INFORMATION SHARING PROTOCOL

Between

The Probation Board for Northern Ireland

(PBNI)

&

The Probation Service (Ireland)

In respect of

The Management of Sex Offenders and Offenders assessed as a Risk of Serious Harm to Others

June 2014

VERSION CONTROL SHEET

TITLE	**The Management of Sex Offenders and Offenders assessed as a Risk of Serious Harm to Others**
Information Asset Owner (s)	PBNI and PS
Version 1	Implemented June 2006
Version 1.1	Reviewed June 2007
Version 1.2	Reviewed May 2010
Version 1.3	Reviewed January 2014
Version 2	FINAL June 2014
Next review	May 2016

TABLE OF CONTENTS

APPENDICES

1. INTRODUCTION

1.1 The aim of this protocol is to protect the public in Northern Ireland and Republic of Ireland from Sex Offenders and Offenders assessed as Risk of Serious Harm (RoSH) who move between jurisdictions by:

- Providing a framework for the secure and confidential sharing of information (personal and non personal) between the Probation Board for Northern Ireland, hereafter, in this protocol referred to as PBNI, and the Probation Service, (Ireland), hereafter in this protocol referred to as PS.
- Co-ordinating and strengthening the supervision and management of sex offenders and offenders assessed as Risk of Serious Harm, in the community in both jurisdictions.

1.2 For the purpose of this protocol:

a) a sex offender is an individual who has been convicted of a sex offence as defined by the Sexual Offences Act 2003 as applied to Northern Ireland and the Sex Offenders Act 2001 (Ireland).

b) an offender assessed as Risk of Serious Harm is defined as follows:

PBNI:

Where there is high likelihood that an offender will commit a further offence, causing serious harm. (PBNI RoSH Policy 2013)

Serious harm is defined in the Criminal Justice (Northern Ireland) Order 2008 as death or serious personal injury whether physical or psychological

PS:

Serious harm is defined as “personal, physical or psychological harm which is life threatening and/or traumatic and from which recovery is usually difficult or incomplete”. (PSROSH Guidance Document January 2012)

1.3 This protocol is effective from 1 June 2014. It replaces the protocol issued in May 2010.

1.4 This protocol does not impose a duty to disclose information in any particular case nor does it provide the power to demand disclosure.

1.5 This protocol may be cancelled by either party at any time, in writing, to be sent to the relevant signatory. (para 17)

2. DRIVERS

2.1 This protocol has been developed in part due to the fact that it is not legally possible to transfer court orders from one jurisdiction to another. It is to facilitate and/or implement the arrangements and/or legislative requirements as per:

a) The Memorandum of Understanding between the Government of the UK and the Government of Ireland on information sharing arrangements relating to Sex Offenders.

b) The Criminal Justice Inspection report on the Management of Sex Offenders in Northern Ireland, (2005) i.e.

Recommendations No 4 (page 10) and at Para 2.15 (page 23) "*Inspectors would encourage progress in respect of Recommendation 291 of the Criminal Justice Review which suggests a coordinated cross-border approach to dangerous offenders"*

Recommendation 291 of the Review of the Criminal Justice System in Northern Ireland refers to dangerous offender registers and consideration to sharing information between the authorities in the two jurisdictions so that there can be a co-ordinated approach to dangerous offender registers (Criminal Justice Review Implementation Plan November 2001)

c) The Probation Service (Ireland) Protocol for Service Operation of Part 5 of Sex Offender Act 2001

d) The SOMEC European Union (Serious Offending by Mobile European Criminals) initiative project which aims to improve cross-border information sharing on serious violent or sexual offenders travelling across the European Union

and

e) Co-operation on Criminal Justice Matters through the work of the Public Protection Advisory Group, under the Inter-Governmental Protocol

3. APPLICATION

3.1 This protocol applies to persons who:

a) Are subject to the notification requirements of part 2 of the Sexual Offences Act 2003 (Northern Ireland) or Part 2 of the Sex Offenders Act 2001 (Ireland) and are subject to supervision by the probation service in either jurisdiction, or

b) Have been convicted of a sexual offence (but are not subject to supervision orders) and are leaving prison, or

c) Whose current offence is not a sexual one, but who have a previous conviction for a sexual offence and who are currently subject to supervision.

d) Offenders in Northern Ireland who have been assessed as a Risk of Serious Harm to others in accordance with PBNI Policy (2013) are currently subject to a Licence or Order in Northern Ireland and

e) Offenders in the Republic of Ireland who are assessed as being a Risk of Serious Harm to others and who are subject to Probation Supervision.

3.2 For the purposes of this protocol 'move' is defined as:

- A planned change of residence to the adjacent jurisdiction
- An unplanned or unauthorised move to the adjacent jurisdiction
- Offenders who are working or regularly visiting within the adjacent jurisdiction
- Offenders who cannot be traced and there is a reasonable concern they may currently be/or likely to cross into the adjacent jurisdiction.

3.3 From this point, persons subject to this protocol will be referred to as:

a) Sex Offenders

b) Offenders assessed as Risk of Serious Harm to others (RoSH)

4. PURPOSE

4.1 The purpose of this protocol is to facilitate the exchange of personal data and other information to enable the Probation Board for Northern Ireland (PBNI) and the Probation Service (Ireland) (PS) to:

- Agree voluntary arrangements for community sentences
- Agree voluntary arrangements for post custodial supervision
- Share information for the preparation of pre-sentence reports on sex offenders and Offenders assessed as Risk of Serious Harm to others who move between respective jurisdictions in Ireland
- Enhance public protection in both jurisdictions.

4.2 The parties agree that the personal data and sensitive personal data obtained through the protocol shall not be used for any purpose other than that specified at 4.1, and shall not be

shared with any other individual or group, other than in circumstances where disclosure is required by law or in the interests of public protection.

4.3 Where there is a clearly identified risk to the public in Northern Ireland, PBNI will share information on an individual Sex/RoSH Offender with Police Service for Northern Ireland (PSNI) and/or Health & Social Care Trusts in accordance with current Public Protection Arrangements for Northern Ireland (PPANI) and PBNI Child Protection procedures.

4.4 Where there is a clearly identified risk to the public in Republic of Ireland, the Probation Service will share information on the relevant Sex/RoSH Offender with the Garda Síochána and / or Child and Family Agency in accordance with the Sex Offender Risk Assessment and Management (SORAM) Procedures / Probation Service Child Protection Policy 2009 / Data Protection Act 1998 / 2003.

5. PARTIES TO THE PROTOCOL

The Probation Board for Northern Ireland (PBNI)
The Probation Service (Ireland)

6. DEFINITIONS IN RESPECT OF THE DATA PROTECTION ACT 1998 AND DATA PROTECTION ACT 1988 AND 2003

See Appendix 1

7. OPERATIONAL PROCEDURES FOR THE SHARING OF INFORMATION

7.1 Sender's Role: This is the Area Manager (AM), PBNI /Senior Probation Officer (SPO), Probation Service, in the jurisdiction where the offender is currently being supervised or residing.

It is the Sender's responsibility, on becoming aware of an offender who has or is preparing to move as defined in paragraph 3.2.

Advise the Area Manager (AM) or Senior Probation Officer (SPO) in the adjacent jurisdiction – this should initially be done by phone[1]

1. Advise **your** Assistant Director (PBNI) or Regional Manager (Probation Service)
2. Send collated information, by encrypted email as referred to in para 7.3, to your single point of contact for **your** organisation within 3 working days

[1]For out of office hours contacts, Probation Service staff will phone PBNI's out of hours number **048 9056 5795 -** PBNI staff will telephone the Probation Service on **00353(0)862416429 / (0)868179609**

3. If appropriate, advise Garda/PSNI and/or Social Services / Child and Family Agency as per current public protection and/or child protection arrangements.

7.2 Receiver's Role: This is the AM/SPO in the jurisdiction to which the offender has moved.

On receiving information under the protocol it is the responsibility of the AM/SPO to:

1. Advise **your** Assistant Director or Regional Manager.
2. On approval from Assistant Director/Regional Manager allocate a Probation Officer (in case where offender has moved to jurisdiction).
3. If appropriate advise local police and/or social services as per current public protection and/or child protection arrangements.
4. Ensure offender's details are recorded appropriately, including on electronic information systems where appropriate.

7.3 Single Point of Contact Role; (SPOC)

The role of the SPOC is to act as a central point of contact within each jurisdiction for the collation and communication of all transfer requests and information exchanges.

Northern Ireland	
Email	intdesk.pbni@pbni.gsi.gov.uk
Phone	04890 262469
Mobile	0044 7789412608

Republic of Ireland	
Email	internationaldesk@probation.ie
Phone	0035318173600
Mobile	00353862546987

The SPOC, on being advised by their AM/SPO of a change in an individual's circumstances, is to:

- Collate the detailed information and forward electronically to the single point of contact in the receiving jurisdiction within one working day

- The receiving SPOC is to forward the information electronically on to the relevant AM/SPO in the receiving jurisdiction within one working day.

7.4 Operational Procedures for Voluntary Supervision

7.4.1 Where an offender on supervision indicates his intention to move to the other jurisdiction, he should be advised of the arrangements for supervision.[2]

7.4.2 Process to be followed:

1. The AM/SPO (sending) should contact **their** SPOC
2. The SPOC will liaise with their counterpart in the adjacent jurisdiction who will then inform the relevant AM/SPO of the request for voluntary supervision
3. Once this has been approved by the Assistant Director/Regional Manager the AM/SPOs are to make the arrangements for the case transfer.

7.4.3 The proposed address should be supplied as well as any details and information relevant to the assessment of risk in the new circumstances.

7.4.4 The SPO/AM receiving will arrange for a home visit or office interview with relevant people (e.g. proposed employer or head of household of proposed residence).

7.4.5 Offenders will be supervised in accordance with practice standards extant in the receiving jurisdiction.

7.4.6 Where child protection concerns arise, the SPO/AM will inform the relevant Social Services/ Child and Family Agency.

7.4.7 The PPANI Administration Unit (Northern Ireland) or Regional Manager, (Republic of Ireland) will be informed by the receiving AM/SPO as deemed appropriate according to assessed level of risk. (see 4.3)

7.4.8 In the event of failure to co-operate with voluntary supervision, the receiving SPO/AM will provide all information to the sending SPO/AM to facilitate enforcement in the sending jurisdiction[3].

7.4.9 In cases where an offender has moved without authorisation, the receiving probation service shall consider offering the offender voluntary supervision. This offer of voluntary supervision will not obviate the enforcement responsibilities of the Agency which holds statutory responsibility for supervision of the offender.

[2] These arrangements for voluntary supervision exclude offenders subject to Determinate Custodial Sentences (DCS) or Public Protection Sentence as per Criminal Justice (NI) Order 2008 where offenders are required to reside in the jurisdiction of the United Kingdom.

[3] This information will be communicated through the SPOC in both jurisdictions, as occurs with the original referral

8. DESCRIPTION OF DATA TO BE SHARED

8.1 In the case of an offender proposing to move, or have reported to have moved residence (to the other jurisdiction), a report should be prepared for the purpose of sharing relevant information.

8.2 For the purpose of this protocol the following information will be shared at the outset:

- Name/Alias/Date of Birth/Current address
- Current/previous offence
- Type of order/licence including details of restrictions and/or requirements
- Existence of any other court orders
- Summary of Criminal Record (The Criminal Record must not be attached).
- Most recent work plan and summary of Risk Management Meeting where applicable and where available the RM2000 and SA07 and PSROSH/PSROSH (SO) assessment outcomes, or equivalent.
- Response to supervision
- Current social circumstances for example, employment/accommodation/ lifestyle/associates. Any known supports
- Any information about proposed address
- Length of proposed stay, if known
- Particular areas of concern.

9. SHARING OF INFORMATION – CONSENT

9.1 Obtaining consent remains a matter of good practice and, in circumstances where it is appropriate and possible, explicit consent should be sought from and freely given by the data subject. The individual should always be informed about how their information will be used and with whom it may be shared even if consent not required.

However, in many cases seeking consent might not always be possible or appropriate. In such cases the disclosing body must consider the possible grounds which may give cause to override consent.–See Appendix 2 (Legislative requirements - Public Interest)

10. UNDERLYING PRINCIPLES FOR INFORMATION SHARING

10.1 Each of the parties is responsible for their own information and therefore must be sure that they have the power to disclose the relevant information in each particular case.

Personal information should only be shared when the disclosing party is satisfied that

(i) They are legally empowered to do so

(ii) The proposed disclosure of personal information can be done in accordance with the Principles of the Data Protection Act (1998 for NI) and 1988 & 2003 (Ireland).

(iii) They can disclose personal information reflecting the common law duty of confidentiality and

(iv) The Principles of the Human Rights Act 1998 (NI) and the European Convention of Human Rights Act 2003 (Ireland).

10.2 The information that is shared in accordance with this protocol will be:

a. Treated in the strictest confidence

b. Where applicable, appropriate protectively marked in accordance with respective protective marking policies.

c. Used only for the purposes set out in this protocol

d. Used only by those authorities with a statutory duty to pursue those purposes.

10.3 The protocol will be operated within the context of the individual's rights and protection enshrined in legislation.

10.4 <u>PBNI Legal Authority</u>

The Probation Board (Northern Ireland) Order 1982
The Criminal Justice (Northern Ireland) Order 2008
The Sexual Offences (Northern Ireland) Order 2008

10.5 <u>Probation Service Ireland Legal Authority</u>

The Probation of Offenders Act 1907
The Criminal Justice Act, 2006
The Sex Offender Act 2001
Criminal Justice (Temporary Release of Prisoners) Act 2003

10.6 Other relevant key legislation and guidance

The Data Protection Act 1998

The Data Protection Acts 1988 and 2003

The Human Rights Act 1998

European Convention of Human Rights Act 2003

The Freedom of Information Act 2000

The Freedom of Information (Amendment) Act 2003

The Common Law Duty of Confidentiality

Memorandum of Understanding between the Government of the UK and the Government of Ireland on information sharing arrangements relating to Sex Offenders

Information Commissioner's Office (ICO) Data Sharing Code of Practice.

Data Protection Commissioner – relevant guidance.

10.7 The sharing of information under this protocol is compliant with both parties 'registration arrangements with the Information Commissioner (UK) or the Data Protection Commissioner (Ireland) under the respective Data Protection Acts.

11. ACCESS AND INDIVIDUALS' RIGHTS (REQUESTS FOR INFORMATION)

11.1 The parties to the protocol recognise that when responding to requests for information under the Freedom of Information Act 2000 (UK) or Freedom of Information Act 1997 and the Freedom of Information (Amendment) Act 2003 (Ireland) or in fulfilling their statutory obligations under section 7 of the Data Protection Act 1998 (UK), or Section 4 Data Protection Act 1988 (Ireland) that it would be good practice to consult the party from whom information has been received before disclosing it.

Consultation will allow a party to ascertain whether any of the exemptions set out in the relevant and respective legislation apply to that information.

The party to whom the request was made will respond to it. The request will only apply to information shared for purposes of this protocol.

11.2 The parties agree to provide reasonable assistance to one another to enable them to respond to such a request within the timescales set out in the relevant legislation i.e. 40 days in respect of Data Protection and 20 working days in respect to Freedom of Information.

11.3 Information will be released in accordance with the relevant legislation unless an exemption applies.

11.4 The Probation Board and Probation Service Ireland will adhere to their obligations to maintain a publication scheme in accordance with the Freedom of Information Acts. Consideration will be given to this agreement, when completed, being made available for publication on respective websites (subject to any exemptions).

12. INFORMATION GOVERNANCE[4] (See Appendix 4)

This sets out the key responsibilities of each party in respect of the Data Protection Principles.

13. TRAINING

13.1. Each party must ensure that adequate training is provided to staff involved in the sharing of information under this protocol so that they are aware of their legal responsibilities in this regard. Both parties will ensure that staff are aware that they may be subject to disciplinary and/or legal proceedings should there be any breaches of the Data Protection Act arising out of the operation of this protocol.(see also section 12, Appendix 4)

14. COMPLAINTS

Complaints to either of the parties should be dealt with through the respective organisation's complaints procedure.

15. SENIOR MANAGEMENT COMMUNICATIONS

15.1 In the event of media interest in relation to an offender subject to this protocol the relevant senior manager[5] shall contact his/her counterpart in the relevant jurisdiction. The respective PR/Communications departments should also be consulted.

15.2 In respect of NI, in the event of a decision to make public disclosure with regard to an offender subject to this protocol, the relevant senior manager from PBNI will contact their counterpart in the Probation Service.

15.3 In the event of a serious incident/situation involving an offender subject to this protocol the relevant senior manager will contact their counterpoint to share immediate information and to agree steps to be taken to manage the situation.

[4] Ref First Schedule, Chapter 11 of the Data Protection Act 1988 the Data Protection (Amendment) Act 2003, and Part 1 Section 4 of the Data Protection Act 1998

[5] The relevant senior manager for PBNI is the Assistant Director for Risk. PS is Assistant Director for Risk and Resettlement

16. MONITORING AND REVIEW

This protocol will be monitored on a regular basis to allow either party to advise of changes or raise concerns as required. The relevant senior managers will liaise directly at least on a bi annual basis to monitor the application and operation of the protocol.

The protocol will be formally reviewed every two years from date of commencement (para 1.3) or earlier at the request of either party or to take account of any legislative changes which impact on the protocol. All changes to the protocol are to be agreed and approved by both signatories prior to the changes taking place.

17. SIGNATORIES

We, the undersigned have read and agree to this protocol between The Probation Board for Northern Ireland and The Probation Service (Ireland), to carry out our roles and responsibilities and to share and provide the information as outlined in this protocol.

17.1 Signed for: Probation Board for Northern Ireland

Name: _____
(Print)
Position: _____

Signature: _____

Date: _____

Signed for: The Probation Service (Ireland)

Name: _____
(Print)
Position: _____

Signature: _____

Date: _____

Appendix 1

Definitions

Data Protection Act 1998 (UK) Chapter 29, Part 1 Preliminary

1. Data

Information which:

a) is being processed by means of equipment operating automatically in response to instruction given for this purpose;
b) is recorded with the intention that it should be processed by such equipment;
c) is recorded as part of a relevant filing system; or
d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68 of the Data Protection Act 1998
e) is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d)

Note: Under the Freedom of Information Act 2000 ***S.69 (2)*** *the meaning of personal data has been extended (for public authorities) to include "unstructured personal data". (UK)*

2. Data Controller

A person who (either alone or jointly in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be processed.

3. Data Processor

Any person who, in relation to personal data (other than an employee of the Data Controller) who processes the data on behalf of the Data Controller.

4. Data Subject

An individual who is the subject of the data

5. Personal Data

Data which relate to a living individual who can be identified-

a) from those data; or

b)from those data and other information which is in the possession of, or is likely to come into the possession of, the Data Controller, and includes any expression of opinion about the individual and any indication of the intentions of the Data Controller or any other person in respect of the individual

6. Processing

Means obtaining, recording or holding information or data or carrying out any operation or sets of operations on the information or data, including:

a) organisation, adaptation or alteration of the information or data;
b) retrieval, consultation or use of the information or data;
c) disclosure of the information or data by transmission, dissemination or otherwise making available; or alignment, combination, blocking, erasure or destruction of the information or data

7. Sensitive personal data

Personal data consisting of information as to:-

a) the racial or ethnic origin of the data subject;
b) his political opinions;
c) his religious beliefs or other beliefs of a similar nature;
d) whether he is a member of a trade union
e) his physical or mental health or condition;
f) his sexual life;
g) the commission or alleged commission by him of any offence; or
h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

Data Protection Act 1988 (Republic of Ireland) Number 25, Preliminary & First Schedule, Chapter 1, Article 2 and Data Protection Act (Amendment) 2003 Section 2

1. **Data** means information in a form in which it can be processed*:*

2. **Data controller** means a person who, either alone or with others, controls the contents and use of personal data

3. **Data equipment** means equipment for processing data

4. **Data material** means any document or other material used in connection with, or produced by, data equipment

5. **Data processor** means a person who processes personal data on behalf of a data controller but does not include an employee of a data controller who processes such data in the course of his employment

6. **Data subject** means an individual who is the subject of personal data

7. **Personal Data** means any information relating to an identified or identifiable individual ("Data Subject")

8. **Automated Data File** means any set of data undergoing automatic processing

9. **Automatic processing** includes the following operations if carried out in whole or in part by automated means: storage of data, carrying out of logical and/or arithmetical operations on those data, their alteration, erasure, retrieval or dissemination.

10. **Sensitive personal data** means personal data as to—

(*a*) the racial or ethnic origin, the political opinions or the religious or philosophical beliefs of the data subject,
(*b*) whether the data subject is a member of a trade union,
(*c*) the physical or mental health or condition or sexual life of the data subject,
(*d*) the commission or alleged commission of any offence by the data subject, or
(*e*) any proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings;

Appendix 2

LEGISLATIVE REQUIREMENTS (NI) CONSENT (Para 9.1)

1. Northern Ireland - <u>Public Interest</u>

If consent has been sought and refused, or if it would prejudice the work of the Probation Board for Northern Ireland, in this instance, to seek consent, an overriding public interest may justify disclosure of information.

The criteria for public interest includes:

- The administration of justice
- Maintaining public safety
- The apprehension of offenders
- The prevention of crime and disorder
- The detection of crime
- The protection of vulnerable members of the community

When judging the public interest it is necessary to consider the following:

- Is the intended disclosure proportionate to the intended aim?
- What is the vulnerability of those who are at risk?
- What is the likely impact of the disclosure on the offender
- Is there another equally effective means of achieving the same aim?
- Is the disclosure necessary to uphold the rights and freedoms of the public?
- Is it necessary to disclose the information/data to protect other vulnerable people?

The rule of proportionality should be applied to ensure that a fair balance is achieved between the public interest and the rights of the data subject.

2. LEGISLATIVE REQUIREMENTS: IRELAND Public Interest: Section 8 of the Data Protection Acts 1988 & 2003

This section of the Act lifts the restriction on disclosure in certain circumstances, so that disclosures may be made in cases where the individual's right to privacy must be balanced against other needs of civil society including:

- Section 8(b) "required for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders…"
- Section 8(d) "The disclosure is required urgently to prevent injury or other damage to the health of a person or serious loss of or damage to property".

Disclosures Permitted under section 8 of the Data Protection Acts 1988 & 2003

Section 2(1) (c) of the Data Protection Acts, provides that a data controller shall not further process personal data (which includes disclosure to a third party), except in ways that are compatible with the purpose for which the data were obtained.

However, this non-disclosure rule is not unqualified. Section 8 of the Act lifts the restriction on disclosure in certain circumstances, so that disclosures may be made in cases where the individual's right to privacy must be balanced against other needs of civil society, or where the disclosure is in the interests of the individual. The circumstances specified in section 8 are listed below, along with some explanatory comments.

Section 8(b) *"required for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders or assessing or collecting any tax, duty or other moneys owed or payable to the State, a local authority or a health board, in any case in which the application of those restrictions would be likely to prejudice any of the matters aforesaid"*

Comment: The individual's right to privacy must be balanced against the need to investigate offences and collect taxes effectively. If a data controller is approached by a law enforcement authority or by a tax collecting authority, which seeks to have personal data disclosed to it under this section of the Data Protection Act, it is a matter for the data controller: (i) to satisfy itself that the provisions of this section are met, for example by establishing the bona fides of the authority and by obtaining assurances that the disclosure is actually necessary, and not merely of side interest, for the investigation of an offence; and (ii) to decide whether or not to comply with the request for disclosure. While this section of the Data Protection Act lifts the restrictions on disclosure by a data controller to a law enforcement authority or to a tax collecting authority, this section does not impose any obligation on a data controller to comply with the request for disclosure.

Section 8(d) *"The disclosure is required urgently to prevent injury or other damage to the health of a person or serious loss of or damage to property"*

Comment: The individual's right to privacy can be set aside where personal data must be disclosed in order to save someone's life or protect someone's health, or to prevent property from being destroyed. This provision does not authorise disclosures of personal information for general health research purposes, or for other medical purposes where there is no immediate or urgent risk to someone's life or health. In such cases, the normal data protection rules apply, including the obtaining of consent where necessary.

Section 8(e) *"required by or under any enactment or by a rule of law or order of a court"*

Comment: If you are under a legal obligation to disclose personal data, then this obligation takes precedence over the Data Protection Act's prohibition on disclosure. However, if you have a statutory discretion to make information available, matters are not so clear-cut. The Data Protection Commissioner has found, in the past, that a statutory discretion to make information available did not come within the scope of section 8(e) of the Data Protection Act, and that accordingly the restriction on disclosure of personal data remained in force.

Section 8(h) *"made at the request or with the consent of the data subject or to a person acting on his behalf"*

Comment: If a third party, such as a prospective employer, requests personal information from you about an individual, and if the third party has the clear consent of that individual, then you may disclose the personal data, if you wish. This section of the Data Protection Act places you under no obligation to respond positively to the request for information, if you do not want to[6].

Rights and restrictions regarding the disclosure of information are also governed by the Freedom of Information Acts 1997 and 2003. The main purpose of this legislation is:

"To enable members of the public to obtain access to the greatest extent possible consistent with the public interest and the right to privacy, to information in the possession of public bodies".

[6] Data Protection Commissioner's Office.

APPENDIX 3

CONDITIONS RELEVANT FOR PURPOSES OF THE FIRST PRINCIPLE:

PROCESSING OF ANY PERSONAL DATA

The Data Protection Act 1998 requires that at least one condition from those listed in Schedules 2 and 3 to the Act apply in relation to the processing of personal data and sensitive personal data. The relevant conditions are listed below in an abridged form (please refer to the Data Protection Act for detail).

Conditions in Schedule 2:	Conditions in Schedule 3:
Paragraph 1: The data subject has given consent to the processing.	**Paragraph 1:** The data subject has given explicit consent to the processing.
Paragraph 2: The processing is necessary for (a) the performance of any contract to which the data subject is a party; or (b) for the taking of steps at the request of the data subject with a view to entering into a contract.	**Paragraph 2:** (1)The processing is necessary for the purposes of exercising or performing a legal right or obligation in the context of employment.
Paragraph 3: The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.	**Paragraph 3:** The processing is necessary (a) to protect the vital interests of the data subject or another person in a case where – (i) consent cannot be given by or on behalf of the data subject, or (ii) 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.
Paragraph 4: The processing is necessary in order to protect the vital interests of the data subject.	**Paragraph 4:** The processing is of political, philosophical, religious or trade union data in connection with its legitimate interests by any non-profit bodies.
Paragraph 5: The processing is necessary: (a) for the administration of justice; (b) for the exercise of any functions conferred on any person by or under any enactment; (c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department; or (d) for the exercise of any other functions of a public nature exercised in the public interest by any person.	**Paragraph 5:** The processing is of information made public as a result of steps deliberately taken by the data subject. **Paragraph 6:** The processing is necessary in connection with legal proceedings or the seeking of legal advice. **Paragraph 7: (1)**The processing is necessary (a) for the administration of justice; (b) for the exercise of any function conferred on any person by or under any enactment; (c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department.
Paragraph 6(1): 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 where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.	**Paragraph 8:** The processing is necessary for medical purposes and is carried out by medical professionals or others owing an obligation of confidence to the data subject. **Paragraph 9:** The processing is necessary for ethnic monitoring purposes.
Paragraph 6(2): The Secretary of State may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied.	**Paragraph 10:** The personal data are processed in circumstances specified in an order made by the Secretary of State for certain purposes. The Data Protection (Processing of Personal Data) Order 2000 (SI 2000 No 417) specifies a number of circumstances in which sensitive personal data may be processed such as crime prevention, policing and regulatory functions (subject to a substantial public interest test);

Appendix 4

Information Governance

1. Fair and Lawful

Both parties agree that personal data shall be processed fairly and lawfully and in particular shall not be processed unless certain conditions are met as required by Principle 1 of the Data Protection Act 1998 and First Schedule, Chapter 11 Article 4 of the Data Protection Act 1988.

Where information is shared under the terms of this Protocol for the purposes set out para 4 the following conditions are relevant.

- (Ireland) Section 8 (b), See Appendix 2
- (NI) Schedule 2 paragraphs 1, 2(a), 6.1 & Schedule 3 paragraphs 1, 3, 7(a), See Appendix 3

2. Common Law duty of Confidentiality

Where an organisation owes a common law duty of confidentiality, that duty of confidentiality continues to apply. Where consent cannot be obtained from the data subject to share/disclose his or her personal data with the other agency, that agency must consider whether they have sufficient public interest grounds to override this duty. If the organisation does not consider that there is sufficient overriding public interest to make the disclosure it must not do so.

3. Human Rights Act 1998

Article 8 of the Human Rights Act 1998 states that everyone has the right to respect for his private and family life, 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 and is necessary in a democratic society in the interests of:

a) National Security
b) Public Safety
c) Economic well-being of the country
d) The prevention of crime and disorder
e) The protection of health or morals
f) The protection of the rights or freedoms of others

If the disclosure of data will in some way infringe the rights of the data subject we will consider the rule of proportionality. This is to ensure that fair balance must be achieved between the protection of the individual's rights, with the general interests of society.

4. European Convention on Human Rights Act 2003 (Ireland)

Article 8 of the European Convention on Human Rights Act 2003 states that 1) everyone has the right to respect for his private and family life, home and his correspondence and

There shall 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 interests of national security, public safety or the economic well-being 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.

5. Limited Purposes

Both parties agree that information will not be used for any other purpose than for which it was given (para 4) and will not be disclosed to another agency or body without the permission of the party which provided the information.

6. Adequate, Relevant and Not Excessive

Both parties agree that only the minimum data necessary will be exchanged to satisfy the purpose of the disclosure.

7. Data Quality

Both parties agree to ensure that the data shared is as far as reasonable accurate and up to date. Both parties agree that data discovered to be inaccurate or inadequate for the specified purpose will be brought to the notice of the originator of the data. The originator will be responsible for correcting the data and notifying all other recipients of the corrections.

8. Retention and Destruction of the Data

Both parties agree that the relevant data will be retained by the party to whom it is disclosed until such times as it is no longer required for the purposes of any legal action or appeal process.

At the expiry of this period the party to whom it had been disclosed will destroy the relevant information securely in keeping with that organisations retention and disposal policy and in accordance with the Government Protective Marking scheme, if relevant..[7]

9. Security

Both parties to this protocol are responsible for ensuring that they have appropriate security arrangements in place. They will consider how the relevant data will be stored, accessed and transmitted. The single point of contact for each party will ensure that adequate steps are taken to prevent:

a) accidental or deliberate destruction of the data;
b) accidental or deliberate modification of the data;
c) deliberate and unauthorised unavailability of the data;
d) unauthorised access to information to any computer system containing the data;
e) misuse of the data

10. The information to be shared by PBNI, for purposes of this protocol, will be protectively marked as OFFICIAL-SENSITIVE under the current Government Protective Marking Scheme (includes hard copy and if sent via secure email). This will depend on the sensitivity of the information disclosed. Information for example which includes references to offences, court disposal or risk, should be marked OFFICIAL-SENSITIVE.

11. Personal and sensitive personal information, if sent electronically, will **only** be sent to a PBNI and Probation Ireland approved secure email address. (see 7.3)

12. Secure briefcases, where available, should be used when transporting manual personal or sensitive personal information. Personal or sensitive information shall not be left unattended by any of the parties.

13. Each party will adhere to their respective organisation's data handling policies and procedures – e.g. Records Management, Management of Information, and Security.

14. Protectively marked information, when posting, should be only be sent by special delivery, double enveloped, with inner envelope marked as restricted or protect (depending on the sensitivity of the information contained).

[7] Changes to the current protective marking scheme (UK) are due to be implemented in April 2014

15. Breaches

Both parties will ensure that staff are aware that they may be subject to disciplinary and/or legal proceedings should there be any breaches of the Data Protection Act arising out of the operation of this protocol. This may be as a result of not adhering to the correct data handling procedures for the exchange of information or through the wrongful disclosure of information or the withholding of relevant personal information in respect of this protocol. This may also result in enforcement action by the Information Commissioner's Office and/or the Data Protection Commissioner (Republic of Ireland).

16. All suspected or confirmed breaches of protectively marked/sensitive information including information which has been lost or inadvertently disclosed must be reported immediately upon discovery. The relevant organisation's data loss/incident response plan must be engaged and the single point of contact for each party (para 7.10) must be informed. Relevant line managers must also be informed.

17. In respect of PBNI, this should be done, where possible, via email in the first instance to the Information Security Officer at infosec@pbni.gsi.gov.uk
Please ensure that you also information your line manager of the situation.

18 In respect to Probation Service, Ireland, this should be done, where possible, via email in the first instance to the Data Protection Officer at: foi@probation.ie
Please ensure that the Director of Operations is made aware of the situation through your line manager.

19. Each organisation must ensure that it is familiar with the relevant Information/Data Commissioner's Guidance on data security breach management and its guidance/codes on how and when to notify the respective Information Commissioner's Office/Data Protection Commissioner in the event of a breach.