Information Sharing Agreement

Under The Criminal Justice Act 2003 to facilitate the assessment and management of risks posed by relevant sexual and violent offenders in Humberside

Between

National Probation Service

Humberside Police

HM Prison Service

And

MAPPA Duty to Co-Operate Agencies

Serving our communities to make them safer and stronger

HM PRISON SERVICE
Public Sector Prisons

HM Prison & Probation Service

1 Background

1.1 MAPPA

Multi-Agency Public Protection Arrangements (MAPPA) are statutory arrangements for managing sexual and violent offenders. MAPPA is not a body, but a framework to enable participating agencies to better discharge their statutory responsibilities to protect the public in a co-ordinated manner. All agencies participating in MAPPA retain their full responsibilities and obligations at all times and nothing in this Agreement is intended to interfere with that.

1.2 Statutory Framework

Section 325 of the Criminal Justice Act 2003 (the Act) imposes a statutory duty on the MAPPA Responsible Authority (RA – comprising the Police, the National Probation Service (NPS) and HM Prison Service) to establish arrangements to assess and manage the risks posed by:

a) relevant sexual and violent offenders; and

b) other persons who, by reason of offences they have committed, are considered by the Responsible Authority to be persons who may cause serious harm to the public.

1.3 Duty to Co-Operate Agencies

Section 325(3) of the Act also imposes a duty on other specified agencies to co-operate with the RA within the MAPPA framework. Co-operation under Section 325(3) may include the exchange of information. These agencies are known as Duty to Co-Operate (DTC) agencies and consist of:

- Youth offending teams (YOT)
- Department for Work and Pensions (DWP)
- NHS England
- Education, social services and health functions of local authorities
- The local housing authority
- Private registered providers of social housing and registered social landlords providing or managing residential accommodation in which MAPPA offenders may reside
- The Health Authority
- The Clinical Commissioning Group (CCG) or Local Health Board
- The NHS Trust

- Providers of electronic monitoring services
- Home Office Immigration Enforcement (formally UKBA)

1.4 Information Sharing Agreement

While each agency should follow its own data protection policies in sharing information, co-operation between agencies is easier when there is a shared understanding of each other's policies, as there may be differences on points of detail. This Agreement sets out how agencies will share information with each other, so that they are following a common set of rules and security standards as far as possible. This Agreement covers systematic, routine data sharing where the same data sets are shared between MAPPA agencies for MAPPA established purposes; and one-off decisions to share data for any of a range of purposes within MAPPA. Each agency must resolve any actual or perceived conflict between its statutory duty to co-operate with MAPPA under the Act and its own policies and procedures. The RA may establish other arrangements with DTC Agencies, including good practice guidance, protocols and memoranda of understanding to help protect the public.

1.5 Data Protection Legislation

The main function of MAPPA is to prevent crime by co-ordinating the involvement of different agencies in assessing the risk presented by offenders and ensuring that any risks are managed effectively to protect the public. Participation in the MAPPA framework enables the RA and DTC agencies to reduce the risk of serious crime being committed by MAPPA eligible offenders. Data will therefore only be processed under this Agreement for the Law Enforcement Purposes identified in Section 31 of the Data Protection Act (DPA) 2018, namely the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. As such, data processing under this Agreement will comply with Part 3 DPA 2018 (Law Enforcement Processing) rather than General Processing under Part 2 DPA 2018 or the General Data Protection Regulation (GDPR). Data will not be processed under this Agreement for any purpose other than a Law Enforcement Purpose.

1.6 MAPPA Guidance

Under Section 325(8) of the Act, the Secretary of State has issued statutory national MAPPA Guidance (available at mappa.justice.gov.uk). The RA and the DTC agencies must have regard to this Guidance in exercising their functions under MAPPA. The MAPPA Guidance sets out clear principles to be followed when agencies participating in MAPPA share information about offenders. This Agreement has been formulated to facilitate the exchange of personal information between the specified agencies where it is lawful, necessary and proportionate.

2 Objectives of this Information Sharing Agreement

2.1 Principles of Information Sharing

Sharing information about offenders is essential to the multi-agency approach to their management. The quality of both risk assessment and risk management is reliant on the RA and DTC agencies (and others as appropriate) sharing accurate personal information in a timely manner.

The practice of information-sharing between MAPPA agencies is governed by legislation and certain principles, including those set out in the MAPPA Guidance and the Data Sharing Code of Practice issued in 2011 by the Information Commissioner's Office (ICO).

2.2 Information Sharing Practice

The MAPPA information sharing process works through the involvement and attendance of the appropriate agencies at MAPPA meetings; bilateral communication and meetings between practitioners outside of MAPPA meetings and the use of proper information sharing documentation, consistent with the MAPPA Guidance, which provides a consistent process for sharing information across England and Wales. These meetings and documents enable agencies to share information that:

- is relevant to undertaking a multi-agency risk assessment;
- identifies the likelihood of re-offending;
- identifies serious risk of harm issues and their imminence, and
- is critical to delivering an effective risk management plan.

3 Shared Information

3.1 General Principles

The purpose of sharing information about individuals (data subjects) is to enable the relevant agencies to work more effectively together in assessing risks and considering how to manage them. This points towards sharing all available relevant information, so that nothing is overlooked and public protection is not compromised. On the other hand, agencies must respect the rights of data subjects, which may limit what can be shared. These rights are set out in the DPA and the Human Rights Act 1998 (HRA). In summary, the principles derived from this legislation require that information sharing is lawful, necessary and proportionate.

3.2 Ownership of Shared Information

All information shared under MAPPA must be processed in line with the DPA 2018. Most personal information remains the responsibility of the agency that provided it and they are considered to be the data controller under DPA. For example, the NPS is the data controller for information regarding their statutory supervision of the offender and the police are the data controller for information regarding their management of a registered sexual offender. All agencies that retain copies of the minutes of MAPPA meetings or other information shared under MAPPA act as joint data controllers for those minutes or that information under DPA. Subject Access Requests (SAR) and Freedom of Information (FOI) requests concerning shared information must be responded to in line with the MAPPA Guidance (see Chapter 13b – MAPPA Meeting Minutes). Each MAPPA agency will have responsibility for complying with its legal obligations as data controllers under the DPA.

3.3 Information-sharing must be lawful

Information shared under this Agreement must be in accordance with the law. The statutory basis for sharing information between RA and DTC agencies under MAPPA is found in section 325(4) of the Criminal Justice Act 2003 (CJA). This expressly permits the sharing of information between these agencies for the purposes of assessing and managing the risks posed by offenders subject to MAPPA. Other lawful avenues for sharing information are found at 8.1 of this Agreement, but these are most likely to be used in sharing information with non-MAPPA individuals or organizations.

Information shared under this Agreement must also comply with the six Data Protection Principles set out in the DPA 2018. These principles are listed at 8.1-8.7 of this Agreement. Among other things they prohibit sensitive processing (i.e. the sharing of sensitive personal information) unless at least one of the conditions in Schedule 8 to the DPA 2018 is met. Information shared under MAPPA will usually meet the statutory etc. purposes and administration of justice conditions and may meet the safeguarding of children and of individuals at risk condition. The Data Protection Principles also dictate that the purpose of information sharing must be specified and the information shared must be accurate and up-

to-date, stored securely, and not be retained any longer than necessary (each agency should follow its own policy on this).

Information shared under this Agreement is for the purpose of preventing or investigating criminal offences (Law Enforcement Purposes) through the assessment and management of risk presented by MAPPA offenders and may not be processed for a purpose that is not a law enforcement purpose unless it is authorised by law.

3.4 Information-sharing must be necessary

Any interference with the right to private life by a public authority (such as a criminal justice agency) must be "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" (Article 8 of the European Convention on Human Rights). The sharing of information by MAPPA agencies for MAPPA purposes under this Agreement satisfies these conditions in so far as it is necessary to prevent disorder or crime or to administer justice.

3.5 Information-sharing must be proportionate

In human rights law, the concept of proportionality means doing no more than is necessary to achieve a lawful and reasonable result. In addition, the third Data Protection Principle of the DPA 2018 provides that personal data must be adequate, relevant, and not excessive in relation to the purpose for which it is being shared. For MAPPA agencies, this means ensuring that information about the data subject is relevant to assessing and managing risk and that no more information is shared than is needed to manage that risk. For example, if only an individual's name and address are needed, sharing their race and religion would be disproportionate.

Decisions on what is appropriate to share under this Agreement must be made on a case by case basis and there should be a clear link between the information provided and how it will serve the law enforcement purposes. Each agency should follow its own data protection policies and professional guidance. For example, healthcare practitioners should follow the General Medical Council guidance on Disclosure for the Protection of Patients and Others available at https://www.gmc-uk.org/ethical-guidance/ethical-guidance-for-doctors/confidentiality/disclosures-for-the-protection-of-patients-and-others#paragraph-60.

4 Process

4.1 Sharing of information within MAPPA

All relevant information will be extracted from any electronic and physical data systems within RA and DTC agencies and shared appropriately with other RA and DTC agencies. All reasonable steps must be taken to ensure that relevant information is accurate and up to date. Relevant information is information that it is lawful, necessary and proportionate to share in order to prevent crime and protect the public.

Information will be shared at MAPPA meetings where individual offenders are being discussed. Invitations to meetings will include sufficient detail to enable the subject(s) being considered at the meeting to be identified. All attendees at MAPPA meetings will sign a confidentiality statement before each meeting. MAPPA meetings will be formally minuted and all resulting documentation appropriately protected using the Government Security Classification Scheme (GSCS). Numbered copies of these minutes will be provided at the meetings and collected afterwards. Attendees will not take copies to or from meetings.

Information may also be shared using MAPPA documentation, at meetings of professionals, at core group meetings and in ad hoc interactions. Meetings and interactions must either be formally minuted or recorded in case management systems. Where an agency declines to disclose information this should also be recorded together with any reasons to support this view.

4.2 Transmission of information

Transmission of recorded data about MAPPA offenders should be done by secure e-mail where possible (see https://www.gov.uk/guidance/securing-government-email for details). Electronic information must not be sent via unsecure e-mail or other electronic means, such as calendars. If an agency does not have access to secure e-mail then arrangements should be made for them to set up a secure e-mail via the CJSM (Criminal Justice Secure email) service. Where it is not possible or appropriate to send information via secure e-mail, it should be sent by trackable post or trusted courier service using double envelopes, both fully addressed, but with the protective marking and descriptor shown on the inner envelope only. Once information has been transmitted to a partner's systems, they will be responsible for its storage, management and disposal.

4.3 Retention of information

Each agency must have a data retention and destruction policy in line with the Data Protection Principles of the DPA 2018 (see 8.1-8.7 of this Agreement). This policy will set out how personal data is stored and when it will be reviewed and destroyed. Appropriate security measures must be established by each agency to prevent unlawful processing and accidental loss, destruction or damage of personal data.

Personal data must not be kept longer than is necessary for a law enforcement purpose. When papers are no longer necessary they must be destroyed in line with the agency's retention and destruction policies using a cross cut shredder. Information held in electronic systems will also be destroyed in accordance with each agency's retention and destruction policies.

4.4 ViSOR

ViSOR is a Home Office resource designed for the management of MAPPA and Potentially Dangerous Persons. RA agencies should use the ViSOR system to share information under this Agreement. Instructions on the use of ViSOR are available in the ViSOR National Standards V3.2 (currently under review) and the Security Operating Procedure for ViSOR Users (currently under review) and must be adhered to. All parties to this Agreement accept responsibility for ensuring that all agreed security arrangements are complied with. Each party reserves the right to audit where an information security breach has occurred. Any unauthorised access or disclosure of information or breach of this Agreement will be dealt with through the internal discipline procedures of the individual parties. The annual review of this agreement will include a review of any issues around compliance with the agreed security measures.

4.5 Freedom of Information and Subject Access Requests

It is recognised that any of the parties to this Agreement may receive FOI or SAR requests for information that relate to the operation of this Agreement. All agencies will follow the instructions in the MAPPA Guidance in relation to requests for MAPPA minutes. All other requests should be dealt with in line with the receiving agency's procedures. Before disclosing information, all agencies will consult those agencies who are likely to be affected by the disclosure (or non-disclosure) of the information requested.

4.6 Disclosure of Information to Third Parties outside MAPPA

Information about a specific offender may be disclosed to a third party not involved in MAPPA as part of a Risk Management Plan (RMP) or under The Child Sex Offender Disclosure Scheme or Domestic Violence Disclosure Scheme. For the purposes of this Agreement, ***information-sharing*** is the sharing of information between the agencies involved in MAPPA, whereas ***disclosure*** is the necessary sharing of specific information about a MAPPA offender with a third party, not involved in MAPPA, for the purpose of protecting the public. Disclosure is not covered by this Agreement and must comply with the instructions set out in the MAPPA Guidance.

5 Other Arrangements

5.1 Business Continuity

Each partner will keep this agreement in a central location accessible to all members of staff who need to be aware of it. Each partner will appoint a nominated person and a deputy to be its main point of contact for all matters relating to this agreement. Deputies will ensure business continuity if the original point of contact is absent.

5.2 Publication of the Agreement

To comply with the fair and lawful processing principle of the DPA 2018 and the principles of the Freedom of Information Act 2000 (FOIA), the RA will publish this Agreement in their FOIA Publication Schemes so that members of the public can see how their information will be used and with whom it may be shared.

5.3 Breaches

If any party to this Agreement becomes aware of a security breach, or breach of confidence in relation to the data covered by this Agreement, or any breach of the terms of this Agreement, the party with responsibility for the area of activity in which the breach occurred, shall:

- immediately inform other parties to this agreement that a breach has occurred;
- immediately investigate the cause, effect and extent of the breach;
- report the results of the investigation to the other parties, without delay; and
- use all reasonable efforts to rectify the cause of such breach.

Each party will ensure that all staff with responsibility for implementing this Agreement are made aware that the disclosure of personal information without consent of the data subject must only occur where allowed under the DPA and as specified in this Agreement.

5.4 Complaints

Complaints about the disclosure or use of information under the terms of this Agreement should be dealt with in accordance with the relevant party's internal arrangements or in line with the MAPPA Guidance (see Chapter 29 – Complaints).

6 Undertaking to comply with this Agreement

The agencies signing this agreement agree that the principles and procedures set out in this agreement provide a lawful and secure framework for the sharing of information between them in a manner compliant with their statutory and professional responsibilities under MAPPA.

Therefore they undertake to:

- Implement and adhere to the principles and procedures set out in this agreement;
- Ensure timely and comprehensive sharing of information with each other and other partner agencies as appropriate, subject only to restrictions specified in this agreement;
- Engage in a review of this agreement with partners six months after its implementation and annually thereafter.

We, the undersigned, agree and confirm that each agency/organisation that we represent will adopt and comply with this Information Sharing Agreement:

Contact details

Kate Munson, Chair of the SMB and Head of NPS Humberside (Hull and East Riding)

Office address: Probation Services – Barclays House, Hull, HU1 1RS

Telephone: 01482 480000 / 07753 897660

E-mail: Kate.munson@justice.gov.uk

Signed: 

Name in print: Kate Munson

Humberside Strategic Management Board (SMB)

On behalf of the Responsible Authority

Contact details for Duty to Co-operate Agency

Name:……

Organisation:……....

Office address: ……

Telephone:……....

E-mail:……..

Signed……

Name in print……

Post of signatory ……. ……

Date……

7 Annex A - Glossary of Data Protection Act 2018 Terms

- **Data controller** – the competent authority which, alone or jointly with others, determines the purposes and means of the processing of personal data.

- **Data processor** – any person who processes personal data on behalf of the controller (other than a person who is an employee of the controller).

- **Personal data** – any information relating to an identified or identifiable living individual who can be identified, directly or indirectly, by reference to an identifier (such as a name, an identification number, location data or an online identifier), or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

- **Processing of data** – means an operation or set of operations which is performed on information, or on sets of information, such as:

  (a) collection, recording, organisation, structuring or storage;

  (b) adaptation or alteration;

  (c) retrieval, consultation or use;

  (d) disclosure by transmission, dissemination or otherwise making available;

  (e) alignment or combination; or

  (f) restriction, erasure or destruction.

- **Sensitive processing** – means:

  (a) the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;

  (b) the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual;

  (c) the processing of data concerning health;

  (d) the processing of data concerning an individual's sex life or sexual orientation.

- **Data protection impact assessment** – is an assessment of the impact of the envisaged processing operations on the protection of personal data.

- **Subject access request (SAR)** – a data subject is entitled to obtain from the controller confirmation as to whether or not personal data concerning him or her is being processed, and where that is the case, access to the personal data. The controller may restrict, wholly or partly, the right of access for a number of reasons, including as a necessary and proportionate measure to avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties. The information to which the data subject is entitled must be provided in writing within one month.

8 Annex B

8.1 First Principle – Data processing must be lawful and fair

The processing of personal data for a law enforcement purpose is lawful only if and to the extent that it is based on law and either:

(a) the data subject has given consent to the processing for that purpose, or

(b) the processing is necessary for the performance of a task carried out for that purpose by a competent authority.

Section 325 of the Act places statutory obligations on RA and DTC agencies to co-operate in order to carry out their MAPPA functions. Section 325(4) expressly permits the sharing of information between these agencies for MAPPA purposes and is the primary power to share information under MAPPA.

Section 115 of the Crime and Disorder Act 1998 (as amended by the Police and Justice Act 2006) (CDA) empowers any person to disclose information to certain specified authorities (which includes the MAPPA RA and most of the DTC agencies) for the purposes of preventing crime and disorder and re-offending.

Section 14 of the Offender Management Act 2007 empowers certain persons (including the MAPPA RA) to exchange information in relation to the probation and prison services and offender management purposes.

The MAPPA RA and DTC agencies have their own statutory powers to share information on sexual and violent offenders for MAPPA purposes and agencies who are party to this Agreement should expressly identify those statutory powers and ensure that they exercise them.

The Common Law also enables certain authorities (including the police) to process personal information in connection with the exercise of their Common Law powers. The police may use this legal gateway to exchange information with any person if it pursues a policing purpose (defined as including the prevention and detection of crime and disorder, protection of vulnerable groups, and bringing offenders to justice) and it does not breach any statutory restriction or duty of confidentiality.

A duty of confidence may exist towards a data subject when an RA or DTC agency has received any information in confidence. However, a duty of confidence is not absolute and can be overridden by several factors, such as another legal obligation, the consent of the individual concerned, or by demonstrating that disclosing the information would be in the public interest. Public interest factors for MAPPA disclosure include:

- Safeguarding children;
- Protecting other vulnerable people;

- Preventing the commission of criminal offences;
- Bringing offenders to justice.

Sensitive processing for law enforcement purposes may only be carried out if the agency has an appropriate policy document in place and either:

(a) the data subject has given consent to the processing, or

(b) the processing is strictly necessary for the law enforcement purpose and the processing meets at least one of the conditions from Schedule 8 of the DPA (see 8.2 below).

Fair Processing Conditions (Schedule 8 DPA)

Statutory etc purposes

Processing is necessary for the exercise of a function conferred on a person by an enactment or rule of law, and is necessary for reasons of substantial public interest.

Administration of justice

Processing is necessary for the administration of justice.

Protecting individual's vital interests

Processing is necessary to protect the vital interests of the data subject or of another individual.

Safeguarding of children and of individuals at risk

Processing is necessary for the purposes of protecting an individual from neglect or physical, mental or emotional harm, or protecting the physical, mental or emotional well-being of an individual, where the individual is aged under 18, or aged 18 or over and at risk. The processing is necessary for reasons of substantial public interest and is carried out without the consent of the data subject for one of the following reasons:

- consent to the processing cannot be given by the data subject;
- controller cannot reasonably be expected to obtain the consent of the data subject to the processing; or
- the processing must be carried out without the consent of the data subject because obtaining the consent of the data subject would prejudice the provision of protection.

Personal data already in the public domain

Processing relates to personal data which is manifestly made public by the data subject.

Legal claims

Processing is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings), or for the purpose of obtaining legal advice, or for the purposes of establishing, exercising or defending legal rights.

Judicial acts

Processing is necessary when a court or other judicial authority is acting in its judicial capacity.

Preventing fraud

Processing is necessary for the purposes of preventing fraud or a particular kind of fraud, and consists of:

- the processing or disclosure of personal data by a competent authority as a member of an anti-fraud organisation, or
- the processing or disclosure of personal data by a competent authority in accordance with arrangements made by an anti-fraud organisation.

Archiving etc

Processing is necessary for archiving purposes in the public interest, for scientific or historical research purposes, or for statistical purposes.

8.2 Second Principle – Purpose must be specified, explicit and legitimate

The law enforcement purpose for which personal data is collected must be specified, explicit and legitimate, and personal data must not be processed in a manner that is incompatible with the purpose for which it was collected. Personal data collected for a law enforcement purpose may be processed for any other law enforcement purpose (whether by the controller that collected the data or by another controller) provided that the controller is authorised by law to process the data for the other purpose, and the processing is necessary and proportionate to that other purpose. Personal data collected for any law enforcement purpose may not be processed for a purpose that is not a law enforcement purpose unless the processing is authorised by law.

8.3 Third Principle – Data must be adequate, relevant and not excessive

Personal data processed for any the law enforcement purpose must be adequate, relevant and not excessive in relation to the purpose for which it is processed.

8.4 Fourth Principle – Data must be accurate and kept up to date

Personal data processed for any law enforcement purpose must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the law enforcement purpose for which it is processed, is erased or rectified without delay. Personal data based on facts must, so far as possible, be distinguished from personal data based on personal assessments. A clear distinction must, where relevant and as far as possible, be made between personal data relating to different categories of data subject, such as:

- persons suspected of having committed or being about to commit a criminal offence;
- persons convicted of a criminal offence;
- persons who are or may be victims of a criminal offence;
- witnesses or other persons with information about offences.

All reasonable steps must be taken to ensure that personal data which is inaccurate, incomplete or no longer up to date is not transmitted or made available for any law enforcement purpose. The quality of personal data must be verified before it is transmitted or made available. The necessary information enabling the recipient to assess the degree of accuracy, completeness and reliability of the data and the extent to which it is up to date must be included in all transmissions of personal data. If, after personal data has been transmitted, it emerges that the data was incorrect or that the transmission was unlawful, the recipient must be notified without delay.

8.5 Fifth Principle – Data must be kept for no longer than is necessary

Personal data processed for any law enforcement purpose must be kept for no longer than is necessary for the purpose for which it is processed. Appropriate time limits must be established for the periodic review of the need for the continued storage of personal data for any law enforcement purpose.

8.6 Sixth Principle - Security

Personal data processed for any law enforcement purpose must be so processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures (and, in this principle, “appropriate security” includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage).

8.7 Privacy Notice

The controller must make available to data subjects the following information (whether by making the information generally available to the public or in any other way):

- the identity and the contact details of the controller;
- where applicable, the contact details of the data protection officer;
- the purposes for which the controller processes personal data;
- the existence of the rights of data subjects to request from the controller—

  (i) access to personal data,

  (ii) rectification of personal data

  (iii) erasure of personal data or the restriction of its processing;
- the existence of the right to lodge a complaint with the Commissioner and the contact details of the Commissioner.

The provision of this information is commonly known as a ‘Privacy Notice’.