



Association of Chief Police Officers of England,
Wales & Northern Ireland

INFORMATION SHARING AGREEMENT ASSOCIATION OF CHIEF POLICE OFFICERS (ACPO) AND THE NATIONAL OFFENDER MANAGEMENT SERVICE (NOMS)

Status: [To be completed by the ACPO Office at the time of publication]

**Implementation
Date:**

Review Date:

Information Sharing Agreement

For the provision of Pre and Post-Sentence Information by the Police Service to Probation Trusts to enhance preparation of Pre-Sentence Reports and the risk assessment and risk management of all offenders with whom the probation service has statutory contact.

**Association of Chief Police Officers
(ACPO)**

and the

**National Offender Management Service
(NOMS)**

Index

Introduction	Page 4
Section 1. Purpose of the Information Sharing Agreement	Page 5
Section 2. Specific purpose for disclosing information	Page 7
Section 3. Information to be disclosed	Page 9
Section 4. Process	Page 11
Section 5. Information passed onto other parties	Page 14
Section 6. Agency liability	Page 15
Section 7. Review and retention	Page 16
Section 8. Breach of confidentiality	Page 17
Section 9. Dispute resolution	Page 18
Section 10. Signatures	Page 19
Appendix A. ACPO Workbook	Page 20
Appendix B. Legal Considerations	Page 30
Appendix C. Proforma	Page 38
Appendix D. Government Protective Marking Scheme	Page 40
Appendix E. Police National Intelligence Model 5x5x5 Grading	Page 41

Introduction

The primary objectives of the National Offender Management Service (NOMS) are to reduce re-offending and to protect the public. The role of Probation Trusts is crucial in supporting these objectives, through assessing and managing the risk of defendants subject to bail, and post-conviction, offenders who are subject to statutory supervision. They also play a critical role in supporting the sentencing process in courts through the preparation of pre-sentence reports (PSRs). Currently, in order to fulfil both these obligations, probation staff are required to make professional judgements based amongst other things upon the results of various assessment tools such as the Offender Group Reconviction Scale (OGRS) and the Offender Assessment System (OASys). In addition to other sources of information, these tools use statistical information, the information gleaned from the offenders themselves, information from the police concerning conviction history in the form of a Police National Computer (PNC) printout and sanitised information from ViSOR, used with permission of the source/originator.

There has been both research and also the recommendations of various high profile reports following the commission of serious offences¹ which have shown that more information is often available but not used in making decisions around risk. These reports and other enquiries highlighted the failures in processes for sharing information more generally. However, each has strongly indicated that risk management decisions could and should be enhanced if information from other sources and other types of information is made available.

The Statutory Code of Practice for the Management of Police Information was enacted following the Bichard enquiry. The Code and its associated guidance ensure consistency between forces in relation to the management of information. Chief Officers of Police have a duty to obtain and use a wide variety of information (including personal information) for the effective discharge of their legal responsibilities in compliance with the law, specifically the Data Protection, Human Rights and Freedom of Information Acts. The Code ensures that procedures are in place for the effective use and availability of information within and between forces and partnership agencies and where appropriate, the public.

Not all offending results in conviction. Narrowing The Justice Gap (2002) detailed the attrition rate which in 2000-01 showed that only 19.8% of crimes recorded resulted in an offender being brought to justice. Arrest activity related to incidents strongly believed to have happened but which could not be proved, may be indicative of a pattern or emerging pattern of behaviour and therefore can be significant in assessing the risks an offender may present to the public.

Although risk posed by offenders in the community can never be fully eliminated, only managed, the police service holds key information about many offenders that under existing arrangements is sometimes not available to inform decisions taken by probation staff.

The arrangements in this information-sharing agreement (ISA) support and complement existing information sharing arrangements for specific groups of offenders, e.g. MAPPA, joint working on Prolific and Priority Offenders (PPOs) and those offenders concerned with cases subject to the Multi Agency Risk Assessment Conference (MARAC) process. It formalises current ad hoc arrangements for sharing information on offenders who present

¹ For example, the cases of: Hanson and White, Rice, Sonnex and the Climbie and Bichard Enquiries

risks but are not covered by MAPPA, PPO or MARAC frameworks. While it sets out principles to be adhered to as good practice, it is not intended to preclude the proactive sharing of information on a case-by-case basis where risks are identified. Fundamentally, this ISA is intended to emphasise the importance of sharing information in order to protect the public.

Section 1 Purpose of the Information Sharing Agreement

This Information Sharing Agreement (ISA) has been developed to:

- Support appropriate Information sharing between Probation Trusts and the police
- Protect the public from dangerous offenders
- Define the specific purposes for which the signatory agencies have agreed to disclose information.
- Describe the roles and structures that will support the disclosure of information between agencies.
- Set out the legal gateway through which the information is disclosed, including reference to the Human Rights Act 1998 and the common law duty of confidentiality.
- Describe the security procedures necessary to ensure compliance with responsibilities under the Data Protection Act 1998 and other relevant legislation, together with agency-specific security requirements.
- In addition, completion of this document will ensure that the police service can meet the information sharing requirements of the Statutory Code of Practice on the Management of Police Information (MoPI) 2005, and its associated guidance.
- Support the introduction of public protection networks in accordance with Sir Ian Magee's Review of Criminality Information.

Resource Implications

This agreement builds on existing information sharing arrangements and seeks to formalise existing practice. It will provide a consistent standard for information sharing in England and Wales. NOMS and police staff will require briefing in relation to the agreement as part of implementation. As information sharing is already common place in practice, it is not envisaged that local implementation of this agreement will have any significant resource implications.

Police forces and Probation Trusts may want to determine at a local level how this ISA will be audited and should consider that it will be a cause for criticism in Serious Case Reviews (of Serious Further Offences) if it is found that a failure to communicate effectively (as specified in this ISA) has contributed to the committing of an SFO.

Signatories

This agreement has been signed by a senior representative from ACPO and NOMS with a clear commitment that they will facilitate the adoption of this agreement within their organisations. It is expected that all probation trusts and police forces will operate

according to the principles contained within this framework agreement, to enable information sharing both within areas and across area boundaries.

The agencies signing this agreement accept that the procedures laid down in this document provide a secure framework for the disclosure of information between the parties to this ISA in a manner compliant with their statutory and professional responsibilities. As such they will:

- Implement and adhere to the standards for procedures and structures set out in this document.
- Ensure that, providing the provisions of this agreement have been satisfied, no restriction will be placed on the disclosure of information other than those specified within this agreement.
- Ensure that any arrangements developed locally between the partner agencies comply with the principles and general procedures contained within this ISA.
- Engage in a review of this agreement 12 months after its implementation and thereafter on a yearly basis or as and when required.

Section 2 Specific Purpose for Disclosing Information

This document proposes a rationale for the police service to provide in certain circumstances (see Section 4) more detailed information to probation trusts, including arrest history and where proportionate to the management of risk, other non-conviction information. In order to formalise the provision of this information and to ensure that as robust a process as possible is constructed and maintained, the legal, security and procedural issues surrounding this process will be captured in this document.

As mentioned previously, this document is intended to promote appropriate information sharing whilst at the same time ensuring decisions are legally justifiable. Appendix B provides details of the relevant legislation regarding disclosure of information. It is anticipated that the overwhelming majority of such decisions will be covered by this agreement and will be straightforward. However, it is possible that a situation could arise where further legal advice may need to be sought. Staff should seek legal advice where there is any doubt about the legality of the basis for sharing information.

Stages or activities along the offender pathway at which a request for police information might be sought would include:

- Bail information to inform bail conditions and assessments regarding suitability for placement in accommodation
- Pre-Sentence Reports
- OASys Assessment and Reviews
- Other specialist assessments
- Sentence Planning
- Unpaid Work placement decisions
- Victim Liaison
- Assessment for licence conditions
- Home Detention Curfew assessments
- Parole reports and Parole Board Reviews/Oral Hearings
- Recalls
- Any other circumstance justifiable on public protection grounds, e.g. domestic abuse enquiries.

Where an enhanced CRB check has been requested in respect of an offender's unpaid work placement, it is unlikely that there will be a need to make an additional request for information from the police.

Pre-Sentence

Arrest history can help to enhance the overall picture of the offender's potential range and volume of offending behaviour when combined with conviction information already available to the probation service. Equally, a record of call outs to domestic abuse incidents may not result in any charge but can provide valuable background and behavioural information which will be helpful in determining, for example, the appropriateness or otherwise of an accredited programme.

Other intelligence concerning allegations or information in relation to sexual and/or violent offences (in particular in relation to children) would also be relevant. This may include sharing information on the existence of a Sexual Offences Prevention Order (SOPO), Risk of Sexual Harm Order (RSHO) or Violent Offender Order (VOO).

Arrest history can be used as an enquiry trigger (e.g. sexual offences) to encourage greater disclosure by the offender of patterns of offending behaviour. Without such information risk assessments in certain cases may be less comprehensive, potentially leading to sentencing proposals which do not adequately address the risks the offender presents. Where police hold such information which could support appropriate sentencing (and subsequent case management) decisions and they are aware of probation involvement with a case, they should share it, where it is necessary and proportionate to the risk that individual poses, to ensure compliance with the Data Protection Act 1998 or Human Rights Act 1998.

Arrest history, or other information provided pre-sentence, *must not* result in a proposal for a more onerous sentence for the offender, but may result in a more appropriate one, e.g. when assessing which requirements are most suitable in a Community Order. The overall 'punitive weight' of the sentence must be proportionate to the court's assessment of seriousness, but the specific make-up of that sentence should appropriately address the offender's risks and needs.

When sharing information pre-sentence it must be appropriately graded to ensure future handling instructions are clear. It should be borne in mind that information on which a pre-sentence report recommendation is based may be challenged by, and hence made available to, the defence. If such information is sensitive and may result in harmful implications should it be passed on then due consideration should be given to whether it is appropriate to share the information.

Post-sentence

While an offender is being managed by a probation offender manager, ongoing reviews and risk assessments are taking place. Without relevant and proportionate information from police sources about the history and behaviour of the offender, there is a major risk of an inaccurate assessment being made. An offender may remain on an unsuitable community programme for example, with the risks highlighted above or, in more extreme cases, an opportunity to intervene to prevent a more serious offence is lost.

After the initial enquiries, ongoing information exchange between police and probation will ensure that offenders serving community and custodial sentences are managed comprehensively and risks to the public are minimised. Staff are reminded that for violent offenders and sexual offenders subject to active multi-agency management within MAPPA there should be a ViSOR Nominal Record available for initial information exchange. There will also be a nominal record available on all Registered Sexual Offenders managed at MAPPA Level 1. This agreement is not intended to replace existing information sharing processes already in operation in relation to MAPPA, PPO and MARAC cases. Staff are encouraged to continue exchange of information via those processes for such cases.

Section 3 Information to be disclosed

Information to be disclosed by Police to Probation

Pre-sentence

The criteria below limit pre-sentence information sharing to those defendants or offenders whose current conviction or behaviour indicates that they present a potential or actual risk of serious harm to the public.

For offenders charged with or convicted of:

- violent and sexual offences (defined in Criminal Justice Act 2003 Schedule 15)
- other offences motivated by domestic abuse, the targeting of specific groups or individuals, domestic extremism
- offences falling under terrorism legislation or terrorism-related offences
- any offence, but where during interview with probation staff the offender has disclosed information which indicates a potential risk of serious harm to the public,

Probation may, using an agreed and auditable process, request details of the offender's arrest history or other information on the offender held by the police which would be relevant to the assessment of risks posed by the offender, where they do not feel they have sufficient information to properly assess the case. Further information about the circumstances of previous arrests or call out history to a specific address/victim may also be requested. This information will be necessary to assist the probation service to identify any patterns of behaviour that would not be evident by considering conviction information only.

Where the police are already aware of such information that would be relevant to assessing the risks posed by the offender and they are aware of probation involvement with a case, they should share this information using an agreed auditable process, where it is necessary (e.g. for the purpose of effective risk management of offenders) and proportionate (e.g. to the risks posed by that person).

In many cases offenders will acknowledge responsibility for incidents or activities which form part of a pattern of offending behaviour but for which they were not prosecuted or convicted. Nevertheless, caution must be exercised as any information subsequently referred to in a pre-sentence report (e.g. call out history) must be disclosed to and discussed with the offender.

At the same time staff should note that there may be substantive information already available on ViSOR which will be available locally to all Probation staff with a legitimate business reason for accessing the system. However, staff must remember that as a 'Confidential' system ViSOR should not be directly quoted as a source in any reports. Rather, the clearly identified and recorded source of the ViSOR information should be contacted directly and permission sought to include their data within any reports, taking heed of the relevant National Intelligence Model (NIM) grading as referred to later. (Appendix E provides a short guide to the NIM 5x5x5 grading.) This source should be cited on the relevant report or document.

Post-sentence

Requests for police information which could contribute to the ongoing assessment and management of offenders should be prioritised where:

- a) arrest history indicates the offender has previously come to the attention of the police for a violent and/or sexual offence
- b) the offender has a previous conviction for a violent and/or sexual offence but is not currently under supervision for that offence
- c) the offender has disclosed during the course of supervision information which indicates that he or she has the potential to present a risk of serious harm to the public, including domestic or other violent extremism
- d) there is information available suggesting that the offender may be a gang member or involved in a gang
- e) information has come to the attention of probation staff which indicates that the offender may present a risk of serious harm to the public
- f) offenders are being considered for Unpaid Work placements in potentially sensitive settings, e.g. schools (N.B. offenders do not work during school hours but the placement nevertheless remains potentially sensitive.) In accordance with Probation Circular 20/2006 probation staff considering placing offenders in such settings should first consider whether an enhanced CRB check is needed. If so, this would replace the need for a separate information request from the police.

Based upon offender management criteria that are indicative of risk, police, in some circumstances, will supply timely ongoing updates to probation staff. This could include arrests and the circumstances surrounding them, sightings and, in some cases after due consideration using the National Intelligence Model (NIM) 5x5x5 assessment, information from third parties. Such circumstances should be agreed locally by the relevant managers and case officers.

Information to be disclosed by Probation to Police

For any offender in contact with Probation, where information arises that would assist the Police in the prevention and detection of crime, Probation staff will share that information with the Police in line with the terms of this ISA. Again this information can be added, where relevant, to the existing ViSOR Nominal record utilising the agreed methods that exist under the NOMS ViSOR Business Models.

Section 4 Process

Process for managing a request for information

Requests should be made in writing or, where telephone requests form part of the ongoing management of the case, a written record of the request including the justification should be documented on the case file.

Such requests should be responded to appropriately and within a timescale proportionate to the severity and circumstances of the crime being investigated. Probation information should be shared with police immediately where there is an imminent risk of serious harm to the public and/or a crime may be prevented. In other circumstances information should be shared as soon as practically possible or within 5 working days. The reasons for information sharing should be clearly documented on the case file.

Probation staff should request information using a standard request proforma (example attached at Appendix C). It is anticipated that single points of contact (SPOCs) will be identified to facilitate information sharing. Police will assess what information, other than arrest history and sanitised as necessary, should be shared. It is anticipated that information will be shared electronically wherever possible and appropriate. Probation staff will adhere to the NIM 5x5x5 grading and disclosure advice on the response form.

It is recognised that information is exchanged between Police and Probation on a daily basis. It is essential to have an audit trail for such exchanges but processes should not inhibit information sharing or compromise public safety.

In the context of ordinary case work it will be appropriate for probation offender managers and Police staff to exchange information on the telephone or by secure email. Information classified as 'Restricted' can be exchanged between Probation 'GSI' to Police 'PNN' email addresses. Any offender information discussed by phone should be recorded in case records to an access level appropriate to the sensitivity of the information as advised by Police.

Police will endeavour to respond to the request within the appropriate timescale identified on the request form. The following timescales are provided for guidance:

Reason	Timescale
Information is required for a court date	5 working days
There is a high or very high risk of serious harm	5 working days (see note re: imminent risk of serious harm)
There is a medium risk of serious harm	10 working days
There is a low risk of serious harm	15 working days

N.B. The above must not prevent *immediate* working together where the risk of serious harm is *imminent*.

Access to records

Authorised Probation staff, predominantly probation offender managers and members of the Offender Management Team working with the offender, will have access to disclosed material.

The default minimum Protective Marking category for all NOMS offender personal information is 'Restricted'. This applies to information in any format, whether physical hard copy, digital or electronic.

The probation electronic network is authorised to exchange information classified as 'Unclassified', 'Protect' or 'Restricted' with other authorised e-mail addresses (such as all e-mail addresses on the GSI network).

No 'Confidential' information can be exchanged across the probation electronic network. There are special security arrangements for ViSOR. Local Agency ViSOR Central Points of Contact (CPC) should be consulted regarding these arrangements.

Any 'Confidential' information must be stored in a clearly-designated section of the offender file. Information that cannot be disclosed to the offender must be clearly marked as such and stored in a separate sub-section within the 'Confidential' file.

Purposes for which information can be used

- To inform risk assessment and risk management
- To protect the public from serious harm
- For the protection of children and vulnerable adults
- For the protection of specific and potential victims
- To inform decisions on whether other procedures for managing offenders (e.g. MAPPA) should be invoked

Process for maintaining and updating information

Probation National Standards for the management of offenders requires probation staff to update records contemporaneously. Regular information exchange on cases identified according to criteria specified above will ensure that case records remain up to date and accurate.

Under the ISA *routine* information exchange will cease at the termination of the order or licence. However, situations will arise, when the offender is not subject to any statutory supervision, which require information sharing for specific purposes e.g. during the investigation of a crime. It is important to recognise that information exchange will, at times, mirror the cycle of offending behaviour and probation offender managers should be confident that sharing of information, after statutory supervision by NOMS has finished, can be appropriate.

Security arrangements

NOMS and police must ensure that a baseline level of security is in place to ensure compliance with Principle 7 of the Data Protection Act. The security standard must be

compatible with ISO 27001, although non police agencies do not have to be accredited to this standard.

NOMS holds GSI accredited status. Once Police information is received, it will be handled by Probation staff in accordance with the security operating procedures published for the service.

The majority of information disclosed by the police will be categorised as 'Restricted' under the Government Protective Marking Scheme (GPMS). On the rare occasions when information classified as 'Confidential' is to be disclosed additional security must be applied. The local security arrangements must comply with the GPMS Handling Rules detailed in Appendix D.

Some national systems, e.g. ViSOR and the Police National Database (PND) are designated as 'Confidential' systems under GPMS. Therefore data obtained through accessing the ViSOR system must be treated as 'Confidential'. This places specific obligations on users of the system and their organisations (see ViSOR Standards v1.0: 2008 – Section 2.1.2). However, certain reports may be recorded at 'Restricted' level, which will be reflected on the report. Such reports should be treated in accordance with their level of protective marking.

Section 5 Information passed on to other parties

Freedom of Information Requests

Normal practice will be to make all information disclosure agreements available on the Publication Schemes of the respective signatory agencies. It is also recognised that either party to this ISA may receive a request for information made under the Act that relates to the operation of this ISA. While there is no requirement to consult with third parties under Freedom Of Information Act 2000 (FOIA), the parties to this agreement must consult and will take account of views of the third party from whom the information originated and this will inform any exemptions to FOIA that may be relied on. FOIA also includes a process by which one authority may also transfer all or part of a request to another authority if it relates to information that is not held by the authority to whom the request is made.

Subject Access Rights

All requests for information under the subject access provisions of the Data Protection Act 1998 will be dealt with by the person responsible for Data Protection within the organisation. If personal data is identified as belonging to another agency, it will be the responsibility of the receiving agency to contact the Data Protection Officer for the originating agency to determine whether the latter wishes to claim an exemption under the provisions of the Data Protection Act, so that this can be taken into consideration.

Secondary use

Information exchanged under this agreement is only to be used for the purposes of this ISA and will not be used for any other purpose without the express agreement of the originating agency.

Information obtained by probation can be used to meet their statutory functions, which may include sharing with other parties such as prison establishments where appropriate for maintaining good order and discipline.

Unauthorised disclosure of information to persons or agencies outside the terms of this agreement (e.g. the forwarding of e-mails containing information marked 'Restricted' to third parties) will be deemed to constitute a breach of the agreement, unless a clear, legal justification and evidence can be provided to support the disclosure.

Section 6 Agency Liability

Each of the parties to this agreement will be solely responsible for any and all costs, expenses, claims and liabilities arising out of any breach of this agreement and in particular, but without limitation, the unauthorised or unlawful access, loss, theft, use, destruction or disclosure of data obtained in connection with this agreement by its sub-contractors, employees, agents or any other person within its control.

Section 7 Review and Retention

The Data Controller for each probation trust is required to establish procedures for compliance with the Data Protection Act 1998. Information provided by police and retained within probation records will be kept for the periods specified in each probation trust's compliance policy.

The Data Controller in each police force will keep information provided by probation under this agreement in accordance with the retention periods identified in the Management of Police Information (MoPI) Guidance and within force policy.

Section 8 Breach of Confidentiality

In the case of a breach of confidentiality involving any information covered by this agreement the following personnel MUST be informed in writing immediately.

If it appears there has been a breach of the Data Protection Act 1998 (including the potential commission of a criminal offence under the Data Protection Act 1998) the local Police and Probation Data Protection Officers must be notified in writing within 24 hours of such breach being identified.

In the case of any suspected breaches of the Data Protection Act 1998 that involve personal data processed by the PNC or in any other case which comes to the attention of the Chief Constable or one of his/her officers the Police will be responsible for any subsequent investigation.

Any complaint made will be brought to the attention of the nominated officer of the relevant partner(s), and they will be dealt with in accordance with their own policies and procedures. Partners will keep each other informed of developments following a complaint received, where relevant.

In the case of that suspected breach of Data Protection incurred by the abuse of data processed by Probation, the Probation Trust will be the initial investigatory body.

The above does not preclude any disciplinary action any employer may decide to take in any disciplinary procedures against any of its staff.

The Information Commissioner's Office must be informed as and when necessary.

Section 9 Dispute resolution

In day to day local operations, if circumstances arise in which one agency has concerns in relation to the operation of this agreement every effort should be made to resolve this so that information exchange is not disrupted. The following process should guide dispute resolution:

If a dispute arises out of or in connection with this agreement or the performance, validity or enforceability of it (Dispute) then, except as expressly provided in this agreement, the parties shall follow the dispute resolution procedure set out in this clause:

- a. either party shall give to other written notice of the Dispute, setting out its nature and full particulars (Dispute Notice), together with relevant supporting documentation. On service of the Dispute Notice the [title and address of relevant police postholder for Police] and the [title and address of relevant postholder for Probation] shall attempt in good faith to resolve the Dispute;
- b. if the [Police postholder] and the [Probation postholder] are for any reason unable to resolve the Dispute within 14 days of service of the Dispute Notice, the Dispute shall be referred to the [Police postholder]'s Line Manager and the [Probation postholder]'s Line Manager who shall attempt in good faith to resolve it; and
- c. if the [Police postholder]'s Line Manager and the [Probation postholder]'s Line Manager are for any reason unable to resolve the Dispute within 28 days of it being referred to them, the Dispute shall be referred to the [relevant Chief Executive of the Probation Trust] on behalf of NOMS and to the [relevant Chief Constable of Police].

Locally, either agency may suspend this Information Sharing Agreement for up to 30 calendar days, if they feel that security has been seriously breached. This should only be considered as a last resort and on the undertaking that the 30 day period will be used to resolve the issue.

Section 10 Signatures

We the undersigned agree that the agency/organisation we represent will adopt and adhere to this information sharing agreement.

AGENCY	NAME	POST HELD	SIGNATURE	DATE
NOMS	Michael Spurr	Chief Operating Officer NOMS		
NOMS	Ann Beasley	Director of Finance and Performance		
Police Service	Keith Bristow	Chief Constable ACPO Lead for Crime Business Area		



Appendix A

WORKBOOK FOR THE CREATION OF ACPO GUIDANCE/PRACTICE ADVICE

No new work to develop Guidance etc. can be commenced unless a Workbook, with the first page completed and accompanied by a completed Appendix 'A' is first submitted, through the Head of the Business Area, to the ACPO Programme Support Office for approval. This workbook, with all sections completed, must be included in the final document as an Appendix and submitted, through the Head of the Business Area, to the Programme Support Office for quality assurance prior to submission to Cabinet for approval as ACPO Doctrine.

Title of Draft Guidance/Practice Advice Document

Information Sharing Agreement, Association of Chief Police Officers (ACPO) and the National Offender Management Service (NOMS)

ACPO Reference Number

Unique reference number:

ACPO Commissioning

Name of ACPO Business Area:	Crime
Head of Business Area commissioning the work:	CC Keith Bristow
Date Authorised:	16/03/10
Projected date of completion:	30/06/10

PERSON COMPLETING WORK BOOK

Name:	Force Address:
T/DI Emma Wright (Staff Officer)	West Mercia Police
Email address:	Contact Tel. No:
emma.wright@westmercia.pnn.police.uk	01905 331491

Date the first page of this Workbook was completed and forwarded to the Programme Support Office:

16/03/10

For ACPO use only

Date QA check completed:	
Date referred to HBA:	
Date Guidelines/Practice Advice signed off by HBA:	

SECTION A - FOR USE ONLY WHERE AN EXISTING GUIDANCE OR PRACTICE ADVICE DOCUMENT IS BEING AMENDED AS THE RESULT OF A REVIEW

A.1 Title of original document:

N/A

A.2 Date of publication of original document:

N/A

SECTION B – IMPACT UPON OTHER ACPO BUSINESS AREAS

B.1 Give details of the impact on/dependencies with other ACPO Business Areas and existing Guidance/Advice

N/A

If B.1 applies, please inform the relevant ACPO Policy Officer who will consult across other business areas

SECTION C - ACPO EQUALITY IMPACT ASSESSMENT TEMPLATE (DIVERSITY AUDIT) AS AGREED WITH THE CRE

C1. Identify all aims of the guidance/advice

C.1.1 Identify the aims and projected outcomes of the guidance/advice:

- Define the specific purposes for which the signatory agencies have agreed to disclose information.
- Describe the roles and structures that will support the disclosure of information between agencies.
- Set out the legal gateway through which the information is disclosed.
- Describe the security arrangements necessary.
- Describe how this agreement will be monitored and reviewed.
- Compliance with MOPI.
- Support the introduction of public protection networks in accordance with Sir Ian Magee's Review of Criminality Information.

C.1.2 Which individuals and organisations are likely to have an interest in or likely to be affected by the proposal?

The Police Service, National Offender Management Service and individuals who are subject of information sharing in accordance with this Agreement.

C2. Consider the evidence

C.2.1 What relevant quantitative data has been considered?

Age	N/A
Disability	N/A
Gender	N/A
Race	N/A
Religion / Belief	N/A
Sexual Orientation	N/A

C.2.2 What relevant qualitative information has been considered?

Age	N/A
-----	-----

Disability	N/A
Gender	N/A
Race	N/A
Religion / Belief	N/A
Sexual Orientation	N/A
C.2.3 What gaps in data/information were identified?	
Age	N/A – no relevant data was identified for consideration.
Disability	N/A – no relevant data was identified for consideration.
Gender	N/A – no relevant data was identified for consideration.
Race	N/A – no relevant data was identified for consideration.
Religion / Belief	N/A – no relevant data was identified for consideration.
Sexual Orientation	N/A – no relevant data was identified for consideration.
C.2.4 What consideration has been given to commissioning research?	
Age	N/A – the commissioning of research is not considered necessary.
Disability	N/A – the commissioning of research is not considered necessary.
Gender	N/A – the commissioning of research is not considered necessary.
Race	N/A – the commissioning of research is not considered necessary.
Religion / Belief	N/A – the commissioning of research is not considered necessary.
Sexual Orientation	N/A – the commissioning of research is not considered necessary.

C3. Assess likely impact

C.3.1 From the analysis of data and information has any potential for differential/adverse impact been identified?	
Age	None – except that certain groups who are statistically more likely to commit the offences covered by the agreement may be subject of more requests to share information under the agreement.
Disability	As above.
Gender	As above.
Race	As above.
Religion / Belief	As above.
Sexual Orientation	As above.
C.3.2 If yes explain any intentional impact:	
Age	No intentional impact.
Disability	No intentional impact.
Gender	No intentional impact.
Race	No intentional impact.
Religion / Belief	No intentional impact.
Sexual Orientation	No intentional impact.
C.3.3 If yes explain what impact was discovered which you feel is justifiable in order to achieve the overall proposal aims. Please provide examples:	
Age	If certain groups (as described above at C.3.1.) are more likely to be the subject of information sharing requests this is justifiable as all information sharing will be legal, proportionate and necessary to protect the public.
Disability	As above.
Gender	As above.
Race	As above.
Religion / Belief	As above.

Sexual Orientation	As above.
C.3.4 Are there any other factors that might help to explain differential /adverse impact?	
Age	None.
Disability	None.
Gender	None.
Race	None.
Religion / Belief	None.
Sexual Orientation	None.

C4. Consider alternatives

C.4.1 Summarise what changes have been made to the proposal to remove or reduce the potential for differential/adverse impact:
None.
C.4.2 Summarise changes to the proposal to remove or reduce the potential for differential/adverse impact that were considered but not implemented and explain why this was the case:
None.
C.4.3 If potential for differential/adverse impact remains explain why implementation is justifiable in order to meet the wider proposal aims:
If certain groups (as described above at C.3.1.) are more likely to be the subject of information sharing requests this is justifiable as all information sharing will be legal, proportionate and necessary to protect the public.

C5. Consult formally

C.5.1 Has the proposal been subject to consultation? If no, please state why not. If yes, state which individuals and organisations were consulted and what form the consultation took:	
Age	Consultation has taken place across the ACPO Violence and Public Protection Portfolio. No specific consultation with individuals/groups in relation to these factors was considered necessary.
Disability	As above.
Gender	As above.
Race	As above.
Religion / Belief	As above.
Sexual Orientation	As above.
C.5.2 What was the outcome of the consultation?	
Age	No identified outcome.
Disability	No identified outcome.
Gender	No identified outcome.
Race	No identified outcome.
Religion / Belief	No identified outcome.
Sexual Orientation	No identified outcome.
C.5.3 Has the proposal been reviewed and/or amended in light of the outcomes of consultation?	
N/A.	
C.5.4 Have the results of the consultation been fed back to the consultees?	
N/A.	

C6. Decide whether to adopt the proposal

C.6.1 Provide a statement outlining the findings of the impact assessment process. If the proposal has been identified as having a possibility to adversely impact upon diverse communities, the statement should include justification for the implementation:
It has been identified that there may be a potential that that certain groups who are statistically more likely to commit the offences covered by the agreement may be subject of more requests to share information under the agreement. If certain groups are more likely to be the subject of information sharing requests (as above) then this is justifiable as all information sharing will be legal, proportionate and necessary to protect the public.

C7. Make Monitoring Arrangements

C.7.1 What consideration has been given to piloting the proposal?
The Agreement seeks to formalise existing information sharing arrangements therefore a pilot is not considered necessary.
C.7.2 What monitoring will be implemented at a national level by the proposal owning agency and/or other national agency?
Compliance with the Agreement will be reviewed via a yearly audit.
C.7.3 Is this proposal intended to be implemented by local agencies that have a statutory duty to impact assess policies? If so, what monitoring requirements are you placing on that agency?
None.

C8. Publish Assessment Results

C.8.1 What form will the publication of the impact assessment take?
As recommended (<i>It is recommended that for publication on the ACPO website, the impact assessment be attached to the completed document as the first appendix. On the ACPO Intranet, the whole workbook will be attached to assist in the preparation of local audits</i>).

SECTION D - HUMAN RIGHTS REVIEW

D1. Does the proposal have significant human rights implications, either for the public or for the Police Service? Answer YES or NO:

YES

If NO, go straight to Section E

If YES, answer the following questions and consider seeking legal advice

D.1.1. Who will be affected by this proposal?

- Consider not only the direct subject of the proposal, but also other people who may be affected (e.g. bystanders, victims, general public, police staff, subject's family)

Individuals who are subject of information sharing via this agreement will be affected. Past/potential victims and the general public will be affected in that they will be protected from potential harm by information sharing taking place.

D.1.2 Which of their rights are being protected?

- E.g. the right to life; right to security; freedom of belief, expression or assembly; right to family life; right to privacy; right to property

Victims/general public – right to life

D.1.3 For each person or group of people, which of their Convention rights may the proposal potentially interfere with and how?

- E.g. right to life; prohibition of degrading treatment; right to liberty; right to fair trial; right to due process; right to privacy; freedom of belief, expression, assembly and association

Individual who are subject of information sharing – right to privacy will be affected by the sharing of personal information. The right to a fair trial could be affected by the sharing of information at the pre-conviction stage, however, this agreement makes it clear that the information shared should not be for the purpose of making an offender's sentence more onerous but to ensure the most appropriate sentence is passed.

Answer the following questions in respect of each interference with a right.

D.1.4 Is the interference legal? Explain in full:

- e.g. European legislation, Act of Parliament, statutory instrument, statutory codes, common law

Yes, information will only be shared in a manner that is legal (in accordance with common law, the Data Protection Act and the Human Rights Act).

D.1.5. Is the interference necessary? Explain in full:

- It may for example be justified if it protects others' rights, e.g. right to life; right to security; freedom of belief, expression or assembly; right to family life; right to privacy; right to property
- What "legitimate aims" under the Convention are being pursued in interfering with the right?

The interference is necessary to protect the rights of victims/the general public (right to life, freedom from torture, degrading or inhumane treatment). It is also necessary to ensure the Police Service fulfils it's duty to protect the public.

D.1.6 Is the interference proportionate? Explain in full:

- What practical alternative actions are available? Will any of these not interfere or interfere less with a right? If they will, why are they not being used?
- Is the interference the least intrusive means available?

The interference is proportionate. There are no practical alternative options to achieve the aims of this Agreement (that are less intrusive) and the intrusion as a result of this Agreement is the least intrusive means possible.

D.1.7 Having considered the above points, do you consider that the proposal -

(a) Breaches a Convention right? YES or NO:

NO

(b) Is vulnerable to challenge? YES or NO

NO

Note: interference with a right does not equal a breach – if an interference is justified, there is no breach.

If the answer to (a) or (b) above is YES and you consider that there is a breach of a Convention right or that the proposal is vulnerable to challenge, seek legal advice.

SECTION E - DATA PROTECTION REVIEW

E.1 Does this proposal relate in any way to the processing of personal data? Answer YES or NO. If NO, go straight to Section F.

If YES, outline how it complies with the Data Protection Act, listing the principles summarised below. The ACPO Data Protection and FOI Portfolio Group will provide assistance in identifying and addressing compliance:

YES

The Principles:

- a) *Personal data shall be processed fairly and lawfully ...*
- b) *Personal data shall be obtained only for one or more lawful purposes ...*
- c) *Personal data shall be adequate, relevant and not excessive in relation to the purpose for which it is processed*
- d) *Personal data shall be accurate and, where necessary, kept up to date*
- e) *Personal data processed for any purpose shall not be kept longer than is necessary for that purpose*
- f) *Personal data shall be processed in accordance with the rights of data subjects under the Act*
- g) *Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data ...*
- h) *Personal data shall not be transferred to any country outside the European Economic Area (EEA) unless the country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to processing of personal data*

The above principles are outlined in the Agreement and information shall only be shared in a manner that is compliant with these principles. The ACPO Data Protection and FOI Portfolio have been engaged in the production of this Agreement to address compliance.

SECTION F - HEALTH & SAFETY REVIEW

F.1 Does this proposal have significant health and safety implications for the public or for police staff? Answer YES or NO.

NO.

If YES, answer questions F.2. & F.3. If NO, go straight to Section G1.

F.2 Explain how the risks to health and safety have been assessed and what control measures have been put in place:

N/A.

F.3 What are the health and safety duties and who is responsible for them? Explain in full:

N/A.

SECTION G - BUREAUCRACY REVIEW

G.1 List the forms or databases that police staff will be required to complete as part of this proposal:

No forms. Use of existing police databases holding the information requested shall be required (e.g. local intelligence systems, PNC, INI (thereafter PND), ViSOR).

G.2 Give details of how you have reviewed the need for, content of and appropriateness of the forms or databases. Have you reduced their quantity or content?

Factors to consider:

- *Whether the benefit of gathering the information exceeds the effort*
- *The cumulative impact – especially when there is repeated entry of the same information*
- *Retention period – is the information disposed of at the optimum time?*

The benefit of gathering the information (i.e. ensuring agencies can properly assess risk to effectively manage offenders and protect the public) exceeds the effort. The Agreement should not have a cumulative impact as any information already shared by established processes (under MAPPA, PPO or MARAC arrangements) will continue to be shared via these means. Any sharing outside of these arrangements will already be occurring and this Agreement seeks to merely formalise those processes. Retention periods are covered within the Agreement to ensure information is disposed of at the optimum time.

SECTION H - FREEDOM OF INFORMATION REVIEW

H.1 Is this reviewed proposal exempt from publication under the FOIA? Answer YES or NO:

NO

IF NO, go straight to Section I. If YES, give full details of the exemptions that apply and the reasons for them at H.2.1 – 2.3 below:

H.2 Reasons for Non- or Partial Disclosure under Freedom of Information Act 2000**H.2.1 Is this document completely non-disclosable? Answer YES or NO**

--

H.2.2 If yes, why? Which exemptions apply?

Section	Description and Type of Exemption	Evidence / Rationale for Application

H.2.3 Is this document partially disclosable? Answer YES or NO

--

H.2.4 If yes, which parts of the document are not disclosable and why? Which exemptions apply?

Part of the Document	Section	Description and Type of Exemption	Evidence / Rationale for Application

SECTION I – IMPLEMENTATION AND EVALUATION

I.1 Now that the audit is complete the Guidance/Advice document should be prepared for consideration by the Head of Business Area - either for approval and sign-off or, in some cases, referral to ACPO Cabinet or Council. Please follow the attached ACPO Practice Guidance/Advice Template.

I.2 Please ensure that a full consultation on the content of the final draft document is conducted with stakeholders, both internal and external and ensure that their views are fully considered. Please detail below the organisations/individuals consulted:

- | |
|--|
| <ul style="list-style-type: none"> - <i>Expert consultation via ACPO Management of Sexual Offenders and Violent Offenders Workstream.</i> - <i>Wider consultation via ACPO Violence and Public Protection Portfolio.</i> - <i>External consultation via NOMS lead on the Agreement.</i> |
|--|

1.3 Full consideration should be given to the following:

- Financial implications/benefits
- Resource implications/benefits
- Potential performance/service improvements
- Risks
- Learning requirement

Monitoring and Review**1.4 Detail below the on-going effects of this proposal:**

The ongoing effects of the Agreement are to formalise information sharing that is already occurring about offenders who are considered to pose a risk of harm, therefore impact is expected to be minimal. Financial implications of developing and implementing the Agreement have been consumed via the day to day roles of those staff (ACPO and NOMS) concerned. No additional resources should be required for the Police Service to implement and comply with the Agreement.

1.5 How will it be monitored?

Compliance with the Agreement will be monitored by a yearly audit (suggested a minimum of 25 cases). The Agreement itself will be reviewed 6 months after implementation and thereafter annually.

1.6 By whom?

By ACPO and NOMS staff.

1.7 At what intervals?

As above.

1.8 When is the next review of this proposal planned?

Note. Diversity Reviews are required at least every 3 years under the RRAA but this review is in relation to the ongoing relevance of the document. If you consider that an earlier review is needed, please give the reasons and explain what process is in place to prompt those in post at that time to conduct the review:

The Agreement will be reviewed as outlined above by the ACPO Staff Officer for the Management of Sexual Offenders and Violent Offenders and the NOMS lead for this Agreement. Reminders in calendars will be set by respective staff to ensure review.

This Workbook must be attached to the completed Guidance/Advice document as Appendix, 'A' (or 'B' if existing guidance etc. is being amended) which must then be submitted, through the relevant ACPO head of business area, to the ACPO Programme Support Office by email, where it will undergo quality review prior to submission to the head of the business area for approval. Only then will it be put before the ACPO Cabinet for final approval.

Appendix B Legal Basis and Considerations

The Offender Management Act 2007

The Offender Management Act 2007 provides the legal basis for probation trusts, which have now replaced all local probation boards. Relevant sections of the Offender Management Act 2007 for the purposes of this agreement include:

- Section 1(1) In this Part “the probation purposes” means the purposes of providing for—
- (a) courts to be given assistance in determining the appropriate sentences to pass, and making other decisions, in respect of persons charged with or convicted of offences;
 - (b) authorised persons to be given assistance in determining whether conditional cautions should be given and which conditions to attach to conditional cautions;
 - (c) the supervision and rehabilitation of persons charged with or convicted of offences;
 - (d) the giving of assistance to persons remanded on bail;
 - (e) the supervision and rehabilitation of persons to whom conditional cautions are given;
 - (f) the giving of information to victims of persons charged with or convicted of offences.
- (2) The purpose set out in subsection (1)(c) includes (in particular)—
- (a) giving effect to community orders and suspended sentence orders (or, in the case of persons mentioned in subsection (3), any corresponding sentence which is to be carried out in England and Wales);
 - (b) assisting in the rehabilitation of offenders who are being held in prison;
 - (c) supervising persons released from prison on licence;
 - (d) providing accommodation in approved premises.
- (3) That purpose also applies in relation to persons who—
- (a) are convicted of an offence under the law of a country outside England and Wales, and
 - (b) receive a sentence which is to any extent to be served or carried out in England and Wales, as it applies in relation to persons convicted of offences.

Section 2(1) It is the function of the Secretary of State to ensure that sufficient provision is made throughout England and Wales—

- (a) for the probation purposes;
 - (b) for enabling functions conferred by any enactment (whenever passed or made) on providers of probation services, or on officers of a provider of probation services, to be performed; and
 - (c) for the performance of any function of the Secretary of State under any enactment (whenever passed or made) which is expressed to be a function to which this paragraph applies; and any provision which the Secretary of State considers should be made for a purpose mentioned above is referred to in this Part as “probation provision”.
- (2) The Secretary of State shall discharge his function under subsection (1) in relation to any probation provision by making and carrying out arrangements under section 3.

- (3) The Secretary of State must have regard to the aims mentioned in subsection (4) in the exercise of his functions under subsections (1) and (2) (so far as they may be exercised for any of the probation purposes).
- (4) Those aims are—
- (a) the protection of the public;
 - (b) the reduction of re-offending;
 - (c) the proper punishment of offenders;
 - (d) ensuring offenders' awareness of the effects of crime on the victims of crimes and the public; and
 - (e) the rehabilitation of offenders.

Section 14 (1) This section applies to—

- (a) the Secretary of State;
- (b) a provider of probation services (other than the Secretary of State);
- (c) an officer of a provider of probation services; and
- (d) a person carrying out activities in pursuance of arrangements made by a provider of probation services as mentioned in section 3(3)(c).

(2) In this section “listed person” means—

- (a) a government department;
- (b) a relevant local authority;
- (c) the Youth Justice Board for England and Wales;
- (d) the Parole Board for England and Wales;
- (e) a relevant contractor;
- (f) a chief officer of police;
- (g) a person who is responsible for securing the electronic monitoring of an individual; and
- (h) any other person specified or described in regulations made by the Secretary of State.

(3) Information may be disclosed—

- (a) by a person to whom this section applies—
 - (i) to another person to whom this section applies, or
 - (ii) to a listed person, or
- (b) by a listed person to a person to whom this section applies, but only if the disclosure is necessary or expedient for any of the purposes mentioned in subsection (4).

(4) Those purposes are—

- (a) the probation purposes;
- (b) the performance of functions relating to prisons or prisoners of—
 - (i) the Secretary of State;
 - (ii) any other person to whom this section applies; or
 - (iii) any listed person; and
- (c) any other purposes connected with the management of offenders (including the development or assessment of policies relating to matters connected with the management of offenders).

The Police Act 1996

The police's power to request information comes in the main from the Police Act 1996 and other pieces of legislation which enable police officers or police staff to carry out their duties e.g. Police and Criminal Evidence Act 1984 (PACE) and the Criminal Procedures Investigations Act 1996 (CPIA). The Police Act 1996, Section 30(1), gives constables all the powers and privileges of a constable throughout England and Wales. Section 30(5) defines powers as powers under any enactment whenever passed or made. These powers include the investigation and detection of crime, apprehension and prosecution of offenders, protection of life and property, and maintenance of law and order. Under the Police Reform Act 2002, the Chief Officer can delegate certain powers to police staff.

Common Law

The common law is law developed by custom and general agreement which is not enshrined in statute but nevertheless gives the police a duty to investigate crimes.

The police have a general common law power to disclose information for policing purposes, usually for one or more of the following purposes:

- prevention and detection of crime;
- apprehension and prosecution of offenders;
- protection of life and property and assisting the public.

This allows the disclosure of identifiable information on a case-by-case basis for these purposes subject to appropriate safeguards.

The Crime and Disorder Act 1998

The Police and Justice Act 2006 amended the Crime and Disorder Act 1998 to include s.17A, which provides a statutory duty to disclose non-personal data to other Section 115 relevant authorities and goes on to specifically exclude any personal data from the duty to disclose. The Crime and Disorder Act (Prescribed Information) Regulations 2007 (SI 1831 of 2007) was made pursuant to s.17A of the Crime and Disorder Act 1998.

The Data Protection Act 1998

The Data Protection 1998 governs the processing of personal data including the collection, use of and disclosure of such information. The legislation requires that data controllers meet certain obligations. It also gives individuals or 'data subjects' certain rights with regard to their own personal data, including that of 'subject access' to the information we are processing on them.

The main standard for processing personal data is compliance with the eight data protection principles – see Appendix B.

The most significant principle is the first principle which states that personal data shall be processed fairly and lawfully and shall not be processed unless at least one Schedule 2 condition and in the case of 'sensitive personal data', at least one Schedule 3 condition is also met (see Appendix B).

The type of information being disclosed for the purposes of this exchange agreement will almost always be 'sensitive personal data' which means that at least one of both Schedule 2 *and* Schedule 3 conditions must be satisfied.

Even in the event that the *prevention and detection of crime* exemption (Section 29 Data Protection Act) is being relied upon, Schedules 2 and 3 conditions must still be satisfied.

Critically, any decision to share information must satisfy *both* the principal authority for disclosure e.g. public interest, Offender Management Act 2007 and also the Schedule 2 and Schedule 3 conditions of Data Protection Act 1998.

The Principles also cover issues such as accuracy of the data, security, and the length of time the information should be retained.

Each party to this agreement should have in place its own data controller, mechanisms for ensuring compliance with the Data Protection Act 1998.

For probation staff, the scope and limits of any right to confidentiality arrangement which the offender can expect between him or herself and the OM should be clarified as part of induction procedures.

Further Legal Considerations

Appendix B contains further considerations which have informed the development of this ISA.

This appendix contains details of supporting legal considerations that inform the disclosure process.

DUTY OF CONFIDENCE

The duty of confidence falls within common law as opposed to statutory law and derives from cases considered by the courts. There are generally three categories of exception to the duty of confidence:

- Where there is a legal compulsion to disclose
- Where there is an overriding duty to protect the public
- Where the individual to whom the information relates consented.

Whilst in some circumstances consent may be given by the offender it is clear that the first and second of these conditions are the more relevant ones for the purposes of this exchange agreement. The legitimate basis for this information exchange is documented above and an overriding public interest relating to the protection of the public will almost certainly exist and such information will usually be disclosed unless such disclosure may cause substantial prejudice to a criminal investigation or prosecution or otherwise cause significant harm. A record of the decision and the rationale for it will be made as part of the disclosure.

Public Interest

Disclosure can be made if there is an over-riding public interest or justification for the disclosure. The following considerations have been made:

- The disclosure is necessary for the prevention or detection of crime, prevention of disorder, to protect public safety or to protect the rights and freedoms of others
- The disclosure may be necessary for the protection of young or other vulnerable people
- The risk to others or their vulnerability will depend upon the activity engaged in by this individual
- The impact of the disclosure on the offender would depend upon the seriousness of the offence and could lead to court proceedings
- The disclosure should be proportionate to the purpose of the agreement
- There is no equally effective but less intrusive alternative means of achieving the purpose of the agreement.

The Human Rights Act 1998

The UK Human Rights Act 1998 gives further effect in domestic law to Articles of the European Convention on Human Rights (ECHR). The Act requires all domestic law be compatible with the Convention Articles and places a legal obligation on all public authorities to act in a manner compatible with the convention. Should a public authority fail to act in such a manner then legal action can be taken under Section 7 of the Act.

The Convention does allow limited interference with certain convention rights by public authorities under broadly defined circumstances or 'legitimate aims'. However, simple reliance on a legal power may not alone provide sufficient justification and the following principles have been considered:

- The legal basis for the action being taken is that conferred on the chief constable by the Police Act and the probation trust by the Offender Management Act 2007
- Information sharing is in pursuit of the legitimate aim of the prevention and detection of crime and the management of offenders
- The action being taken is proportionate and uses the least intrusive method of achieving that purpose.

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.'

As such, the sharing of information can be justified, to the extent that it is necessary and proportionate, on one of the following grounds:

- In the interests of national security
- Public safety
- Economic well being of the country
- The prevention of crime and disorder
- The protection of health or morals
- The protection of the rights or freedoms of others

Data Protection Principles

The Act enshrines eight principles, which all users of personal data must adhere to. Further guidance on how the principles apply in practice is available on both intranet and internet through searching under 'data protection act/principles'. The principles are:

1. Personal data shall be processed fairly and lawfully and in particular, shall not be processed unless:
 - (a) at least one of the conditions in Schedule 2 is met, and
 - (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met
2. Personal data shall be obtained only for one or more specified and lawful purpose, and shall not be further processed in any manner incompatible with that process or those purposes
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed

4. Personal data shall be accurate and, where necessary, kept up to date
5. Personal data processed for any purpose or purposes shall not be kept longer than is necessary for that purpose or those purposes
6. Personal data shall be processed in accordance with the rights of data subjects under this Act
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and 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 Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

SCHEDULE 2

CONDITIONS RELEVANT FOR PURPOSES OF THE FIRST PRINCIPLE: PROCESSING OF ANY PERSONAL DATA

- 1 The data subject has given his consent to the processing.
- 2 The processing is necessary—
 - (a) for the performance of a 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.
- 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.
- 4 The processing is necessary in order to protect the vital interests of the data subject.
- 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.
- 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.
 - (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.

SCHEDULE 3

CONDITIONS RELEVANT FOR PURPOSES OF THE FIRST PRINCIPLE: PROCESSING OF SENSITIVE PERSONAL DATA

- 1 The data subject has given his explicit consent to the processing of the personal data.
- 2 (1) The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment.
 - (2) The Secretary of State may by order—

- (a) exclude the application of sub-paragraph (1) in such cases as may be specified, or
 - (b) provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.
- 3 The processing is necessary—
- (a) in order 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.
- 4 The processing—
- (a) is carried out in the course of its legitimate activities by any body or association which—
 - (i) is not established or conducted for profit, and
 - (ii) exists for political, philosophical, religious or trade-union purposes,
 - (b) is carried out with appropriate safeguards for the rights and freedoms of data subjects,
 - (c) relates only to individuals who either are members of the body or association or have regular contact with it in connection with its purposes, and
 - (d) does not involve disclosure of the personal data to a third party without the consent of the data subject.
- 5 The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.
- 6 The processing—
- (a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),
 - (b) is necessary for the purpose of obtaining legal advice, or
 - (c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.
- 7 (1) The processing is necessary—
- (a) for the administration of justice,
 - (b) for the exercise of any functions conferred on any person by or under an enactment, or
 - (c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department.
- (2) The Secretary of State may by order—
- (a) exclude the application of sub-paragraph (1) in such cases as may be specified, or
 - (b) provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.
- 8 (1) The processing is necessary for medical purposes and is undertaken by—
- (a) a health professional, or

- (b) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.
 - (2) In this paragraph “medical purposes” includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.
- 9 (1) The processing—
- (a) is of sensitive personal data consisting of information as to racial or ethnic origin,
 - (b) is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained, and
 - (c) is carried out with appropriate safeguards for the rights and freedoms of data subjects.
- (2) The Secretary of State may by order specify circumstances in which processing falling within sub-paragraph (1)(a) and (b) is, or is not, to be taken for the purposes of sub-paragraph (1)(c) to be carried out with appropriate safeguards for the rights and freedoms of data subjects.
- 10 The personal data are processed in circumstances specified in an order made by the Secretary of State for the purposes of this paragraph.

APPENDIX C - (Proforma will be 'Restricted' when completed)**NATIONAL OFFENDER MANAGEMENT SERVICE (NOMS)
REQUEST FOR POLICE INFORMATION**

This request for information is made under the Information Sharing Agreement between NOMS and ACPO. The information provided by the local constabulary to the probation area or trust will assist in the preparation of Pre-Sentence Reports and the risk assessment and risk management of offenders with whom the probation service has statutory contact.

Section 1 Police Recipient Of Request

Name of SPOC	
Position	
Department	
Constabulary	
Contact Details	

Section 2 Subject Of Request (Offender)

Family Name	
First Names	
Date of Birth	
Aliases (if relevant)	
Previous Names	
PNC ID Number	

Section 3 Nature Of Probation Contact With Offender And Reason For Request

Case Stage	Yes	No
This request relates to the consideration of bail information		
I confirm that this request relates to a defendant whose charge or behaviour indicates that he/she presents a potential or actual risk of serious harm to the public and that the offender is charged with:		
a) violent and sexual offences (defined in Criminal Justice Act 2003 Chapter 15)		
b) other offences motivated by domestic abuse or targeting of specific groups or individuals		
c) any other offence, but where during interview with probation staff the offender has disclosed information which indicates a potential risk of serious harm to the public		
This request relates to the preparation of a Pre-Sentence Report		
I confirm that this request relates to an offender whose current conviction or behaviour indicates that he/she presents a potential or actual risk of serious harm to the public and that the offender has been convicted of:		
a) violent and sexual offences (defined in Criminal Justice Act 2003 Chapter 15)		
b) other offences motivated by domestic abuse or targeting of specific groups or individuals		
c) any other offence, but where during interview with probation staff the offender has disclosed information which indicates a potential risk of serious harm to the public		
This request relates to the ongoing risk assessment and risk management of the offender		
I confirm that this request will contribute to the ongoing assessment and management of the offender which is prioritised because:		
a) the offender has an arrest history which indicates that he/she has previously come to the attention of the police for a violent and/or sexual offence		
b) the offender has a previous conviction for a violent and/or sexual offence but is not currently under supervision for that offence		
c) the offender has disclosed during the course of supervision information which indicates that he/she has the potential to present a risk of serious harm to the public		
d) information which has come to the attention of probation staff which indicates that the offender may present a risk of serious harm to the public		
e) the offender has been considered for an Unpaid Work placement in a potentially sensitive setting		

Section 4 Information Requested

Type Of Information Sought	Check
Any evidence of a capacity to inflict serious harm e.g. history of threats, hate-based behaviour, domestic abuse, predatory behaviour or domestic extremism	
Concerns in relation to children or vulnerable adults	
Behaviour involving a breach of trust	
Evidence of established links or associations which might increase the risk of serious harm e.g. gang membership, contact with known sex offenders or other established criminal groups	
Evidence of substance abuse or mental health issues	
Any other information pertinent to the ongoing assessment and management of the offender (specify and justify)	
Other (specify and justify)	

Section 5 Details Of Probation Requester

Name	
Position	
Location/Address	
Probation Trust	
Phone	
Fax	
Email	
Signature	
Name of countersigning supervisor or manager	
Signature	

Section 6 Method Of Information Sharing

Please indicate how the information should be given/exchanged, taking account of the handling requirements for the potential security marking (GPMS). (Secure electronic exchange should be regarded as the default method of information exchange.)

Check/Method	Secure Email	Fax	In Person	Post
√				

Section 7 Confirmation Of Legal Basis

The NOMS/ACPO Information Sharing Agreement details the steps that must be taken to ensure that the proposed information sharing is lawful, necessary and proportionate. Further legal advice should be sought if there is any doubt as to whether the information can be shared in accordance with the NOMS/ACPO Information Sharing Agreement and all relevant laws, in particular, with the Data Protection Act 1998 and the Human Rights Act 1998.

APPENDIX D

GOVERNMENT PROTECTIVE MARKING SCHEME – HANDLING RULES

Probation Trusts receiving sensitive information from Police do so on the understanding that the protective measures described below are applied. If, for any reason, you are unable to comply with these requirements, you must contact the person that sent the information to you immediately.

Police information carries a protective marking on it. This indicates how sensitive its contents are, and determines the protective measures that need to be applied to it. The appropriate measures for each marking are shown below.

	RESTRICTED	CONFIDENTIAL	DESCRIPTOR (If used)
STORAGE OF PAPERS, IMAGES, CD's, FLOPPY DISKS OR OTHER ELECTRONIC MEDIA/DEVICE.	Protected by <u>one</u> barrier, e.g. a locked container (Restricted access) within a secure building. OR in a locked room (Restricted access) within a secure building.	Protected by <u>two</u> barriers e.g. a locked container in a locked room (both with restricted access) within a secure building.	Follow instructions provided by the originator.
DISPOSAL OF PAPERS	Shred in a strip or cross-cut shredder or return to Police. Keep secure if storing prior to disposal.	Shred in a cross-cut shredder or return to Police. Keep secure if storing prior to disposal.	Shred in a strip or cross-cut shredder or return to Police. Keep secure if storing prior to disposal.
DISPOSAL OF FLOPPY DISKS CD's & ANY OTHER ELECTRONIC STORAGE MEDIA/DEVICE.	Dismantle floppy disks by either cutting inner disks or shredding. CD's by cutting into at least quarters. Dispose with in un-classified waste	Dismantle floppy disks by either cutting inner disks or shredding. CD's by cutting into at least quarters. Dispose with in un-classified waste	Dismantle floppy disks by either cutting inner disks or shredding. CD's by cutting into at least quarters. Dispose with in un-classified waste
MOVEMENT WITHIN YOUR ORGANISATION	By trusted hand OR in a sealed envelope or container with the protective marking & descriptor shown. Include a copy of these instructions inside.	By trusted hand OR in a sealed envelope or container WITH THE PROTECTIVE MARKING & DESCRIPTOR SHOWN. Include a copy of these instructions inside.	
RETURN TO POLICE	By trusted hand in a sealed envelope or container OR by post or courier service in a sealed envelope with no protective marking or descriptor shown (other than PERSONAL or PRIVATE) & addressed to an individual by name or appointment.	By trusted hand in a sealed envelope or container, OR by post or courier service in a sealed envelope using double envelopes, both fully addressed but with the PROTECTIVE MARKING SHOWN ON THE INNER ENVELOPE ONLY. Provide a return address on the outer envelope. Always use either recorded delivery or a private courier service recorded delivery.	
E-MAIL	Only PNN and GSI email addresses allowed.	NOT PERMITTED.	
FAX	Check recipient is on hand to receive. Send cover sheet first and wait for confirmation before sending.	NOT PERMITTED	
TELEPHONE (Mobile or landline NOT WAP)	May be used	Only if operationally urgent. Use guarded speech and keep conversation brief.	

APPENDIX E POLICE NATIONAL INTELLIGENCE MODEL 5X5X5 GRADING

SOURCE EVALUATION

A - ALWAYS RELIABLE

There is no doubt of the authenticity, trustworthiness and competence of the source, or the information is supplied by an individual who, in the past, has proved to be reliable in all instances. Examples might include technical deployments and information known directly to law enforcement officers. Information in the past has always been 100% accurate.

B - MOSTLY RELIABLE

Sources where information in the past has, in the majority of instances, proved to be reliable. Examples might include contacts and informants whose information has proved correct the vast majority of times but not enough to be graded as 'A'

C - SOMETIMES RELIABLE

Sources where information in the past has in the majority of instances, proved unreliable. Information has in the past proved correct but the majority of times has been incorrect. Information should not be acted on without corroboration. It might also include the product of technical deployment where the quality of the recording is poor.

D - UNRELIABLE

Examples might include persons who have routinely proved unreliable in the past, or where there is some doubt about the authenticity, trustworthiness or competency, for example is known second or third hand.

E - UNTESTED SOURCE

This does not necessarily mean the information is unreliable but should nonetheless be treated with caution. Corroboration should be sought.

EVALUATION OF INTELLIGENCE

1 - KNOWN TO BE TRUE WITHOUT RESERVATION

Examples might include the product of technical deployments or events witnessed by a law enforcement officer. However, special care should be taken in assuming that everything heard through the use of technical equipment is 'A1'. Whilst it will be an accurate record of what the officer heard, the intelligence itself may still not be accurate, for example the source may be repeating hearsay or may be lying.

2 - THE INFORMATION IS KNOWN PERSONALLY TO THE SOURCE BUT IS NOT KNOWN PERSONALLY TO THE REPORTING OFFICER

3 - THE INFORMATION IS NOT KNOWN PERSONALLY TO THE SOURCE BUT IS CORROBORATED BY INFORMATION ALREADY RECORDED.

4 - THE INFORMATION IS NOT KNOWN PERSONALLY TO THE SOURCE AND CANNOT BE CORROBORATED IN ANY WAY.

5 - SUSPECTED TO BE FALSE

Action should be taken with extreme care and reliable corroboration sought. Whilst it may be desirable to record such intelligence onto the intelligence system it must be assessed for the potential risks arising from its inclusion.

HANDLING CODES

CODE 1

Permits dissemination to other law enforcement and prosecuting agencies within EEA and EU compatible (no special conditions), for example the Benefits agency.

CODE 2

Permits dissemination to UK non prosecuting parties, e.g. credit card companies and commercial organisations. Subject to authority levels and records being maintained. Special conditions for dissemination can be endorsed.

CODE 3

Permits dissemination to Non EEA law enforcement agencies, where no adequate safeguards for the rights of individuals exist, only on the grounds of substantial public interest and only after additional risk assessment. Special conditions for dissemination can be endorsed.

CODE 4

Permits dissemination but only within the originating organisation, i.e. the Avon & Somerset Constabulary.

CODE 5

Dissemination can only be made in compliance with the special conditions imposed. These conditions should be detailed. Any further dissemination of the content will only take place when the documented conditions have been met and/or the originating agency has been consulted.