk and Wear Valley NHS Trust
Data Protection Officer	Co Durham & Darlington Foundation Trust
Information Governance Manager	County Durham Primary Care Trust
Information Governance Manager	Darlington Primary Care Trust

APPENDIX E
Letter informing victim of MARAC

PRIVATE AND CONFIDENTIAL

Dear

Domestic abuse is a crime that can include assault, sexual assault, harassment, injury and damage to property. It is a crime that the police and other agencies treat seriously.

Occasionally people are identified as being at “very high risk” of becoming a victim again, and it is normal procedure that a Multi Agency Risk Assessment conference (M.A.R.A.C) is held, to discuss various issues in relation to the safety and well being of the identified person, and, if appropriate, their children.

The meetings are attended by individuals from various organisations, information may be sought from County Council Children and Adult Services, Health, such as G.P, Health Visitor, Mental Health, School Nurse etc, Domestic Violence Forum, Police, Probation Service, Independent Domestic Violence Advocate and Housing. Any information is shared and treated in the strictest confidence. A risk management plan is often implemented, offering the appropriate support available. We would like your consent to gather and share relevant information, so that we can look towards reducing repeat victimisation and any further harm being caused. If you give your consent please could you sign below.

We also work with many organisations that may be able to provide further help and advice. The National Domestic Violence helpline offers a 24 hour service and their contact details are 0808 2000247. Telephone calls from a landline are free but calls from mobile telephones are variable.

If you would like to discuss the contents of this letter or have any questions, please do not hesitate to contact the person who distributed it on our behalf.

I give my consent for information to be shared with the relevant agencies and for MARAC purpose only. I can also withdraw my consent at any time.

I would / would not (*please delete as appropriate*) like a copy of this form.

Signed Date

Yours sincerely

Eric Malkin
Detective Inspector

Dawn Maddison
MARAC Coordinator