Information Sharing Agreement

Women's Estate Case and Support Panel (WECASP)

THIS ISA is made on the 01042021

BETWEEN

The Parties that are stated as core members of the Panel as mentioned above; namely the following representatives:

Her Majesty's Prison and Probation Service (HMPPS) and National Health Service England (NHSE/I)

1 Background:

a. Data Protection legislation places certain obligations upon Information controllers and processors to ensure that they provide sufficient guarantees to ensure that the processing of personal Information (including special categories of personal Information and sensitive processing) carried out is secure;
b. This ISA exists to ensure that there are sufficient security guarantees in place and that the processing complies with all such obligations as set out in Data Protection legislation;
c. HMPPS and the Information Recipient will both be responsible for compliance with Data Protection legislation in relation to the shared information and this ISA exists to provide a framework for that compliance.
d. This ISA may follow on from a Privacy/Data Impact Assessment and confirms a lot of the information already gathered and agreed.

IT IS NOW AGREED as follows:

2 Definitions and interpretation

2.1 For the purposes of this ISA the HMPPS who are the Controllers (and give the representatives mentioned above information for them to use for their own purpose under the documented legal basis as 'processors'. The representatives are not sharing HMPPS information with anyone else.

2.2 In this ISA the following words and phrases shall have the following meanings, unless expressly stated to the contrary:

a. "**Act**" means UK Data Protection Legislation including the Data Protection Act 2018 (DPA);

b. "**Information Controller**" has the meaning as given in the DPA;

c. "**Data Protection Legislation**" means the DPA, Regulation (EU) 2016/679 of The European Parliament and of The Council of 27 April 2016 (the General Data Protection Regulation (GDPR)), Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 (the Law Enforcement Directive), the Regulation of Investigatory Powers Act, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations, the Electronic Communications Data Protection Directive, the Privacy and Electronic Communications (EC

Directive) Regulations and all applicable laws and regulations relating to processing of personal Information (including special categories of personal Information and sensitive processing) and privacy, in force at the time of the processing being conducted including where applicable the guidance and codes of practice issued by the Information Commissioner;

d. "**Data Subject**" has the meaning as given in the DPA;

e. "**Information Recipient**" has the meaning of the organisation/person receiving the Information in this ISA;

f. "**Environmental Information Regulations**" means the Environmental Information Regulations 2004, as amended, together with any guidance and/or codes of practice issues by the Information Commissioner or relevant Government Department in relation to such regulations;

g. "**FOIA**" means the Freedom of Information Act 2000, as amended;

h. "**Parties**" means the parties to this ISA, namely HMPPS and the Information Recipient;

i. "**Personal Information**" has the meaning as given in the DPA;

j. "**Special categories of personal Information**" (formerly known as 'sensitive personal Information') has the meaning as given in the DPA;

k. "**Project**" means the steps described in Clause 6 of this ISA;

l. "**Processing**" has the meaning as given in the DPA;

m. "**Sensitive processing**" has the meaning as given in the DPA;

n. "**Request for Information**" means a request for information or an apparent request under FOIA or the Environmental Information Regulations;

o. "**Responsible Information Asset Owner**" means an individual occupying the position of Information Asset Owner within HMPPS, who has asset ownership obligations in relation to the Shared Information;

p. "**Shared Information**" means the information to be shared as set out in Clause 5 of this ISA;

q. "**Joint Controllers**" has the meaning as given in the DPA.

r. **HMG** – Her Majesties Government – Security Policy Framework (referenced throughout and security classifications detailed in Annex 1)

In this ISA:

2.3 the masculine includes the feminine and neuter;

2.4 person means a natural person;

2.5 the singular includes the plural and vice versa;

2.6 a reference to any statute, enactment, order, regulation or other similar instrument shall be construed as a reference to the statute, enactment, order, regulation or instrument as amended by any subsequent statute, enactment, order, regulation or instrument or as contained in any subsequent re-enactment, and in any event, to the version currently in force at the time of this ISA.

2.7 Headings are included in this ISA for ease of reference only and shall not affect the interpretation or construction of this ISA.

2.8 References in this ISA to Clauses, Paragraphs and Annexes are, unless otherwise provided, references to the Clauses, Paragraphs and Annexes of this ISA.

2.9 In the event and to the extent only of any conflict or inconsistency between the provisions of the Clauses and the provisions of the Annexes, the provisions of the Clauses shall prevail; or

a. the provisions of this ISA and the provisions of any document referred to or referenced herein, the provisions of this ISA shall prevail.

3 Purpose(s) and legal basis

3.1 The shared Information is provided for the following purpose(s).

3.2 The WECASP take referrals for those individuals who are located across the women's estate in either Public Sector Prisons or Private Contracted Prisons who have given consent for their information to be shared. This information includes overview information around offence and sentence, prison behaviour including adjudications, transfer history, engagement with prison departments including healthcare, therapeutic needs and the presenting behaviour challenges. Supporting documents are also provided that may include psychological assessments or formulations for specific cases (by the NHS) and there are, on occasion, written behaviour updates statements from the prison staff. Referred cases are discussed at the multidisciplinary Panel and pathways, advice and support services are recommended to the operational staff. Minutes and Actions are drawn up by HMPPS Women's Team, (who chair and administer the panel) and submitted out to the core panel members in addition to interested parties for cases.

3.3 The objective of the WECASP is to provide multidisciplinary support to prisons in the management of a small number of complex individuals within the women's estate who are not progressing in their sentence; with the aim of stabilising their behaviour, improving their wellbeing and supporting the surrounding staff groups to help reduce their risk accordingly. This is a direct response to the Women's Custodial Estate Review in 2013 and the legal basis for HMPPS sharing information is contained within the provisions of the Section 14 of Offender Management Act 2007. By identifying and enabling those within the women's estate to overcome the specific barriers to them progressing through their sentence plan, the parties will, by virtue, reduce re-offending within that cohort. Where possible, information will be shared with the data subject's consent. This is to enable a bond of trust to be built up between the data subject and the parties. Any risks to self, others and children are to be raised immediately and it is understood by all parties that consent does not need to be obtained from the data subject in these exceptions. These exceptions can be found in the various Schedules of the DPA 2018.

3.4 The information to be shared under this Agreement consists of the following:

The initial information shared between the parties will be that information which is contained within the referral form at Annex 1 to this Agreement and supporting documentation that is sent alongside the referral.

Any additional information will be assessed and shared on a case by case basis either prior to or at the WECASP Panel. It is at this point that the Public Sector Prison / Contracted Prison representative will provide an update on the case to the Panel for consideration of acceptance onto the WECASP caseload.

The outcomes of the Panel will be shared with all attending parties, via the distribution of meeting minutes.

It is agreed that the minutes of each meeting will be sent to all core Panel members, in addition to the allocated Prison and/or Probation staff responsible for the case who attended the meeting.

The minutes will then be redacted and disseminated to the Governors/Directors of the prisons, providing the information in relation to data subjects within their establishment only. This redaction is to reduce the risk of information being transferred to establishments without a legitimate interest in the data subject.

Any requests from Governors/Directors for information relating to additional individuals known to the WECASP must be submitted to the Chair of the WECASP and will be considered on a case by case basis, having regard to the principles of proportionality.

Information exchanged under this Agreement will be classified as "official sensitive", under the terms of the Government's Information Handling criteria, and must be handled, processed and stored in accordance with the same. All parties must familiarise themselves with these requirements and the expectation is that they are able to comply with the same. If any party is unable to comply then they must contact the HMPPS as soon as practicable and in any case prior to placing their signature on any agreement in relation to sharing of HMPPS information.

The data recipient will ensure that the information requested is both reasonable and proportionate to meet a legitimate need and is not excessive in its nature.

Multidisciplinary meetings are sometimes held outside of the WECASP Panel. The remit of these meetings is detailed within the Policy Framework guidance, however, for the purpose of this Agreement, it is sufficient to state the following. A brief note will be taken at these meetings which captures concerns / actions in relation to the data subject. The notes will be circulated to interested parties following the meeting. These notes may also be requested at a later date and may be discussed at the WECASP Panel, should they become relevant to the data subject's sentence progress.

Data Ref	Type of Data	Purpose of Data	Format and Detail of Data
Example	***Personal Contact Information***	***To enable access and communication whilst assessing services***	***Housing Consent Form and/or NPS Referral***
1	Referral Form (as annexed)	This will enable consent from the service user to share their details with the panel and to accept that the panel are acting in their best interests to secure further support	As per the annex
2	Input to the panel – need to list all things mentioned in background	Information in relation to behaviour, reports, adjudications. Info is normally already stored on PNOMIS system. Sometimes, prior to meeting, reports from HMPPS Psychologists and Offender Managers are submitted. Reports are completed by HMPPS staff. Reports from community agencies may also be introduced, with the express consent of the data subject to share.	Via written and verbal updates to the Panel
3	Outputs from the Panel	Minutes and actions to reflect the discussion and record any decision from the meeting	Word Documents submitted over email

3.5 The legal basis for sharing this information is:

1. Section 14 Offender Management Act 2007 allows for the NPS to share of information for offender management purposes
2. Article 6(1)(a) of the GDPR allows for the processing of personal information whereby the data subject has given their consent for the data to be processed. This processing applies to the initial referral form in this Agreement.
3. Article 6(1) (e) of the GDPR provides a legal basis for sharing information to fulfil a function of official authority within the Member State. As the Secretary of State for Justice has devolved the responsibility to manage offenders to the HMPPS then in so doing we are fulfilling our obligations under this Article.
4. Schedule 8, paragraph 4 of the DPA 2018 provides that information can be shared for safeguarding purposes without the consent of the data subject, where circumstances dictate that this is necessary to fulfil the legitimate aim.

4 Further use of Shared Information

4.1 The Information Recipient agrees not to process the shared Information for purposes that are incompatible with the purposes in Clause 3.

4.2 The Information Recipient agrees not to process the shared Information, except as necessary for the performance of the information share and to achieve the purposes in Clause 3, unless expressly authorised in writing by HMPPS.

4.3 The steps comprising the Information share are set out in Clause 6. This ISA does not relate to any Information sharing between the Parties not forming part of the Information share.

5 Representatives

5.1 The Parties will each appoint a representative to be the primary point of contact in all matters relating to this Agreement:

Organisation	SPOC name	Contact details
HMPPS		
NHS England		

5.2 The Parties agree that these nominated representatives will correspond at regular intervals throughout the Information share to discuss activity in general and will provide updates to each other on matters of mutual interest.

5.3 The persons who will be supervising the processing of the shared Information are the relevant positions within the organisations identified in Clause 5.1.

5.4 The persons who will be processing the shared Information are operational staff and operational support staff within those organisations identified in Clause 5.1 above.

5.5 The persons who will have access to the shared Information are as per 5.3 and 5.4 above.

6 Protection of personal Information

6.1 The Information Recipient, agrees to process any personal Information (including special categories of personal Information and sensitive processing) in the shared information in accordance with the requirements of this ISA, and in particular the Information Recipient agrees that it shall:

a. process the personal Information (including special categories of personal Information and sensitive processing) only in accordance with instructions from HMPPS (which may be specific instructions or instructions of a general nature as set out in this ISA or as otherwise notified by HMPPS to the Information Recipient).

b. have an information risk policy setting out how they implement the measures in Her Majesties Government (HMG) Security Policy Framework in their own activity and that of their delivery partners, and monitor compliance with the policy and its effectiveness.

c. process the personal Information (including special categories of personal Information and sensitive processing) only to the extent, and in such manner, as is necessary for the information share or as is required by law.

d. comply with obligations equivalent to those imposed on HMPPS as the Information Controller by applicable DPA and in particular implement appropriate technical and organisational measures to protect the personal Information (including special categories of personal Information and sensitive processing) against unauthorised or unlawful processing and against accidental loss, destruction, damage, alteration or disclosure. These measures shall be appropriate to the harm which might result from any unauthorised or unlawful processing, accidental loss, destruction or damage to the personal Information (including special categories of personal Information and sensitive processing) and having regard to the nature of the personal Information (including special categories of personal Information and sensitive processing) which is to be protected.

e. handle all personal information within the scope of this Information sharing ISA and in accordance with the allocated Government Security Classification (as per Annex 1) and therefore the appropriate handling rules while it is within the Information control of the Information recipient. Where it is marked with the handling caveat OFFICIAL-SENSITIVE you should specify any

additional access controls and review both the classification and access controls regularly and allocate a higher level if justified**.**

f. obtain prior written consent from HMPPS in order to transfer the personal Information (including special categories of personal Information and sensitive processing) to any sub-contractor or other third party.

g. ensure that all Information Recipient personnel required to process the personal Information (including special categories of personal Information and sensitive processing) are informed of their obligations under this ISA with regard to the security and protection of personal Information (including special categories of personal Information and sensitive processing) and that those obligations are complied with and that they successfully complete information risk awareness training at least annually.

h. take reasonable steps to ensure the reliability of any Information Recipient personnel who have access to the personal Information (including special categories of personal Information and sensitive processing).

i. ensure that none of Information Recipient personnel publish, disclose or divulge any of the personal Information (including special categories of personal Information and sensitive processing) to any third party unless directed in writing to do so by HMPPS.

j. notify HMPPS (within five Working Days) if it receives:
   i. a request from an Information Subject to have access to that person's personal Information (including special categories of personal Information and sensitive processing); or
   ii. a complaint or request relating to HMPPS's obligations under Data Protection legislation.

k. provide HMPPS with full co-operation and assistance in relation to any complaint or request made, including by:
   i. providing HMPPS with full details of the complaint or request;
   ii. complying with an Information Access Request within the relevant timescales set out in Data Protection legislation and in accordance with HMPPS's instructions; and
   iii. providing HMPPS with any personal Information (including special categories of personal Information and sensitive processing) it holds in relation to an Information Subject (within the timescales required by HMPPS).

l. permit HMPPS or HMPPS's Representative (subject to reasonable and appropriate confidentiality undertakings), to review the Information Recipient's personal Information processing activities (and/or those of its agents, subsidiaries and sub-contractors) and comply with all reasonable requests or directions by HMPPS to enable HMPPS to verify and/or procure that the Information Recipient is in full compliance with its obligations under this ISA. These activities could include but are not limited to:
   i. Inspection of a sample of the activities of those individuals with rights to transfer personal Information (including special categories of personal Information and sensitive processing) to removable media, to ensure that there is still a business case for them to have those rights;
   ii. Inspect a sample of those individuals who have left roles with access to personal Information (including special categories of personal Information and sensitive processing), to ensure that access rights have been removed;
   iii. Inspect a sample of removable media (if used) to ensure that required safeguards are in place;
   iv. Inspect unencrypted back-ups and reconcile them with material that has been recorded;
   v. Monitor disposal channels for paper records containing personal Information (including special categories of personal Information and sensitive processing) to ensure this has been properly handled;
   vi. Ask for sample electronic media to be processed and tested to attempt Information recovery.

m. Provide a written description of the technical and organisational methods employed by the Information Recipient for processing personal Information (within the timescales required by HMPPS); and

n. not process personal Information outside the European Economic Area.

6.2 The Information Recipient shall at all times comply with the "Framework for Information Processing by Government" as provided by Sections 191-194 of the DPA and all guidance published by HMG, and the Information Commissioner, and when applicable the provisions of the Law Enforcement Directive as embodied in the DPA, and shall not perform its obligations under this ISA in such a way as to cause HMPPS to breach any of its applicable obligations under the DPA.

6.3 In consideration of the obligations undertaken by the Information Recipient, HMPPS, as Information Controller, agrees that it shall ensure that it complies at all times with Data Protection legislation, and, in particular, HMPPS shall ensure that disclosure of Shared Information is lawful with regard to its powers, the requirements of Data Protection legislation, the Human Rights Act 1998 and the common law of confidentiality.

7 Security of Shared Information

7.1 The Information Recipient agrees to process all the shared information in accordance with the following security requirements:

a. access to the shared information, any copies made of the shared information and the information contained in them is limited solely to the persons specified in this ISA;

b. access to the shared information is minimised to the smallest pool of accessible records possible;

c. the confidentiality of the shared information will be preserved in outputs and publications, as detailed in Clauses 15 and 16;

d. shared Information will only be accessed by devices or services that are themselves subject to restricted access.

e. Access to cloud-hosted or on-premise devices or services that can access the shared information will only be through mechanisms that comply with HMG Security Policy Framework such as suitability strong passwords and multi-factor authentication;

f. the means of access to the shared information (such as passwords or pass-phrases) will be kept secure and not disclosed to any person or service, under any circumstances other than those specified in this ISA;

g. hard copies and backups of shared information will be stored in a secure, access restricted filing cabinet or shared folder;

h. shared information will not be accessed at a location outside the UK;

i. shared information should be held and accessed on paper or ICT systems on secure premises;

j. whenever possible, data should be protected by Transport Layer Security when in transit i.e. communicated over the open internet, and encrypted at rest i.e. when its resident on another domain."

k. the Information is backed up in case of corruption.

l. technical and organisational controls and processes for system, network and security capabilities and components are tested regularly to maintain and demonstrate the continuing correctness of their operation and correct functioning.

m. logs of processing operations as set out in section 62 of the DPA will be kept for all Information processing in this information share for law enforcement purposes (as defined by section 31 of the DPA

7.2 HMPPS reserves the right to conduct an on-site audit of the Information Recipient's confidentiality and security procedures and practices, or to require a report of such an audit by an independent assessor.

8 Integrity of Shared Information

8.1 The Information Recipient shall not delete or remove any proprietary notices contained within or relating to the shared information.

8.2 The Information Recipient shall take responsibility for preserving the integrity of the shared information and preventing the corruption or loss of the shared information.

9 Freedom of information

9.1 The Data Protection Officer at the information asset owning organisation should be contacted by any Partner Organisation receiving a SAR or FOI request that captures information disclosed to them under this Agreement. They will contact the relevant nominated Data Protection Officers at all relevant Partner Organisations to determine whether they wish to claim an exemption or if they have any objections under the provisions of the relevant Act before disclosure takes place.

9.2 Where the Parties are subject to the provisions of FOIA and the Environmental Information Regulations and shall assist and co-operate with each other to enable each other to comply with their respective statutory duties in relation to Requests for Information. In particular, where a Party receives a Request for Information pertaining to the subject matter or operation of this ISA, it shall as soon as practicable notify the other Party's nominated representative, in writing, of the details of the information requested, the date such Request was made and, if permitted by law, the name of the person making the Request. The Party which has received the Request shall, prior to responding to the applicant, consult with the other Party and to facilitate such consultation shall provide it with a copy of all information which it proposes to disclose not less than 5 working days before disclosure.

10 Statutory compliance

10.1 The Parties shall comply with all relevant legislation, regulations, orders, statutory instruments and any amendments or re-enactments thereof.

11 Transfer of Shared Information

11.1 The Information Recipient guarantees that the shared Information will be transferred via recognised secure email systems, where possible. These systems must comply with and be certified by the Ministry of Justice as being secure. This will include 3rd party emails. No information, falling under the provisions of a Data Protection Act 2018, will be sent by the NPS / HMPPS to any unsecured email account or stored on an unsecure computer system.
Information will also be exchanged between the signatories to this Agreement verbally at the WECASP Panel. Throughout every exchange, all parties will observe and have regard to the common law principles of confidentiality.

11.2 Transfer of Information to or from removable media will be avoided wherever possible. Where it is not possible to avoid the use of removable media, HMPPS and the Information Recipient(s) will agree to apply all of the following conditions and agree these before invocation:

a. the information transferred to the removable media will be the minimum necessary to achieve the identified purpose, both in terms of the numbers of people covered by the information and the scope of information held;

b. only anonymised information will be held, if possible in the context of the purpose for the information share;

c. the removable media will be encrypted to a standard of at least FIPS140-2 or equivalent. In addition, it will be protected by an authentication mechanism, such as a password;

d. user rights to transfer Information to removable media will be carefully considered and strictly limited to ensure that this is only provided where absolutely necessary for the purposes specified in this ISA and subject to monitoring by HMPPS;

11.3 The Information Recipient guarantees that the shared information will be transferred in accordance with the HMG Security Policy Framework.

12 Ability to access Shared Information

12.1 The Information Recipient will ensure that it can access the shared information provided. When received, shared information should be opened and saved onto the Information Recipient's secure system. It is the Information Recipient's responsibility to inform HMPPS, within one week of receiving the Shared Information, if they are unable to access that shared information.

13 Products and publications

13.1 The shared information may allow for persons to be identified. The Information Recipient, therefore, agrees that no outputs will be produced that are likely to identify a person, unless specifically agreed with HMPPS.

14 Disclosure protection

14.1 Techniques for aggregation and disclosure protection, as part of the output of the Project, will be in accordance with the rules set out below.

a. Tables that contain very small sample numbers in some cells may be disclosive. The Information Recipient will ensure that tables do not report numbers or percentages in cells based on only 5 or less cases. Cells based on 5 or less cases should be combined with other cells or, where this is not appropriate, reported as 0 percent.

b. Tabular outputs should not report analyses at detailed levels of geography. The Information Recipient will clear with HMPPS, before publication, any tables below Government Office Region (Inner/Outer London).

c. Although most outputs from models or other statistical analysis will not be disclosive, the Information Recipient will ensure that persons, households or organisations cannot be identified. In particular, results based on very small numbers, should be avoided. Any output that refers to unit records, e.g. a maximum or minimum value, should be avoided. Models should not report actual values for residuals.

d. Graphical outputs should be based on non-disclosive information. The Information Recipient will take particular care not to report extreme outliers.

15 Matching or linking of Shared Information

15.1 The shared information will not be matched or linked with any other Information or information sources.

16 Duplication and copies

16.1 The Information Recipient agrees that no duplication of the Shared Information may take place or copies of the Shared Information be made other than as agreed in the description of the Project in Clause 3.3 or with the written MOU of HMPPS.

17 Duration of the Information share

17.1 The shared information will be provided for the period of 6 years.

17.2 The maximum duration of the information share will not exceed 6 years.

17.3 If a finite share date has been agreed and an extension is required; a request is to be made ahead of the finite end date and approval should be recorded and filed alongside this ISA.

18 Review

18.1 A review of the information share is to be conducted by HMPPS and Information recipient six months after coming into force and at least annually thereafter; a review form is attached at Annex 1.

18.2 HMPPS and the Information recipient will assess risks to the confidentiality, integrity and availability of information in this information share at least annually, taking account of extant Government wide guidance, and plan and implement proportionate responses.

19 Actions at end of the information share

19.1 At the end of the information share, the Information Recipient agrees to destroy all copies of the shared information, including temporary copies, printed copies, personal copies, derived Information sets and all electronic copies in a controlled way (and any removable media that was agreed for use), i.e.:

a. Destroy paper records by incineration, pulping or shredding so that reconstruction is unlikely;

b. Dispose of electronic media that have been used for protected personal Information through secure destruction, overwriting, erasure or degaussing for reuse.

19.2 The Information Recipient will ensure that the shared information is destroyed to the standards that meet government standards for secure and complete destruction.

19.3 After the shared information has been destroyed, the Information Recipient will sign a declaration to confirm that the Shared Information and all copies of the shared information have been destroyed and to the required standards.

20 Commencement and term

20.1 This ISA shall commence upon signature by the Parties and shall continue in effect until the Information share has been completed in accordance with the requirements of this ISA unless otherwise subject to earlier termination in accordance with Clause 22.

21 Loss and unauthorised release

21.1 The Information Recipient will report to HMPPS any suspected or actual loss or unauthorised access or release of the shared information, as soon as possible or no later than **4 hours** after the suspected or actual loss or unauthorised release.

21.2 The Information Recipient acknowledges that any loss or unauthorised release of the shared information can be treated as valid grounds for terminating this ISA by HMPPS.

21.3 Any loss or unauthorised release of the shared information by the Information Recipient will allow HMPPS to request that a full investigation into the cause of the loss or unauthorised release be undertaken; or allows HMPPS to undertake such an investigation itself

21.4 The Information Recipient fully indemnifies HMPPS for all financial loss and liability that may arise from loss or unauthorised release of the shared information by the Information Recipient.

22 Termination

22.1 Either Party may terminate this ISA upon [one] month's written notice to the other.

22.2 Either Party may terminate this ISA with immediate effect in the event of breach of its obligations by the other Party to this ISA.

AS WITNESS of which the parties have set their hands on the day and year first above written. Signatories are required to understand the responsibility that they hold in signing this ISA

SIGNED for and on behalf of
THE SECRETARY OF STATE
FOR JUSTICE
By:

.....

Name:.....

Title:.....

SIGNED for and on behalf of
THE INFORMATION RECIPIENT
By:

.....

Name:.....

Title:.....

23 Change History

This table depicts the history of the document and what has changed since the last version.

Version	Nature of Change	Author
0.1	First draft – example	Corinna Griggs, Information Management Programme Lead (temporary role)
0.2	Simplified all sections by adding the purpose and legal basis up front and all legal compliance sections thereafter, have also added in annexes as embedded documents for ease. Changes have been made to the annexes as follows: The document classification annex has had top secret and official removed as these are not applicable to ISA's, a document review form has been included to ensure readiness for the 12 month review and a document is available to capture any proposed changes if found throughout the reporting year. Annexes have been included to show the legal basis summaries and the copies of consent forms and or referrals (if required). All comments and changes accepted by the NPS Information Officers	
0.3	1st draft to WECASP for review and comment	Kev Kelly – NPS Info Assurance Officer

0.4	Amendments made in respect of comments from LP and KK	
1.0	Signed and Filed	

24 ANNEXES

These are the documents that are referred to in this document

Annex 1 Review Form
Annex 2 Referral Form
Annex 3 Re-referral Form
Annex 4 Privacy Statements

Annex 1 – Review Form

ISA Template_ANNEX 2 F

Annex 2 – Referral Form

Annex A - WECASP Referral Form.docx

Annex 3 - Re-referral Form

Annex B -
Re-referral form.doc

Annex 4 – Privacy Notices


NPS-Privacy-Notice.pdf


nhs-england-privacy-notice-v1.12.pdf