



National Offender  
Management Service



# National Offender Management Service

Changing lives

Brand guidance

2012

# NOMS Co-Financing Organisation

## Publicity regulations for providers and sub contractors

The NOMS Co-Financing Organisation has received over £140 million of European Social Fund (ESF) money to finance programmes in prisons and in the community to increase offenders' opportunities for employment.

The programmes are delivered on behalf of NOMS by a range of providers and sub contractors across England and Wales.

As a condition of receiving ESF money, NOMS and its contracted providers/sub contractors are required to make every effort to publicise the ESF contribution through all available publicity materials.

This requirement is clearly set out in the contract between NOMS and the EU. In turn, providers and sub contractors are contractually obliged to abide by the requirement too.

Any provider/sub-contractor not abiding by the requirement risks losing funding. The ESF regularly audits provider/sub-contractor publicity material and imposes tough penalties on these organisations that do not comply. British organisations have been fined over £150 million (combined) for not complying with this requirement. So far, NOMS and its providers have complied with the requirement but it must continue to be vigilant to ensure that ESF receives appropriate recognition.

## The requirement

The European Commission regulation no 1828/2006 contains full details and providers/sub contractors must read this document for themselves. It can be found on the ESF website [www.esf.gov.uk](http://www.esf.gov.uk). The information below is a summary of the main points and should not be relied upon for the full picture.

However the main ESF requirements (summarised), plus NOMS's own requirements are:

(1) The ESF logo, and mentions of financial support from the EU, must be displayed when ESF opportunities, activities and achievements are described and/or publicised. This includes, **but is not restricted to**, display on the following:

- All information and publicity materials, including websites, e-communications, correspondence and literature used by participants
- ESF programme documents such as regional ESF frameworks and Co-Financing plans
- Advertisements, press releases and any media targeted materials
- Display stands and exhibition material

(2) Co-Financing organisations and providers /sub-contractors must display ESF plaques (see below)

(3) Providers and sub contractors must ensure that:

- Information on funding opportunities offered by ESF and match funds is publicised as widely as possible
- They support other measures to publicise the ESF programme that may be agreed at national, regional and local levels
- All participants are notified and reminded of EU and ESF support at the start of and throughout their activity

For NOMS providers and sub contractors this means that offenders must all be informed at the start of a programme that their support is ESF funded. Posters and leaflets are provided to prisons and probation trusts

- The ESF logo and EU support are publicised on any document including any attendance or other certificate (eg course completion)
- Providers must give data about their projects to NOMS for inclusion in the publicly accessible list of beneficiaries and providers
- Providers and their sub contractors must provide case studies on request to NOMS for use in publicity

### **ESF Plaques**

All providers and sub-contractors must display an ESF plaque showing the European flag at their main locations (where more than 50 ESF or Match participants attend over the lifetime of the project).

The plaque must be clearly visible to staff, participants and other visitors using the building. Posters cannot be used as a substitute for a plaque.

For more details, providers must read the ESF action note 018/09 on the ESF website. It is a contractual requirement that a plaque is displayed. Plaques will be supplied by the NOMS Co-Financing Organisation.

### **ESF logo**

The ESF logo, along with guidance for its use, is available at [www.esf.gov.uk](http://www.esf.gov.uk). Organisations must read the guidance before using the logo. The logo strapline “Investing in jobs and skills” may be used but no other strapline is permitted.

## NOMS Branding

NOMS logo should also be used on the same items as those to which the ESF regulations apply. This can include:

- Websites
- Posters and leaflets
- Strategy documents and framework plans
- Display stands

The NOMS logo (below) is also governed by guidelines on its use. A copy of the logo and guidance for use is also available as a pdf in Annex 1:



National Offender  
Management Service

National Offender  
Management Service

For more information please contact Internal Communications by email:



**Q) The work that we do for NOMS, funded by ESF, is a very small part of our business. Do we still need to display a plaque?**

A) Yes. If you run any NOMS CFO/ESF funded activity, however small, you must display the plaque.

**Q) We are a small sub-contractor organisation and do not have a website. Do we need to set one up?**

A) No, not specifically but if you have any sort of web presence it must include the ESF logo. However there may be information that you must make publicly available and if you don't have a website it must be available in hard copy.

It is important to note that a website is a more cost effective option than providing printed material and it may be worth considering this as a long term saving measure.

**Q) I have been asked to give a leaflet to every offender that takes part in the programme. Is this practical?**

A) Yes. NOMS will supply the leaflets and further copies are available from your regional engagement manager. It is a specific requirement that offenders are informed at the start of their programme that this support receives ESF funding.

**Q) Must we have the logo on internal documents or memos?**

A) No. it is not necessary for most routine internal documents. However it should be included on larger high profile documents or committee papers that may have an external circulation.

**Q) Surely the ESF don't check everything?**

A) The ESF has committed a very significant amount of money to this project and in return they expect that this will be respected by the recipients and the appropriate recognition given. They make regular checks on publicity material from organisations of all types and sizes. So far, British organisations have been fined around £150 million because they did not comply with publicity requirements. In some cases up to 10% of the total grant has been recalled.

**Q) What do I do if I am not sure whether the item needs a logo?**

A) If you are a provider please contact NOMS CFO. If you are a sub-contractor please contact your provider in the first instance. Please check if you are uncertain as a wrong decision could lead to financial penalties.

## Annex 1 – NOMS Brand Guidance



# National Offender Management Service

Brand guidance



# Contents

Foreword	1
Old NOMS (now decommissioned)	2
New logo	3
Logo size (English)	4
Logo size (Welsh)	5
Logo without Royal Coat of Arms (English and Welsh)	6
Placing and size of the logo	7
Who should use the logo?	8
How should I use the logo?	9
How should I use the logo with existing brands?	10
Do not	11
Typefaces	12
Stationery templates	13
Online use	14
Contact	15





## Foreword

The National Offender Management Service was launched in April 2008 and is responsible for the delivery of all probation and prison services in England and Wales.

This presentation provides instruction on the use of the new logo for NOMS.



National Offender  
Management Service

The old NOMS logo is now  
decommissioned. It should not  
be used in any circumstances.

## Old NOMS



Ministry of  
**JUSTICE**

National Offender  
Management Service



## National Offender Management Service

This is the current NOMS logo. It is recommended that either white or black should appear as the background colour for the logo as illustrated below. If black or white is not available or applying the logo over an image background please choose the correct colour to achieve maximum contrast.

Do not place the logo over a busy background image.

## New logo



National Offender  
Management Service



National Offender  
Management Service





# National Offender Management Service

## Exclusion zone and minimum size (English)

In order to maximise its visual presence space is required around the logo. This is called an exclusion zone and serves the purpose of preventing any graphic element from interfering with the integrity of the logo.

### Exclusion zone

The dimensions of the exclusion zones are constructed as shown here. Any graphic element, including type, is only allowed to bleed up to the edge of the exclusion zone.

### Minimum size

If permission is granted the minimum size at which the landscape version can appear is 30mm (200pixels for online use). In exceptional circumstances, when the logo needs to be reproduced below minimum size, the logo should be used without the Royal Coat of Arms (see page 6). Examples of when this might occur include co-branding and name badge branding.

## Logo size (English)



X = Exclusion zone

At any scale, the exclusion zone around the logo is the height of the Royal Coat of Arms.

Minimum size – print



Minimum 30mm

Minimum size – on-line



Minimum 200 pixels



## Gwasanaeth Rheoli Troseddwyr Cenedlaethol

### Exclusion zone and minimum size (Welsh)

In order to maximise its visual presence space is required around the logo. This is called an exclusion zone and serves the purpose of preventing any graphic element from interfering with the integrity of the logo.

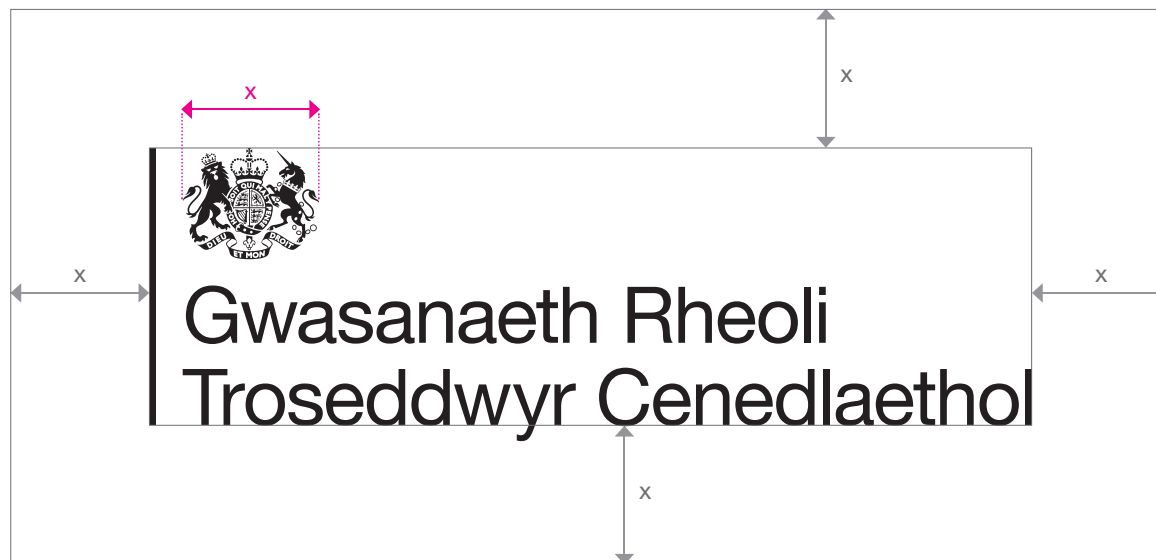
#### Exclusion zone

The dimensions of the exclusion zones are constructed as shown here. Any graphic element, including type, is only allowed to bleed up to the edge of the exclusion zone.

#### Minimum size

If permission is granted the minimum size at which the landscape version can appear is 30mm (200pixels for online use). In exceptional circumstances, when the logo needs to be reproduced below minimum size, the logo should be used without the Royal Coat of Arms. Examples of when this might occur include co-branding and name badge branding.

## Logo size (Welsh)



**x** = Exclusion zone

At any scale, the exclusion zone around the logo is the height of the Royal Coat of Arms.

Minimum size – print



Minimum 35mm

Minimum size – on-line



Minimum 270 pixels



## National Offender Management Service

### The simple version

The NOMS logo is made up of two elements, our name and the Royal Coat of Arms. These two elements should appear together as widely as possible. The Royal Coat of Arms must always appear at the top of a page.

There are some occasions where it is acceptable to use the logo without the Royal Coat of Arms. These are:

- where space is extremely limited
- when the logo is used at the bottom of the page.

### Exclusion zone

The clear space around the logo is known as the exclusion zone. It makes sure the logo is prominent and can be seen clearly whenever it appears. The recommended exclusion zone is based on the height of the colour line as shown. No other elements should appear within this space.

### Minimum size

We want to make sure our logo is presented clearly and consistently. That's why we have created a minimum size. The logo without the Royal Coat of Arms should never appear any smaller than 30mm for the English version and 45mm for the Welsh.

## Logo without Royal Coat of Arms (English and Welsh)

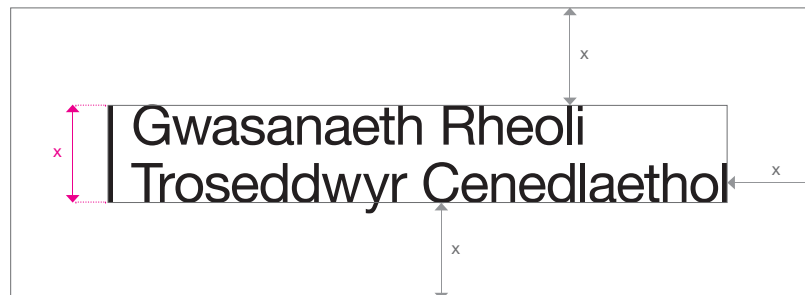
Logo without Royal Coat of Arms exclusion zone (English)



x = Exclusion zone

At any scale, the exclusion zone around the logo is the height of the colour line.

Logo without Royal Coat of Arms exclusion zone (Welsh)



Minimum size – English – print

National Offender  
Management Service

Minimum 30mm

Minimum size – Welsh – print

Gwasanaeth Rheoli  
Troseddwyd Cenedlaethol

Minimum 45mm



## National Offender Management Service

A clear corporate identity relies on the consistent positioning of the logo.

We recommend that logo should be positioned top left in all circumstances.

Take care to follow the exclusion zone guidelines.

The optimum logo size on an A4 sheet should be 60mm wide.

For consistent application of HM Government identities, wherever possible place them in the top left of communications, with equal spacing above and to the left. This will ensure their prominence while adhering to the 'superior rule' and exclusion zone guidelines.

These placement rules apply to both landscape and portrait format communications.

For documents with a spine, we recommend that you leave an extra 5mm of space to the left of the identity, to ensure that it is clear of the binding.

## Placing and size of the logo

A4



A3





## Who should use the logo?

Everyone working in NOMS headquarters should use the new logo. Headquarters covers all regional and national offices. For example, HR Directorate, Shared Service Centre and East of England Office. If you work for NOMS and not in a prison or for a probation board or trust you should just use the NOMS logo.

If you work in a prison or probation service you should continue to use the existing logo for HM Prison Service and Probation Service. These logos should always appear alongside the NOMS brand. Examples are given overleaf. However, please continue to use your existing stationery and stocks.

Any new initiative which is launched or published should have the NOMS logo and HM Prison Service or Probation Service logos. Private sector prison providers should also display the NOMS logo. Instructions for joint branding are given in this document.





## How should I use the logo?

- Use the logos provided with this presentation
- The logo should be placed on the left hand corner of the publication
- Where co-branding is required the logo should be left justified
- The preferred usage of the logo is the landscape version
- There is also a stacked version for specific applications where the landscape version might not be appropriate
- A logo without the Royal Coat of Arms is also available to use if the logo cannot be displayed top-left as required.

### Logo monotone versions

The NOMS logo should be printed in mono black on all NOMS publications, or by third parties on co-branded publications

### Logo white out versions

The NOMS logo can also be printed white out on NOMS publications, or by third parties on co-branded publications.



National Offender  
Management Service

Private sector providers should also display the NOMS logo as demonstrated here.

## How should I use the logo with existing brands?



National Offender  
Management Service



National Offender  
Management Service

Greater  
Manchester  
Probation Trust





## National Offender Management Service

The logo must always be produced in the correct colour, be positioned at the top and aligned left in relation to any other elements of a design and must always be proportionally scaled. No modification can be made to either the logo or the Royal Coat of Arms, as any deviation will undermine the status of the identity.



National Offender  
Management Service

## Do not

- Alter the proportions of the logo
- distort or stretch the logo
- place the logo at an angle
- reverse out the logo on light colours or use the black logo on a dark background
- place the logo on backgrounds such as busy photographs that don't provide the contrast necessary for readability
- add any additional information, such as a department name
- trim, crop or bleed the logo off the edge of the page.



National Offender  
Management Service



National Offender  
Management Service



National Offender  
Management Service



National Offender  
Management Service

Leadership and Talent Development



National Offender  
Management Service



We recommend the use of two primary typefaces, Arial for PC and Helvetica for Apple Mac, for text and headings in corporate documents. The recommended minimum type size for text is 10pt with 14pt leading.

## Typefaces

# Arial

Arial Regular **Arial Bold**

*Arial Italic* ***Arial Bold Italic***

1234567890!@£\$%^&\*()  
abcdefghijklmnopqrstuvwxyz  
ABCDEFGHIJKLMNOPQRSTUVWXYZ

# Helvetica

Helvetica Roman **Helvetica Bold**

*Helvetica Italic* ***Helvetica Bold Italic***

1234567890!@£\$%^&\*()  
abcdefghijklmnopqrstuvwxyz  
ABCDEFGHIJKLMNOPQRSTUVWXYZ



## National Offender Management Service

The logo should be used on all stationery either alone (a) or with the accompanying brands and contact details positioned to the right (b). Stationery templates are available in Microsoft® Word for NOMS employees. They can be accessed by opening a new word document on your PC and choosing an appropriate template.

## Stationery templates

(a)



National Offender  
Management Service

National Offender Management Service  
Directorate/Regional Office  
Address  
Tel

(b)



National Offender  
Management Service



HM Prison Service  
Directorate name  
Cleland House  
Page Street  
London SW1P 4LN  
Tel 020 7123 4567  
Fax 020 7123 4567  
email:firstname.lastname@hmps.gsi.gov.uk  
www.hmprisonservice.gov.uk



National Offender  
Management Service

## Online use

We recommend that logo should be positioned top left in all circumstances.

The minimum landscape logo size online should be 200 pixels wide.



National Offender  
Management Service

[Sign In](#) | [Register](#) | [Contact us](#) ▼



Example



## Contact

Templates are available in Microsoft Word, Powerpoint and Adobe InDesign.

For further guidance please contact NOMS Communications:



## **SCHEDULE K: TRAINING**

### **SPECIAL CONDITIONS: TRAINING AND APPRENTICESHIPS**

#### **K1. Definitions and Interpretations**

**“Apprentice”** means a worker who is party to an apprenticeship agreement as defined in section 32 of the Apprenticeships, Skills, Children and Learning Act 2009

**“Trainee”** means a worker who is employed by the Contractor under a contract of employment which provides for a scheme to allow the worker to obtain a National Vocational Qualification [or enter here industry-wide recognised qualification] through paid study away from the workplace, and to obtain the competencies listed in the Annex to this schedule by working under the direction of experienced workers.

- K2. The Contractor shall take all reasonable steps to employ Apprentices and/or Trainees, and report to the Authority the numbers of Apprentices and/or Trainees employed and wider skills training provided, during the delivery of this Contract.
- K3. The Contractor shall take all reasonable steps to ensure 5% of the employees, or that a similar specified proportion of hours worked in delivering the Contract, (which may include support staff and sub contractors) are to be delivered by an employee on an Apprentice and/or Trainee programme.
- K4. The Contractor is required to make available to its employees working on the Contract, information about the Government’s Apprenticeship programme available at [www.apprenticeships.org.uk](http://www.apprenticeships.org.uk), and wider skills opportunities provided by local authorities.
- K5. The Contractor shall provide any appropriate further skills training opportunities for employees delivering the Contract.
- K6. The Contractor shall provide a written report detailing the following measures in the contract management reporting and be prepared to discuss Apprentices and/or Trainees at contract management meetings:
- K6.1. The number of people during the reporting period employed on the Contract, including support staff and subcontractors;
- K6.2. The number of Apprentices and/or Trainees and number of new Apprentices and/or Trainees directly initiated through the procurement process;



- K6.3. The percentage of all employees which are Apprentices and/or Trainees;
- K6.4. Explanation from the contractor as to why the Contractor has not achieved the specified percentage target of Apprentices and/or Trainees;
- K6.5. Actions being taken to increase the number of Apprentices and/or Trainees;
- K6.6. Other training and skills development being undertaken by employees in relation to the Contract, including:
- work experience placements for 14 to 16 year olds
  - work experience and work trial placements for other ages.
  - student sandwich and gap year placements
  - graduate placements
  - vocational training
  - skills training
  - on-site training provision and facilities.

## **SCHEDULE L: CONFIDENTIAL CONTRACT INFORMATION EXCEPTIONS**

### **SPECIAL CONDITIONS: CONFIDENTIAL CONTRACT INFORMATION EXCEPTIONS**

**L1.** Pursuant to clause 20.1, the Authority declares that the following categories of contract information are exceptions to the contract information to be published and the information falling within these categories is to be considered Confidential Information:

(a) None

## **SCHEDULE M: EUROPEAN SOCIAL FUND PUBLICITY AND AUDIT REQUIREMENTS**

### **SPECIAL CONDITIONS: PUBLICITY AND AUDIT REQUIREMENTS**

**M1.** Where the Authority identifies duties to be undertaken by the Contractor under this Contract that are supported directly or indirectly by the European Social Fund, the Contractor shall comply with this Schedule in relation to those duties.

**M2.** The Contractor shall comply with Articles 8 and 9 of the European Commission Regulation number 1828/2006 ("the Regulation"). The Contractor shall include equivalent reference to the Ministry of Justice and the National Offender Management Service as that given to the European Social Fund in all materials relevant to compliance with those Articles.

**M3.** The statement to be used in compliance with Article 9 (c) of the Regulation shall be "Investing in jobs and skills".

**M4.** The Contractor shall make financial records and supporting documents to comply with the standards described in Article 15 of the Regulation. The duration for which these records and supporting documents are maintained by the Contractor shall be at least twelve (12) years after the final payment of all sums due under the Contract, or such longer period as may be agreed between the parties.

**M5.** The Contractor shall co-operate with the Authority and other bodies in connection with audits conducted pursuant to Article 16 of the Regulation.

**M6.** The Contractor shall provide sufficient relevant information to the Authority to allow it to comply with Article 7.2 (d) of the Regulation when demanded with reasonable notice.

**M7.** Where the Contractor sub-contracts any duties referred to in paragraph M1 the Contractor shall ensure that it imposes on its sub-contractors equivalent compliance obligations to which it is subject by this Schedule.

**M8.** The Contractor shall give due regard to the "Guidance for providers and sub-contractors for Publicity requirements for NOMS/ESF Funded Projects" issued by NOMS from time to time, and shall make this Guidance available to its subcontractors.

**M9.** The Contractor shall indemnify the Authority and keep the Authority indemnified fully against all claims, proceedings, actions, damages, costs, expenses and any other liabilities which may arise out of, or in consequence of the Contractor's failure to comply with this schedule.

## **SCHEDULE N: EUROPEAN SOCIAL FUND**

### **SPECIAL CONDITIONS: EUROPEAN SOCIAL FUND**

#### **N1. DATA MANAGEMENT**

N1.1. To be permitted to have any type of access to NOMS data, or to use the ARC Gateway and CATS software, it is a condition that all Data Users have completed and signed the appropriate forms. The 2 Appendices attached show the new forms:

Appendix 1: Form A1 NOMS Data Usage Agreement

Appendix 2: Form A2 CATS Security Operational Procedure

N1.2. All Contractor, Sub-contractor (as applicable) or other staff with any type of access to NOMS data must fully complete and sign form A1.

N1.3. Standard CATS users must fully complete and sign forms A1 and A2 and must have completed the training provided by the Authority.

N1.4. All fully completed and individually signed forms are to be retained by the Contractor to enable spot checks to be carried out by the Authority.

N1.5. The Contractor must ensure that forms are reviewed by users on an annual basis, with email acceptance that they have done so.

N1.6. All forms are subject to change from the Authority, throughout the lifetime of the project.

N1.7. The Contractor must indicate acceptance of the terms of the Data Sharing Agreement set out at Appendix 3 to this Schedule N by signing the Agreement where indicated.

N1.8. The Contractor must provide the Authority with a list of Contractor Staff that have been authorised to request new CATS user accounts before any CATS users can be created on the system. This list is attached at Appendix 4. Contractor Staff will be considered to have "Authority to Approve" provided that they:

N1.8.1. are cleared to SC (Security Check) level;

N1.8.2. are listed within Appendix 4 to this Schedule;

N1.8.3. and have completed, signed and returned to the Authority a copy of the Authority to Approve User Form, as available from the Authority and updated from time to time.

N1.9. Contractor Staff with Authority to Approve must submit new CATS user account requests to the NOMS CFO Helpdesk. Once delivery locations are defined, an NUA (New User Application) form will be given to the Contractor to allow new user details to be submitted. The Authority will not accept new CATS user account requests sent by any other means or by Contractor Staff without Authority to Approve.

N1.10. Contractor Staff with Authority to Approve must sign the statements within the NUA form (as available from the Authority and updated from time to time) before a CATS account is created for a user.

N1.11. The Contractor must ensure that there are appropriate mechanisms in place within their organisation to notify the Authority within 5 working days, via the NOMS CFO Helpdesk, of any Contractor Staff with a CATS user account who cease to work on the Services provided by the Contractor under this Contract so that CATS user accounts can be disabled. The Contractor acknowledges that removing CATS user accounts from the system in a timely manner is an important requirement in respect of maintaining the security and performance of the CATS system.

N1.12. The Contractor must provide assurance to the Authority that security vetting checks have been undertaken on all staff where it is required, and ensure that evidence of this for existing staff is available on request to allow the Authority to perform sample checks to assure compliance.

N1.13. In the event of a suspected security breach, the Authority reserves the right to suspend any CATS user accounts in relation to that breach.

## **N2. CATS DOCUMENT UPLOADS**

N2.1. The Contractor shall ensure that all CATS users sign the relevant statement provided by the Authority that certifies any scanned documents uploaded to CATS are a true and accurate copy of the original. The Contractor must actively ensure that Contractor Staff are compliant with this requirement.

## **N3. CATS ACCESS FOR OFFENDERS AND EX-OFFENDERS**

- N3.1. The Contractor acknowledges that the Authority does not permit access to CATS to offenders, regardless of whether or not they are employed by the Contractor in the delivery of Services under this Contract or any other Contract with the Authority, including those relating to the NOMS CFO ESF programme.
- N3.2. The Authority will permit access to CATS for ex-offenders who are employed by the Contractor in the delivery of Services under this Contract subject to the Contractor completing a risk and impact assessment which must be submitted to, and approved by, the Authority. This must take place prior to any new CATS user requests being raised by the Contractor and must take into account whether their personal information is held on the system and how the integrity of the CFO programmes and individuals data will be maintained.

#### **N4. CATS TRAINING**

- N4.1. The Contractor acknowledges that the successful completion of CATS training is mandatory for all users of the system before they will be permitted access to it by the Authority.
- N4.2. Training sessions will be provided by the Authority at set regional locations, using a set timetable of dates with places available on a first come, first served basis.
- N4.3. In the event that training sessions become over-subscribed, extra training sessions will be made available by the Authority where possible.
- N4.4. The Contractor must ensure that Contractor Staff are available for the whole training session. The Contractor acknowledges that any Contractor Staff who are unable to complete the full session will not be allowed access to CATS. The Authority will make details of start and end times for the training session available at the publication of training dates.
- N4.5. In the event that any Contractor Staff are unable to complete the full training session, or that any Contractor Staff fail to attend a booked training session, then the Contractor agrees to reimburse the Authority the cost of the NOMS CFO staff time up to the ESF daily rate, along with any travel and subsistence costs, associated with the training.

- N4.6. The Contractor acknowledges that Contractor Staff need to demonstrate a satisfactory level of competence in using CATS, for their role. If the Authority is not satisfied with the standard of CATS knowledge, the individual(s) will be denied access to the system and will be required to attend further training until a satisfactory level of competence is demonstrated.

**N5. EUROPEAN SOCIAL FUND AND OTHER FUNDING**

- N5.1. The Contractor shall observe the European Commission's and the Managing Authority's publicity requirements and regulations regarding ESF projects, as amended from time to time and available from the Managing Authority. The Contractor shall ensure that sufficient publicity is given to all ESF supported activity so that Participants and the general public are made aware of ESF and what it has achieved.
- N5.2. Upon request by the Authority, the Contractor shall provide a copy of its formal publicity policy clearly setting out the publicity arrangements used by the Contractor and its Subcontractors (if any). Whether or not a copy of the foregoing policy is requested by the Authority, the Contractor shall retain copies of its policy (as revised from time to time) as part of the Contractor's record keeping obligations in accordance with the Administrative Instructions. The Contractor shall be required to adhere to the Publicity Regulations for NOMS/ESF Funded Projects, as amended from time to time, which can be found in Schedule J Management and Monitoring Information Appendix G (Publicity regulations for NOMS/ESF Funded projects).
- N5.3. The Contractor shall within four (4) weeks of expiry or termination of this Contract provide evaluation information to the Authority which:
- N5.3.1. summarises the project, focusing on how it has helped to achieve the project objectives set out in Schedule G Specification; and
  - N5.3.2. is concise, being no more than one A4 page in length; and
  - N5.3.3. indicates whether the objectives have been fully achieved or only partly achieved and sets out any other relevant issues in this context.
- N5.4. The Contractor acknowledges the obligation the Authority has to evaluate all ESF projects by ESF measure and to submit, within strict timescales, a final claim to the Managing Authority including an assessment of performance in

each of the measures. Accordingly, the Contractor agrees that time shall be of the essence in relation to its obligation under Clause N5.3 above.

N5.5. The Contractor understands and shall comply with the regular ESF management information reporting obligations set out in the ESF Regulations as available from the Managing Authority and updated from time to time. The Contractor acknowledges that the Authority depends on timely provision of this information in order to claim and receive ESF funds from the Managing Authority.

N5.6. The Contractor shall indemnify and keep indemnified the Authority in respect of any and all costs, claims and losses howsoever incurred resulting from any breach by the Contractor of this Clause N5. The Contractor's liability under this indemnity is not limited under Clause 34 of the General Terms and Conditions.

N5.7. The Contractor has an obligation to ensure that complies at all times with the ESF Regulations as available from the Managing Authority or otherwise and updated from time to time. The Authority will use the rights and remedies contained within this Contract to address any breach of the ESF Regulations by the Contractor.

## **N6. RETENTION OF RECORDS**

N6.1. The Contractor shall refer to Schedule J Management and Monitoring Information on details relating to the retention of records for this Contract.

## **N7. CONTINGENCY ESF CONTRACT AREAS**

1. North West
2. South East
3. Yorkshire and Humberside
4. West Midlands
5. East Midlands
6. London
7. East of England
8. North East



## **N8. AUDIT**

N8.1. Article (60) of Commission Regulation 1083/2006 requires an audit trail to be established. Article 15 of the Commission Regulation 1828/2006 outlines the criteria which must be met in order that the Authority may satisfy the Commission of an acceptable audit trail.

N8.2. The Contractor shall be subject to a programme of audit visits at which their costs and claims and adherence to contract will be reviewed (these visits shall be applied to both Contractors and sub-contractors as appropriate).

N8.3. The Authority will conduct audits on a number of areas, including but not limited to:

N8.3.1. To ascertain if the Contractor is delivering the Service as contracted for by the Authority within this contract, including but not limited to Schedule H Pricing and Payment, Schedule G Specification and Schedule GB: Contractors Tender including Budget Profile Template and Clarifications, Participant Throughput Profile Template and Financial Profile.

N8.3.2. To ensure DAF claims are claims which are eligible under the DAF rules, including to verify if the claim is relevant to the participant's job aims (further to Schedule H Pricing & Payment).

N8.3.3. To ensure that publicity materials are they compliant with any and all applicable ESF rules and regulations.

N8.3.4. To ensure that ESF plaques prominently displayed and in compliance with any and all applicable ESF rules and regulations.

N8.3.5. Prisoner interviews.

N8.3.6. To ensure the Contractor's management of Subcontractors is in line with Schedule P Market Stewardship Principles.

N8.3.7. To ensure that the relevant requirements in respect of document retention are being met.

N8.3.8. To scrutinise the Contractor's quality management systems and procedures.

N8.3.9. To scrutinise the Contractor's risk management and mitigation policies and processes.

N8.4. If, in the opinion of the Authority, an audit highlights an element of the Contractor's delivery of the Services (whether or not mentioned in N5.3) the Authority will take the steps shown in Schedule R Performance Management

## A1 NOMS - Data Usage Agreement

(Staff with access to data, or to systems holding data related to individuals)

Area of control	All Staff
<b>Personnel Security</b> <b>(Access, Identification and Authentication)</b>	<ul style="list-style-type: none"> <li>Before working with NOMS data / systems you must hold a minimum of Baseline Personnel Security Standard (BPSS) or, if you are responsible for working directly with offenders, you must hold a minimum of Baseline Personnel Security Standard (BPSS) and appropriate DBS check. Should your clearance lapse, or for any reason you are unsure regarding the status of your clearance, you should raise this with your line manager.</li> <li>Failure to comply with this Data Usage Agreement may lead to criminal prosecution or civil redress being taken against the individual who is believed to have contravened this Data Usage Agreement.</li> </ul>
<b>Personnel Security</b> <b>(Training and Awareness)</b>	<ul style="list-style-type: none"> <li>You must re-acknowledge agreement to the latest version of this Data Usage Agreement on an annual basis or following any updates</li> <li>If you have line management responsibilities, you must ensure that all your staff that use NOMS data / systems carry out their responsibilities in support of information security and are aware of, and familiar with, all relevant security policies as per the contract with NOMS</li> </ul>
<b>System Security</b> <b>(Data Handling)</b>	<ul style="list-style-type: none"> <li>Do not allow unauthorised personnel to observe NOMS data / systems.</li> <li>You should only use the NOMS data / systems for the businesses purposes for which it is intended. Data must not be used for any other purpose.</li> <li>You must only access NOMS data / systems from a secure location (as defined by your employer's local policies) using equipment provided by your employer.</li> <li>You must apply NOMS data handling procedures to any information processed, taking careful account of the sensitivity of the information.</li> <li>You must follow a 'clear desk policy' and store hard-copy data in lockable, secure containers, with restricted access, when it is not in use.</li> <li>You must destroy paper documents as soon as they are no longer required in a shredder with cross-shredding functionality.</li> <li>Records in any format that contain personal or sensitive information must not be removed from your office location without prior agreement from your line manager.</li> <li>You must not divulge any information after cessation of employment.</li> </ul>

## Appendix 1 – NOMS Data Usage Agreement

### CATS System Operating Procedures

OFFICIAL

---

<b>Physical &amp; Equipment Security</b>	<ul style="list-style-type: none"><li>Printers utilised for NOMS data / systems must be located within sight of the computers to which they are attached or be operated by secure PIN or similar secure functionality.</li><li>Terminals and workstations must have their screen locked when not in use.</li><li>You must retrieve NOMS data that is printed immediately; information must not be left unattended.</li><li>The shut-down procedures must be followed at the end of the day, or whenever the room is left unattended, to ensure cleaners or other visitors have no access to unauthorised information or assets. If you are the last person in the office you must ensure no classified material is left on display and that the area is left secure before leaving.</li><li>Cleaners and visitors must be supervised according to local policies, including where systems are in use or participant data is not secured</li></ul>
<b>Communications (Sending / Receiving)</b>	<ul style="list-style-type: none"><li>If you send personal or sensitive information to NOMS or another recipient, the data is your responsibility until the receiver verifies that the data has been received and has not been compromised (opened or tampered with). It is your responsibility to ensure that the recipient address is correct before sending information.</li><li>Appropriate tracking should be used for sending information between locations such as utilising a courier service or Royal Mail Recorded / Special Delivery – though it should be remembered that the Recorded Delivery tracking service provides limited information.</li></ul>
<b>Email Communications</b>	<ul style="list-style-type: none"><li>NOMS data must only be sent to authorised recipients. It is your responsibility to ensure the recipient email address is correct.</li><li>Personal or sensitive information transferred by email, must be done so securely (e.g. utilising <a href="http://www.cjsm.net">www.cjsm.net</a> or the GSi network)</li></ul>
<b>Security Incident Reporting</b>	<ul style="list-style-type: none"><li>You must be aware of and comply with the Incident Management procedure (Page 3 of this document set)</li><li>You must report any incident involving a suspected or known security breach involving personnel, hardware, software, communications, document or physical security as per the procedure outlined in “Incident Management Procedure” (Page 3 of this document set) within one hour of discovering the loss or compromise.</li><li>You must report any suspected malicious code or viruses present on systems utilised to process NOMS data to your local data protection officer and NOMS CFO Helpdesk [REDACTED] If you suspect a virus is present on your terminal, either:<ul style="list-style-type: none"><li>[1] Turn the computer off and place a label on the terminal stating that the machine has a virus infection and must not be used; or,</li><li>[2] If operationally possible, leave the system switched on in its infected condition and mark the system and any associate storage media with a label stating that the machine has a suspected virus.</li></ul></li></ul>

## Incident Management Procedure

Personal data relates to any information which identifies an identifiable living individual, including any expression of opinion about that person or expression of intentions towards them. Personal data compromise can occur through theft, loss or deliberate or unintentional damage or destruction.

The list below is not exhaustive but examples include:

- Loss of a participant files / paperwork, or one turning up where it should not be;
- Information missing in the post or from a fax transmission;
- Theft of a computer or memory stick containing personal data (Note: no data relating to participants should be held on or used with unapproved devices);
- Loss of a mobile phone containing personal data;
- Deliberate or accidental disclosure of personal data;
- Leaving a computer disk or laptop containing personal information on a train or in any non-secure environment.

How “significant” a compromise is will depend on a number of factors and on the individual circumstances of a case. In all cases of data loss or compromise in relation to the delivery of the NOMS CFO contract, you must:

- Immediately inform your local data protection officer and the NOMS CFO Helpdesk [REDACTED] within one hour of discovering the loss or compromise. Do not send an email and assume it has been received, make a call and confirm that notification has been given.

Within the first day of becoming aware of the loss or compromise you must investigate the cause, effect and extent of the breach utilising the incident reporting form that will be issued to you by the CFO Helpdesk. While some assessment of the significance of the loss will only be apparent after this investigation, it is important that all losses or potential losses are reported immediately (within one hour), without waiting for the results of investigations or risk assessments.

The investigation should cover the following points:

- Numbers of individuals affected;
- Type of data compromised (e.g. personal data, sensitive corporate data, non-sensitive data);
- Circumstances of the incident (including physical environment, time of day);
- Whether the incident concerns or affects other organisations;
- Full assessment of the possible risks arising, covering risks to data subjects, the public, Ministry of Justice or government operations and reputation;

You are advised to keep notes, especially if the incident is complex or developments are moving fast and details need to be captured.

Report the results of the investigation to NOMS CFO, without delay.

Use all reasonable efforts to rectify the cause of such breach.

Data loss is a sensitive issue and a local incident may be of national media interest. All communication concerning the incident outside NOMS such as public or media must be cleared through NOMS CFO who will liaise with the MoJ Press Office.

### CATS System Operating Procedures

OFFICIAL

---

Next steps will include recommendations on whether and how to inform data subjects (those whose data has been lost / compromised) or other parties. These should be based on an objective and accurate assessment of the statutory duties, the potential risks and the benefits of disclosure. The decision concerning whether to inform the Information Commissioner's Office and the Police needs to be made in liaison with the MoJ Information. For example if the incident involves risk information or where the loss involves possible theft of data from premises or systems.

## Appendix 1 – NOMS Data Usage Agreement

### CATS System Operating Procedures

OFFICIAL

---

Your local data protection officers are:

Organisation	Name and Role	Contact Details
*** Provider To Complete ***	*** Provider To Complete ***	*** Provider To Complete ***
*** Provider To Complete ***	*** Provider To Complete ***	*** Provider To Complete ***
*** Provider To Complete ***	*** Provider To Complete ***	*** Provider To Complete ***

By signing below I acknowledge that I have read the NOMS Data Usage Agreement (DUA) policy and Incident Management Procedure for CFO funded programmes and NOMS provided IT systems and agree to be bound by them. I also agree to comply with any organisational and local policies that are not covered, but do not conflict with the above agreement.

Name: \_\_\_\_\_

Date: \_\_\_\_\_

Signature: \_\_\_\_\_



## Appendix 2 – CATS System Operational Procedure

### CATS System Operating Procedures

OFFICIAL

## A2 CATS – Security Operating Procedures (All CATS Users)

Area of control	All Staff
<b>Personnel Security</b> (Access, Identification and authentication)	<ul style="list-style-type: none"><li>• Before working with CATS data you must hold a minimum of Baseline Personnel Security Standard (BPSS) or, if you are responsible for working directly with offenders, you must hold a minimum of Baseline Personnel Security Standard (BPSS) and appropriate DBS check. Should your clearance lapse, or for any reason you are unsure regarding the status your clearance, you should raise this with your line manager.</li><li>• You will only be given an account to access CATS once you have completed the latest New User Agreement (NUA) form and this has been approved and you have completed the required training.</li><li>• Do not allow unauthorised personnel access to the CATS system or information.</li><li>• Do not share your system access credentials with other personnel.</li><li>• Do not allow unauthorised users to observe your screen.</li><li>• Do not allow any person to observe you entering your system credentials. Failure to comply with these Security Operating Procedures may lead to criminal prosecution or civil redress being taken against the individual who is believed to have contravened these Security Operating Procedures.</li></ul>
<b>Personnel Security</b> (System Use)	<ul style="list-style-type: none"><li>• Do not exceed, or attempt to exceed your given access privileges.</li><li>• Personal or sensitive data should not be downloaded from CATS to any un-secure (non-government accredited) system.</li><li>• Personal or sensitive data should not be transferred to an un-secure USB memory stick or any other removable device (e.g. CD).</li><li>• You must not make or attempt to make any change to the configuration of the system.</li></ul>
<b>Personnel Security</b> (Passwords)	<p>The following password policy applies to the CATS system:</p> <ul style="list-style-type: none"><li>• Passwords must be at least 8 characters and consist of a mixture of upper and lower-case letters, numbers and symbols.</li><li>• Passwords must be changed at least every 90 days or after auditing, and they cannot be re-used.</li><li>• You must not use the same password as for other systems. Passwords must be difficult to guess.</li><li>• Passwords should not be written down.</li><li>• CATS, and the ARC Gateway used to access CATS, must be accessed using different passwords.</li></ul>
<b>Personnel Security</b> (Training and Awareness)	<ul style="list-style-type: none"><li>• You must re-acknowledge agreement to the latest version of these Security Operating Procedures on an annual basis or following any updates.</li><li>• If you have line management responsibilities, you must ensure that all your staff that use CATS carry out their responsibilities in support of information security and are aware of, and familiar with, all relevant security policies.</li></ul>
<b>System Security</b>	<ul style="list-style-type: none"><li>• You must apply NOMS data handling procedures to information processed by the CATS system, taking careful account of the sensitivity of the</li></ul>

## Appendix 2 – CATS System Operational Procedure

### CATS System Operating Procedures

OFFICIAL

Area of control	All Staff
(Data Handling)	<p>information.</p> <ul style="list-style-type: none"><li>• Data should only be printed when there is a business need, and should be labelled and handled with their appropriate Security Classification.</li><li>• You must follow a 'clear desk policy' and store hard-copy information in lockable, secure containers, with restricted access, when it is not in use.</li><li>• You must destroy paper documents as soon as they are no longer required in a shredder with cross-shredding functionality.</li><li>• Records in any format that contain personal or sensitive information must not be removed from your office location without prior agreement from NOMS.</li></ul>
System Logging	<ul style="list-style-type: none"><li>• The system records: login attempts; data views; data deletions; data amendments; reports run for management, audit, security and data integrity purposes.</li></ul>
Physical & Equipment Security	<ul style="list-style-type: none"><li>• Your user terminal for accessing CATS must be located in a provider approved, secure area – if you are unsure, speak to your line manager.</li><li>• Check the user machine on a daily basis for evidence of tampering or suspicious devices attached to it. Report suspicious activity to your line manager.</li><li>• Screens must be angled or positioned so that information displayed cannot be viewed through windows or open doorways. Semi-opaque films or blinds should be used if the physical location can not be adjusted to protect screens.</li><li>• Printers connected to CATS must be switched off after each use, or upon office closure if shared, to ensure the internal memory of the printer is wiped.</li><li>• You should invoke the screensaver on the terminal used to access CATS (press 'windows' key + L) when left unattended.</li></ul>

By signing below I acknowledge that I have read the CATS Security Operating Procedures (SyOPs) and the preceding document sets (A1) and agree to be bound by them. I will also agree to comply with any organisational and local policies that are not covered, but do not conflict with the above agreement.

Name: \_\_\_\_\_

Date: \_\_\_\_\_

Signature: \_\_\_\_\_



Ministry of  
**JUSTICE**

## Data Sharing Agreement



National Offender  
Management Service

THIS AGREEMENT is made the 1<sup>st</sup> day of April 2015

BETWEEN

THE SECRETARY OF STATE FOR JUSTICE of 102 Petty France, London SW1H 9AJ (“MoJ”) (“the Authority”)

AND

The Shaw Trust Ltd, 4th Floor, Jessica House, Red Lion Square, SW18 4LS (“the Data Recipient”)

## Appendix 3 – Data Sharing Agreement

### 0. Background:

- (A) This Agreement articulates ;

The sharing of data between the National Offender Management Service (NOMS) Co-Financing Organisation (CFO), and The Shaw Trust Ltd.

- (B) For the purposes of this Agreement the Authority will be a Data Controller and the Data Recipient will be a Data Controller;
- (C) The Authority and the Data Recipient will both be responsible for compliance with the Data Protection Principles under the Data Protection Act 1998 in relation to the Shared Information and this Agreement exists to provide a framework for that compliance.

IT IS NOW AGREED as follows:

### 1. Definitions and interpretation

- 1.1 In this Agreement the following words and phrases shall have the following meanings, unless expressly stated to the contrary:
- a. **“Act”** means the Data Protection Act 1998, as amended;
  - b. **“Data Controller”** has the meaning in section 1(1) of the Act;
  - c. **“Data Processor”** has the meaning in section 1(1) of the Act;
  - d. **“Data Protection Legislation”** means the Data Protection Act 1998, the EU Data Protection Directive 95/46/EC, the Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699), the Electronic Communications Data Protection Directive 2002/58/EC, the Privacy and Electronic Communications (EC Directive) Regulations 2003 and all applicable laws and regulations relating to Processing of personal data and privacy, including where applicable the guidance and codes of practice issued by the Information Commissioner;
  - e. **“Data Subject”** has the meaning in section 1(1) of the Act;
  - f. **“Data Recipient”** has the meaning of the organisation/person receiving the data in this Agreement;
  - g. **“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;
  - h. **“FOIA”** means the Freedom of Information Act 2000, as amended;
  - i. **“NOMS CFO Contract”** means NOMS Co-Financing Organisation (CFO) provision for the European Social Fund (ESF) 2014-2020 Operational Programme
  - j. **“Parties”** means the parties to this Agreement, namely the Authority and the Data Recipient;
  - k. **“Participants”** are offenders eligible for ESF provision and delivery under the associated NOMS CFO Contract
  - l. **“Personal Data”** has the meaning in section 1(1) of the Act;
  - m. **“Project”** means the steps described in Clause 6 of this Agreement comprising ;  
Delivery of the NOMS CFO Contract that has been awarded to the Data Recipient, by NOMS CFO.
  - n. **“Processing”** has the meaning in section 1(1) of the Act;
  - o. **“Request for Information”** means a request for information or an apparent request under FOIA or the Environmental Information Regulations;

## Appendix 3 – Data Sharing Agreement

- p. **“Responsible Information Asset Owner”** means an individual occupying the position of Information Asset Owner within the Authority, who has asset ownership obligations in relation to the Shared Information;
- q. **“Shared Information”** means the information to be shared as set out in Clause 5 of this Agreement.

### 1.2 In this Agreement:

- a. the masculine includes the feminine and neuter;
- b. person means a natural person;
- c. the singular includes the plural and vice versa;
- d. 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.

### 1.3 Headings are included in this Agreement for ease of reference only and shall not affect the interpretation or construction of this Agreement.

### 1.4 References in this Agreement to Clauses, Paragraphs and Annexes are, unless otherwise provided, references to the Clauses, Paragraphs and Annexes of this Agreement.

### 1.5 In the event and to the extent only of any conflict or inconsistency between:

- a. the provisions of the Clauses and the provisions of the Annexes, the provisions of the Clauses shall prevail; or
- b. the provisions of this Agreement and the provisions of any document referred to or referenced herein, the provisions of this Agreement shall prevail.

## 2. Introduction and aims

### 2.1 The sharing of data allows for information owned by NOMS, such as data held on the Case Assessment and Tracking System (CATS) to be utilised by the Data Recipient to fulfil the requirements of delivering the NOMS CFO funded ESF programme, and for no other purpose.

### 2.2 The sharing of data allows the Data Recipient to utilise CATS, which allows for:

- Compliance with the contractual requirement of recording all information for a participant, that relates to the NOMS CFO Contract delivery on CATS.
- Easier sourcing of participants who may be eligible to enrol on the programme.
- Better compliance with ESF Audit requirements
- Uploading and storage of scanned information (including evidence) relating to participants.

### 2.3 If there is no signed data sharing agreement in place, delivery of the NOMS CFO Contract by the Data Recipient will not be possible

### 2.4 The steps comprising the data share are set out in Clause 6. This Agreement does not relate to any data sharing between the Parties not forming part of the Project/data share.

## 3. Commencement and term

### 3.1 This Agreement shall commence upon signature by the Parties and shall continue in effect until the data share has been completed in accordance with the requirements of this Agreement unless otherwise subject to earlier termination in accordance with Clause 25.

## Appendix 3 – Data Sharing Agreement

### 4. Representatives

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

Name: [REDACTED]

Title: [REDACTED]

Address: NOMS CFO, 1<sup>st</sup> Floor, Unit 1100 Daresbury Park, Warrington, WA4 4HS

Tel. [REDACTED]

Fax. [REDACTED]

E-mail: [REDACTED]

For the Data Recipient:

Name: [REDACTED]

Title: [REDACTED]

Address: Shaw House, Epsom Square, Trowbridge, Wiltshire BA14 0XJ

Tel. Mobile: [REDACTED]

Fax. N/A

E-mail: [REDACTED]

- 4.2 The Parties agree that these nominated representatives will correspond at regular intervals throughout the Project/data share to discuss activity in general and will provide updates to each other on matters of mutual interest.
- 4.3 The persons who will be supervising the Processing of the Shared Information are Director of Justice, Deputy Operations Director of External Delivery, Performance Director, Head of Partnership Management.
- 4.4 The persons who will be Processing the Shared Information are Director of Justice, Deputy Operations Director of External Delivery, Performance Director, Head of Partnership Management.
- 4.5 The persons who will have access to the Shared Information are Director of Justice, Deputy Operations Director of External Delivery, Performance Director, Head of Partnership Management.

### 5. Shared Information

- 5.1 The information to be shared under the Project/data share consists of the following:  
Information held on CATS that is relevant to the Data Recipient (i.e. is due to be on their caseload, has been on the caseload, or is within the remit of being on their caseload)  
All information held by the Data Recipient and controlled by them relating to participants being worked with on the programme, or have been identified as potentially eligible. Individual signed consent will need to have been obtained for this prior to any information being entered on CATS.
- 5.2 The Government Security Classification (GSC) for the data being shared is OFFICIAL.
- 5.3 Parties carrying out the functions outlined in this Agreement should make themselves aware of, and adhere to, their organisation's information security policies and procedures in regards to handling data in a manner appropriate for the assigned GPM.

## Appendix 3 – Data Sharing Agreement

- 5.4 Where practitioners are unable to comply with their organisations policies regarding the safe and secure transfer of information they must ensure that a risk assessment is undertaken by their Information Security/Governance department at the earliest opportunity. Alternative secure methods, as identified within the organisation's policy, must be used until such time as the risk assessment has been undertaken.
- 5.5 A generic list of agreed methods for the safe and secure transfer of personal information is documented within Annex 1. Only data classified as Official should be processed for the NOMS CFO Contract.

### 6. The project/data share

- 6.1 The data share will consist of the following steps of which the Parties are both in agreement and acknowledge their respective obligations:

NOMS CFO will supply through CATS, a list of offenders that are potentially eligible to enrol on the project where available.

NOMS CFO will supply, where available and appropriate, associated data relating to offenders that will assist with the delivery of the NOMS CFO Contract, such as date of birth, gender, location and ethnicity. Local agreements may be required with Prisons, Probation Trusts and Community Rehabilitation Companies to access any data they own or process.

As a minimum the following information, where known, will be made available by NOMS through the Case Assessment and Tracking System.

- Location
- Identifiers (Prison No, CRO Number)
- Gender
- Surname
- Forename(s)
- Date of Birth
- Nationality
- Ethnic Group
- Sentence Information (i.e. Main Offence, Sentence Length)
- Release Information
- Address Information

All data input into CATS is the sole property of NOMS CFO and should not be utilised by anyone else. Dependant on transfers from region to region, data available within CATS may have been updated by other Data Recipients but should be maintained and handled in the same way.

This data shall only be used by the Data Recipient for the purpose of delivering the NOMS CFO Contract awarded. Working with the participant, deciding the course of action to take with them, identifying their needs and requirements and working with them in a safe and secure manner. All relevant data associated with the offender will be input on CATS.

Should any consent be withdrawn, the NOMS CFO Helpdesk should be informed immediately by telephone: 01925 423 423 or by email: [cfo-helpdesk@noms.gsi.gov.uk](mailto:cfo-helpdesk@noms.gsi.gov.uk)

### 7. Legal basis

- 7.1 The Shared Information is provided for the following purposes:

- To allow the Data Recipient to identify potentially eligible offenders.

## Appendix 3 – Data Sharing Agreement

- To allow for synchronisation of this data, keeping it relevant and up to date; in-line with the Data Protection Act 1998
- To access and maintain data that has been input by other data recipients on behalf of NOMS, where the case has transferred to the data recipient
- To accurately deliver and underpin the programmes requirement which will influence the development of policies relating to the management of offenders.

The data share will allow the Data Recipient to receive core information relating to offenders that would normally have to be manually obtained through access to the P-NOMIS and N-Delius systems.

The legal basis for sharing this information is the Offender Management Act 2007, section 14.

- 7.2 The processing of personal and sensitive personal information is primarily governed by the Data Protection Act 1998 which establishes a legal framework of rights and obligations to protect personal information concerning living individuals only. The first data protection principle contained in Schedule 1 to the Act requires data processing (which includes data sharing) to be fair and lawful and, in particular, requires one of the conditions in Schedule 2 to be satisfied and, in the case of sensitive personal data, one of the conditions in Schedule 3.

The lawful basis for this share is identified above. The share is considered to be fair because for the purpose of this Agreement, reliance is placed upon (where required) explicit consent for both Schedules (where required). For the purpose of this Agreement, reliance is placed upon:

Schedule 2, paragraph 5(c) and Schedule 3, paragraph 7(1)(c) of the Data Protection Act 1998 which sets out that data can be shared if it is necessary for the exercise of any functions of the crown, a minister of the crown or a government department.

Schedule 2, paragraph 6 of the Data Protection Act 1998 which sets out that 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.

Government Departments must comply with the Human Rights Act 1998 which, among other things, protects a person's right to respect his private and family life, his home and his correspondence. Any interference with this right is considered to be justifiable because the sharing is lawful, necessary and proportionate.

**Article 8** of the Act 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 must be justified 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

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



## Appendix 3 – Data Sharing Agreement

- 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

7.3 The Data Recipient guarantees that the Shared Information is proportionate to the purpose(s).

### 8. Further use of Shared Information

- 8.1 The Data Recipient agrees not to Process the Shared Information for purposes that are incompatible with the purposes in Clause 2.1.
- 8.2 The Data Recipient agrees not to Process the Shared Information, except as necessary for the performance of the Project/data share and to achieve the purposes in Clause 2.1, unless expressly authorised in writing by the Authority.

### 9. Information security

The Data Recipient, when carrying out the functions outlined in this Agreement, should make themselves aware of, adhere to and implement the following information security policies, procedures and guidance:

- PSI 25/2014 IT security policy
- PSI 12/2014 Government Secure Classification (GSC) policy
- PSI 24/2014 Information assurance policy The GOV.UK End User Devices Security and Configuration Guidance, currently located here: <https://www.gov.uk/government/collections/end-user-devices-security-guidance>
- The CIS (Center for Internet Security) Benchmarks, currently located here: <http://benchmarks.cisecurity.org/downloads/browse/?category=benchmarks>

Where the Data Recipient is unable to comply with the policies regarding the safe and secure transfer of information they must ensure that a risk assessment is undertaken by their Information Security/Governance department at the earliest opportunity and reported to the authority representative outlined in section 4. Alternative secure methods, as identified within the policies, must be used until such time as the risk assessment has been undertaken.

The chosen method of disclosure for this share is through the Case Assessment and Tracking System (application). NOMS will take responsibility for the Case Assessment and Tracking System, however providers should ensure the equipment they use to connect to the system, the associated personnel that use the system and anything associated with the use of the system, for example - passwords, all comply with the security policies and procedures.

No removable media is authorised for use by the Data Recipient in relation to any offender data.

## Appendix 3 – Data Sharing Agreement

### 10. Records management

The Data Recipient, while carrying out the functions outlined in this Agreement should make themselves aware of the following records management procedures, specifically in relation to collecting, processing and disclosing of personal information:

- PSO 9025 - Archiving and Retention policy
- PSO 9020 - Data Protection Act 1998 and Freedom of Information Act

All information, whether held on paper or in electronic format must be stored and disposed of in line with the agreed retention and disposal arrangements as documented within the NOMS CFO Contract.

Personal information will only be collected using the agreed collection methods, ensuring the required information is complete and up-to-date.

Decisions about service users should never be made by referring to inaccurate, incomplete or out of date information.

If information is found to be inaccurate, the Data Recipient will ensure that their records and systems are corrected accordingly. Consideration must also be given to advising the Authority where practical.

### 11. Integrity of Shared Information

- 11.1 The Data Recipient shall not delete or remove any proprietary notices contained within or relating to the Shared Information.
- 11.2 The Data Recipient shall take responsibility for preserving the integrity of the Shared Information and preventing the corruption or loss of the Shared Information.

### 12. Not Subject to Freedom of information

If the Data Recipient is **not** subject to the Freedom of Information act the following will be adhered to:

- 12.1 The Data Recipient acknowledges that the Authority is subject to the requirements of FOIA and the Environmental Information Regulations and shall assist and co-operate with the Authority to enable the Authority to comply with its information disclosure obligations.
  - 12.2 The Data Recipient agrees to:
    - a. transfer to the Authority all Requests for Information that it receives as soon as practicable and in any event within two Working Days of receiving a Request for Information;
    - b. provide the Authority with a copy of all information in its possession, or power in the form that the Authority requires within five Working Days (or such other period as the Authority may specify) of the Authority's request; and
    - c. provide all necessary assistance as reasonably requested by the Authority to enable the Authority to respond to the Request for Information within the time for compliance set out in section 10 of the FOIA or regulation 5 of the Environmental Information Regulations.
  - 12.3 The Authority shall be responsible for determining in its absolute discretion and notwithstanding any other provision in this Agreement or any other agreement whether any information is exempt from disclosure in accordance with the provisions of FOIA or the Environmental Information Regulations.
  - 12.4 In no event shall the Data Recipient respond directly to a Request for Information unless expressly authorised to do so by the Authority.
  - 12.5 The Data Recipient acknowledges that (notwithstanding the provisions of this Clause) the Authority may, acting in accordance with the Ministry of Justice's Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the Freedom of Information Act 2000 ("the Code"), be
- Data sharing agreement (01.11)

## **Appendix 3 – Data Sharing Agreement**

obliged under FOIA or the Environmental Information Regulations to disclose information concerning the Data Recipient or the Project:

- a. in certain circumstances without consulting the Data Recipient; or
- b. following consultation with the Data Recipient and having taken their views into account;

provided always that where paragraph (a) applies the Authority shall, in accordance with any recommendations of the Code, take reasonable steps, where appropriate, to give the Data Recipient advanced notice, or failing that, to draw the disclosure to the Data Recipient's attention after any such disclosure.

- 12.6 The Data Recipient shall ensure that all information is retained for disclosure in accordance with Section 10 and shall permit the Authority to inspect such records as requested from time to time.

### **13. Subject to Freedom of Information**

If the Data Recipient is subject to the Freedom of Information and the Environmental Information Regulations act the following will be adhered to:

- 13.1 The Parties are both 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 Agreement, 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.

### **14. Statutory compliance**

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

### **15. Ability to access Shared Information**

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

### **16. Products and publications**

- 16.1 The Shared Information may allow for persons to be identified. The Data Recipient, therefore, agrees that no outputs will be produced that are likely to identify a person, unless specifically agreed with the Authority.

### **17. Disclosure protection**

- 17.1 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 Data 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.

## **Appendix 3 – Data Sharing Agreement**

- b. Tabular outputs should not report analyses at detailed levels of geography. The Data Recipient will clear with the Authority, 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 Data 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 Data Recipient will take particular care not to report extreme outliers.

### **18. Matching or linking of Shared Information**

- 18.1 The Shared Information will not be matched or linked with any other data or information sources other than as agreed in the description of the Project in Clause 6 or with the written agreement of the Authority.

### **19. Duplication and copies**

- 19.1 The Data 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 6 or with the written agreement of the Authority.

### **20. Duration of the Project/data share**

- 20.1 The Shared Information will be provided for the period of the NOMS CFO Contract.
- 20.2 The maximum duration of the data share will not exceed 5 years and a new data share will be initiated from the 1st January 2018 until completion of delivery of the NOMS CFO Programme.
- 20.3 Requests for extension to the period of the Project must be referred to the Authority for approval prior to the expiry date.

### **21. Review**

- 21.1 A review of the data share is to be conducted by the Authority and data recipient at least annually.
- 21.2 The Authority and the data recipient will assess risks to the confidentiality, integrity and availability of information in this data share quarterly taking account of extant Government wide guidance, and plan and implement proportionate responses. For the Authority this will be done as part of the quarterly Information Asset Register review.

### **22. Actions at end of the data share**

- 22.1 Upon agreed notification from NOMS, the Data Recipient agrees to destroy all copies of the Shared Information, including temporary copies, CDs, printed copies, personal copies, derived datasets and all electronic copies in a controlled way, 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 data through secure destruction, overwriting, erasure or degaussing for reuse.
- 22.2 The Data Recipient will ensure that the Shared Information is destroyed to the standards that meet government standards for secure and complete destruction.

## Appendix 3 – Data Sharing Agreement

- 22.3 After the Shared Information has been destroyed, the Data 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. The declaration will be returned to the Authority.

### 23. Loss and unauthorised release

- 23.1 The Data Recipient will report to the Authority any loss or unauthorised release of the Shared Information, as soon as possible, or no later than 24 hours after the loss or unauthorised release.
- 23.2 The Data Recipient acknowledges that any loss or unauthorised release of the Shared Information can be treated as valid grounds for terminating this Agreement by the Authority.
- 23.3 Any loss or unauthorised release of the Shared Information by the Data Recipient will allow the Authority to request that a full investigation into the cause of the loss or unauthorised release be undertaken; or allows the Authority to undertake such an investigation itself.
- 23.4 The Data Recipient fully indemnifies the Authority for all financial liability that may arise from loss or unauthorised release of the Shared Information by the Data Recipient.

### 25. Termination

- 25.1 Either Party may terminate this Agreement upon one month's written notice to the other.
- 25.2 Either Party may terminate this Agreement with immediate effect in the event of breach of its obligations by the other Party to this Agreement.
- 25.3 Any disputes arising concerning this Agreement will be resolved initially by discussions between the Authority and the Data Recipient. If that fails, the dispute is to be referred in accordance with the contract

AS WITNESS of which the parties have set their hands on the day and year first above written

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

By:

.....

Name: .....

Title: .....

SIGNED for and on behalf of  
THE DATA RECIPIENT

By:

.....

Name: .....

Title: .....

## Annex 1: Specific security requirements

Please refer to Clause 9.

Security handling guidance for OFFICIAL classification level

	<b>OFFICIAL</b>
<b>DESCRIPTION of the classification</b>	<p>All information that is created, processed, generated, stored or shared within (or on behalf of) BIS is, at a minimum, <b>OFFICIAL</b>.</p> <p><b>OFFICIAL – SENSITIVE</b> information is of a particularly sensitive nature. The “SENSITIVE” caveat should be used in limited circumstances (depending on the subject area, context and in some cases, any statutory or regulatory requirements) where there is a clear and justifiable requirement to reinforce the ‘need to know’.</p> <p>Staff need to make their own judgements about the value and sensitivity of the information that they manage, in line with BIS and HMG corporate risk appetite decisions.</p>
We protect this information from:	Hacktivists, single-issue pressure groups, private investigators, competent individual hackers and the majority of criminal individuals and groups.
Why do we protect this information?	<ul style="list-style-type: none"><li>▪ To meet legal and regulatory requirements.</li><li>▪ Promote responsible sharing and discretion.</li><li>▪ Implement proportionate controls appropriate to an asset’s sensitivity.</li><li>▪ Make accidental compromise or damage unlikely.</li></ul>

	<b>OFFICIAL</b>
<b>IMPACT</b>  The compromise or loss would be likely to:	<ul style="list-style-type: none"> <li>▪ Have damaging consequences for an individual (or group of individuals), or NOMS if lost, stolen or published in the media.</li> <li>▪ Cause significant or substantial distress to individuals or a group of people.</li> <li>▪ Break undertakings to maintain the confidence of information provided by third parties.</li> <li>▪ Breach statutory restrictions on the disclosure of information.</li> <li>▪ Undermine the proper management of the public sector and its operations.</li> <li>▪ Shut down or substantially disrupt national operations.</li> <li>▪ Seriously impede the development or operation of government policies.</li> <li>▪ Substantially undermine the financial viability of major organisations.</li> <li>▪ Impede the investigation or facilitate the commission of serious crime.</li> </ul>
Examples	<b>OFFICIAL information</b> <ul style="list-style-type: none"> <li>▪ <b>All routine, day-to-day public sector business</b>, including policy development, service delivery, legal advice, personal data, staff reports, contracts, statistics, case files, and administrative data.</li> <li>▪ Commercial information, including contractual information and intellectual property.</li> <li>▪ Personal information that is required to be protected under the Data Protection Act.</li> <li>▪ Procurement tenders, contracts and correspondence.</li> <li>▪ Offender Case details involving individuals (except for cases where there is a real risk of harm or serious criminal activity may result from disclosure).</li> <li>▪ Company information provided in confidence.</li> <li>▪ Policy or operational minutes and papers.</li> <li>▪ Honours nominations and deliberations.</li> <li>▪ Threat assessments (and countermeasures) relating to the above level threats.</li> </ul>

	<b>OFFICIAL</b>
	<p><b>OFFICIAL – SENSITIVE information</b></p> <ul style="list-style-type: none"> <li>▪ The most sensitive corporate or operational information, e.g. relating to organisational change planning, contentious negotiations, or major security or business continuity issues.</li> <li>▪ Policy development and advice to ministers on contentious and very sensitive issues.</li> <li>▪ Commercial or market sensitive information, including that subject to statutory or regulatory obligations, that may be damaging to HMG or to a commercial partner if improperly accessed.</li> <li>▪ Information about staff corruption investigations or other high profile or sensitive staff investigations.</li> <li>▪ Highly sensitive personal data, such as information about high profile offenders, VISOR data, extremism, and information relating to intelligence sources where it is not considered necessary to manage this information in the SECRET category.</li> </ul>
<p><b>MARKING</b> (of all material, whether paper, electronic, digital media)</p>	<p>There is <b>no requirement to mark</b> routine OFFICIAL information.</p> <p>In limited circumstances where there is a clear and justifiable ‘need to know’ requirement, the “SENSITIVE” caveat should be used. <b>OFFICIAL – SENSITIVE INFORMATION MUST ALWAYS BE CLEARLY MARKED.</b></p> <p>Mark “OFFICIAL – SENSITIVE” in capital letters at the top and bottom of each document page, and in the Subject line and body of all emails. This could be followed by any handling or access requirements.</p> <p><b>NOTE:</b></p> <p>The originator is responsible for determining the appropriate classification for any assets they create. Depending on context and circumstances sensitivities may change over time and it may become appropriate to reclassify an asset. Only the originator can reclassify the asset.</p>



	<b>OFFICIAL</b>
Marking handling instructions	All handling instructions or requirements as stipulated by the Information Asset Owner should be marked at the top and bottom of each document page, and at the beginning of any email message text.
<b>HANDLING OF INFORMATION YOU CREATE</b>  (of all material, whether paper, electronic, digital media)	<p><b>Handling instructions</b> are there to identify why special handling is required; who is to be allowed access to the information; how that information or data is allowed (or not) to be circulated or forwarded on and how it is to be stored.</p> <p>You control how the information you create is to be handled: you can describe any particular sensitivities of the information and offer meaningful handling advice. Additional handling instructions should be included following advice from the Information Asset Owner to identify handling requirements.</p> <p>Handling instructions should be included:</p> <ul style="list-style-type: none"> <li>▪ On the front page of any document, and at the top of each page.</li> <li>▪ As the first paragraph of any letter or minute.</li> <li>▪ As the first paragraph of any email.</li> <li>▪ Highlighted in the operations instructions for any dataset.</li> </ul> <p><b>Basic formula for handling instructions:</b></p> <p>&lt;Reason this is classified as it is&gt;          &lt;What you are allowed to do with this information&gt;          &lt;What you need to do to ensure it is kept secure&gt;</p>

	<b>OFFICIAL</b>
	<p><b>Example handling instructions:</b></p> <ul style="list-style-type: none"> <li>• “Please do not distribute this document further.”</li> <li>• “Draft submission that seeks final Ministerial clearance for <i>[insert]</i>. This is for your eyes only – it remains highly contentious and should not be copied any further.”</li> <li>• "This information has been produced by NOMS. Do not share outside of NOMS without the written approval of the sender."</li> <li>• “To be opened by Addressee Only” – can be used for sending personal information for staff</li> </ul>
<p><b>HANDLING OF INFORMATION</b></p> <p>(of all material, whether paper, electronic, digital media)</p>	<p><b>You must follow any handling guidance stipulated by the Information Asset Owner.</b></p> <p>You have a duty of confidentiality and a personal responsibility to safeguard any NOMS or MoJ information that you are entrusted with, or are handing to others.</p> <p><b>OFFICIAL:</b></p> <ul style="list-style-type: none"> <li>▪ Lock computers when away from your desk.</li> <li>▪ Adhere to the NOMS clear desk policy.</li> </ul> <p><b>OFFICIAL – SENSITIVE:</b> <i>as OFFICIAL plus</i></p> <ul style="list-style-type: none"> <li>▪ Ensure documents are seen by, or passed to individuals only on a ‘need to know’ basis.</li> </ul>

	<b>OFFICIAL</b>
	<p><b>NOTES ON LEGACY INFORMATION:</b></p> <ul style="list-style-type: none"> <li>Information or data marked under the previous protective marking scheme and still in use <b>does not</b> need to be remarked — provided that users / recipients understand how it is to be handled in line with this new Classification Policy.</li> <li>Any legacy information or data marked under the previous protective marking scheme <b>does not</b> require remarking in line with this new Classification Policy.</li> </ul>
<p>Emailing material</p> <p>(inside the GSI / PSN or out over the Internet)</p>	<p><b>OFFICIAL:</b></p> <ul style="list-style-type: none"> <li>You should not normally send work email to non-GSI/PSN/CJSM addresses unless allowed for under local business policies and procedures, or with Information Asset Owner approval.</li> <li>Where more sensitive information must be shared with external partners (e.g. members of the public), consider using secure mechanisms such as password protection, consult IPA Team for advice.</li> <li>No restrictions on emailing information within secure systems, however it should be limited on a 'need to know' basis.</li> <li>You may choose to encrypt it to provide additional protection. Contact the IPA team for advice on encryption.</li> <li>You may choose to include additional handling instructions, if appropriate.</li> <li>You must follow any handling guidance stipulated by the Information Asset Owner.</li> </ul> <p><b>OFFICIAL – SENSITIVE:</b></p>

	<b>OFFICIAL</b>
	<ul style="list-style-type: none"> <li>You must only send work email to non-GSI/CJSM addresses unless allowed for under local business policies and procedures, or with Information Asset Owner approval</li> <li>“Release-Authorised:” must be the first words of the Subject line to signify that you have given thought to the sensitivity of the e-mail's contents and its destination.</li> <li>Information should normally be sent encrypted over the Internet. You can send it unencrypted over the Internet, but you have to make a risk-balanced decision and accept the risk of it being intercepted and exposed.</li> </ul> <p>When emailing OFFICIAL – SENSITIVE information within the department, you should still include the “Release-Authorised:” phrase in the Subject line.</p>
Moving assets by hand or post	<p><b>You must follow any handling guidance stipulated by the Information Asset Owner.</b></p> <p><b>BY HAND:</b></p> <p><i>OFFICIAL</i></p> <ul style="list-style-type: none"> <li>Protected at least by one cover/envelope.</li> <li>Authorisation secured from the Information Asset Owner if moving a significant volume of assets / records / files.</li> </ul> <p><i>OFFICIAL – SENSITIVE: as OFFICIAL plus</i></p>

	<b>OFFICIAL</b>
	<ul style="list-style-type: none"> <li>▪ Carried in a nondescript bag in order to not draw attention to the contents.</li> <li>▪ Never leave papers unattended.</li> </ul> <p><b>BY POST/COURIER:</b></p> <p><i>OFFICIAL</i></p> <ul style="list-style-type: none"> <li>▪ Use single, unused envelope.</li> </ul> <p><i>OFFICIAL – SENSITIVE: as OFFICIAL plus</i></p> <ul style="list-style-type: none"> <li>▪ Include return address on back of the envelope.</li> <li>▪ Never mark the classification on envelope.</li> <li>▪ Consider double envelope for highly sensitive assets (write the classification on the inner envelope only).</li> <li>▪ Consider using registered Royal Mail service or reputable commercial courier's 'track and trace' service.</li> </ul>
Bulk transfer of documents/data	<p><b>You must follow any handling guidance stipulated by the Information Asset Owner.</b></p> <ul style="list-style-type: none"> <li>▪ Requires the approval of the Information Asset Owner.</li> <li>▪ Assess for yourself the risks of transferring the assets.</li> <li>▪ Conduct an appropriate risk assessment.</li> </ul>

	<b>OFFICIAL</b>
	<ul style="list-style-type: none"> <li>▪ Speak to the IPA team for the best course of action to take.</li> </ul>
Faxing	<p><b>You must follow any handling guidance stipulated by the Information Asset Owner.</b></p> <p>Faxes should not be assumed to be secure. Consider using encrypted email if possible to communicate sensitive information.</p> <p><b>OFFICIAL:</b></p> <ul style="list-style-type: none"> <li>▪ No restrictions on faxing documents.</li> </ul> <p><b>OFFICIAL – SENSITIVE:</b></p> <ul style="list-style-type: none"> <li>▪ Sensitive material to be faxed should be kept to an absolute minimum.</li> <li>▪ Confirm the recipient's fax number.</li> <li>▪ Recipients should be waiting to receive faxes containing personal data and/or data marked OFFICIAL – SENSITIVE.</li> </ul>
Printing	<p><b>You must follow any handling guidance stipulated by the Information Asset Owner.</b></p> <p>Permitted – but print only what you need.</p> <p>All printed materials must be disposed of appropriately when no longer required or being used.</p>
Photocopying	<b>You must follow any handling guidance stipulated by the Information Asset Owner.</b>

	<b>OFFICIAL</b>
	Permitted – but make only as many copies as you need, and control their circulation.
<b>STORAGE</b>	
<b>Physical storage</b> (of documents, digital media, when not in use)	Protect physically within a secure building by a single lock (e.g. a locked drawer, container or locked filing cabinet). <ul style="list-style-type: none"> <li>▪ The clear desk policy should be observed.</li> <li>▪ Papers should not be left on desks or on top of cabinets overnight.</li> <li>▪ Laptops must be kept secure at all times and locked away overnight when left in the office.</li> </ul>
<b>Electronic storage</b> on QUANTUM / NICS or OMNI	Permitted  Any electronic document received marked OFFICIAL – SENSITIVE should be saved with OFFICIAL – SENSITIVE in the metadata, and appropriate controls used to limit access.
<b>Electronic storage on digital media</b> (USB memory sticks, CDs, DVDs)	Permitted <ul style="list-style-type: none"> <li>▪ The media must be encrypted.</li> <li>▪ Only NOMS supplied and approved portable media is to be used.</li> </ul>

	<b>OFFICIAL</b>
<b>Re-using digital media</b>  (USB memory sticks, CDs, DVDs)	For both OFFICIAL and OFFICIAL – SENSITIVE, delete contents and re-use digital media only within NOMS buildings and on NOMS computer systems.
<b>Disposing of paper documents</b>	Dispose of documents with care making reconstitution unlikely.  <b>OFFICIAL:</b> tear the document into small pieces and place in a recycling bin.  <b>OFFICIAL – SENSITIVE:</b> shred the document using an approved cross-cut shredder or place in a burn bag.
<b>Disposing of digital media</b>  (USB memory sticks, CDs, DVDs, etc)	<b>CDs and DVDs:</b> <ul style="list-style-type: none"> <li>▪ <b>Used for OFFICIAL information only:</b> Place disk into an envelope and break (with care) the disk into four pieces. Ensure that no piece is no larger than half of the total disc area. Dispose of pieces in ordinary office waste. Do not recycle.</li> <li>▪ <b>Used for OFFICIAL – SENSITIVE information:</b> the disk should be shredded or ground and scrubbed, using an approved shredder or grinder.</li> </ul> <b>USB memory sticks:</b> <ul style="list-style-type: none"> <li>▪ <b>Encrypted sticks:</b> Do not recycle, contact the IPA team for advice on appropriate methods of destruction. Shred any associated passwords.</li> </ul>



	<b>OFFICIAL</b>
	<ul style="list-style-type: none"> <li>▪ <b>Unencrypted memory sticks:</b> You must contact the IPA team.</li> </ul>
<b>Disposing of hard disk drives</b>	<p><b>Hard disk drive is to be / can be re-used</b></p> <ul style="list-style-type: none"> <li>▪ <b>OFFICIAL:</b> The hard disk drive should be overwritten using an approved commercial overwriting product. It can then be reused in an equivalent OFFICIAL environment.</li> <li>▪ <b>OFFICIAL – SENSITIVE:</b> The hard disk drive should be Blanco'd, and then overwritten using an approved commercial overwriting product. It can then be reused in an equivalent classified environment.</li> </ul> <p>Depending upon the sensitivity of the information stored on the hard disk drive, it may be more appropriate to shred the disk when it is no longer needed. Please contact the IPA team for advice.</p> <p><b>Hard disk drive no longer required and is not reusable</b></p> <ul style="list-style-type: none"> <li>▪ Regardless of the information stored on it, the drive should be shredded by an approved commercial contractor. Please contact the IPA team for advice on this.</li> </ul>
<b>REMOTE WORKING</b>	<ul style="list-style-type: none"> <li>▪ <b>Permitted following with the line manager's approval and compliance with the above guidance.</b></li> <li>▪ <b>No personal IT assets (eg, your home computer and peripherals) are to be used to process or store NOMS information.</b></li> <li>▪ Limit the amount of information you take out of the office. Only take what is necessary.</li> <li>▪ Laptops and removable media used to store OFFICIAL and OFFICIAL – SENSITIVE information must be encrypted.</li> </ul>

	<b>OFFICIAL</b>
	<ul style="list-style-type: none"> <li>Information must not be emailed to or from home e-mail accounts.</li> </ul> <p><b>OFFICIAL:</b></p> <ul style="list-style-type: none"> <li>Only encrypted, NOMS-supplied and approved portable media is to be used.</li> <li>Ensure information cannot be inadvertently overlooked.</li> <li>Store papers / portable media out of sight.</li> <li>NEVER leave papers or portable media in your car overnight.</li> </ul> <p><b>OFFICIAL – SENSITIVE:</b> <i>as OFFICIAL plus</i></p> <ul style="list-style-type: none"> <li>Items must not be opened or worked on whilst travelling or in a public area.</li> <li>Never leave papers / portable media unattended.</li> <li>If working from home, store papers, laptops and portable media in a locked drawer / cabinet.</li> </ul>
Discussing work on telephones (landline or mobile), in video conferences, via Microsoft Lync or in public places	<p><b>You should not assume telephony systems, video conferencing are secure.</b></p> <p><b>OFFICIAL:</b></p> <ul style="list-style-type: none"> <li>No restrictions but be careful of straying into areas that could be deemed as OFFICIAL – SENSITIVE.</li> </ul> <p><b>OFFICIAL – SENSITIVE:</b></p> <ul style="list-style-type: none"> <li>Details of sensitive material should be kept to an absolute minimum.</li> </ul>

	<b>OFFICIAL</b>
<b>PERSONNEL SECURITY</b>	<p><b>OFFICIAL:</b></p> <ul style="list-style-type: none"> <li>▪ Prior to recruitment, HR / line managers should carry out appropriate recruitment checks to Baseline Personnel Security Standard (BPSS).</li> <li>▪ Once recruited line managers should ensure staff complete the 'Responsible For Information' e-learning via Civil Service Learning.</li> <li>▪ Line Managers should ensure that staff read the NOMS IPA team Intranet pages and know where to go if assistance is required.</li> </ul> <p><b>OFFICIAL – SENSITIVE:</b> <i>as OFFICIAL plus</i></p> <ul style="list-style-type: none"> <li>▪ Staff should only share information on a 'Need to Know' basis.</li> </ul>
<b>Access requirements</b> (clearance levels)	Baseline Personnel Security Standard (BPSS)
<b>INCIDENT REPORTING</b>	Follow incident reporting procedures set out in B1 – Incident Management Procedure.

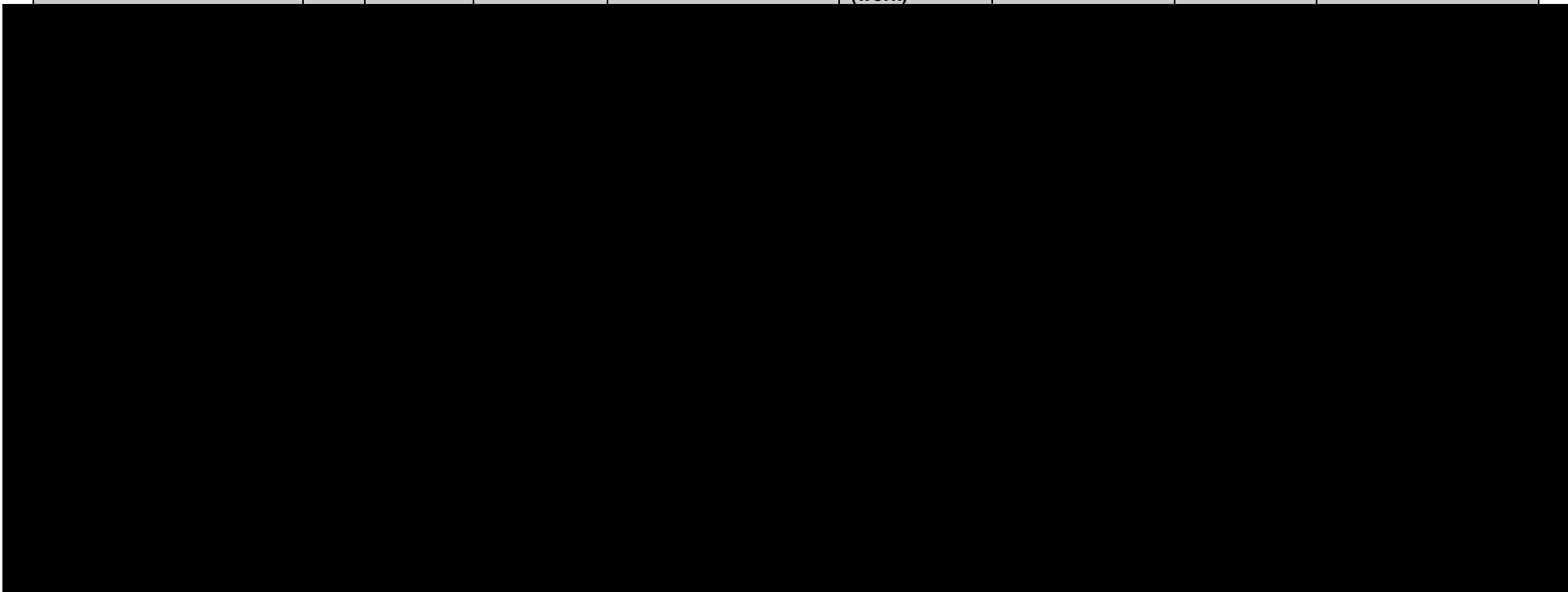
#### **Appendix 4 – Contractors Staff with Authority to Approve**

As per Clause N1.8, the inclusion of any member of the Contractors Staff with the list below does not, on its own, indicate that the Authority will consider an individual to have been granted Authority to Approve.

Individuals identified below will be asked to complete, sign and return to the Authority a copy of the Authority to Approve User Form, which will be available from the Authority and subject to periodic changes and updates.

The individuals shown below must also be cleared to SC (Security Check) level, which will be subject to validation by NOMS CFO.

<b>Service Provider (Contractor/Subcontractor)</b>	<b>Title</b>	<b>Name</b>	<b>Job role/Title</b>	<b>Business Address</b>	<b>Telephone number (work)</b>	<b>Telephone number (mobile)</b>	<b>Fax number</b>	<b>Email address</b>
--	--------------	-------------	---------------------------	-------------------------	--	--------------------------------------	-------------------	----------------------





## **SCHEDULE O: CHANGE PROTOCOL**

### **O1. Introduction**

- O1.1. Each of the Authority and the Contractor may request a Change in accordance with this Schedule O.
- O1.2. Each Change shall be discussed and implemented through the NOMS CFO Performance Board meeting, as the case may be.
- O1.3. The parties agree that a Change shall only take effect where a Change Notice is signed in accordance with this Schedule O by the Authority and the Contractor.
- O1.4. The Authority shall be entitled in its absolute discretion to withdraw or reject any proposed Change other than a Change in Law Change.

### **O2. Authority Changes**

- O2.1. The Authority has the right to propose changes in accordance with these provisions. If the Authority requires a change (an "Authority Change"), it must serve a notice (an "Authority Change Notice") on the Contractor in accordance with the provisions of this condition.
- O2.2. The Authority Change Notice shall:
  - O2.2.1. Set out the required change in the Services required in sufficient detail to enable the Contractor to implement such change;
  - O2.2.2. State whether it is a notification of required variation ("NRVC") or a notification of proposed variation ("NRPC"); and
  - O2.2.3. Require the Contractor to provide to the Authority within fifteen (15) working days of receipt of the Authority Change Notice an estimate of the likely effects of the requested variation including without limitation its effect on the profile payment (the "Estimate").
- O2.3. Notwithstanding any other condition in the Contract, where the Authority Change Notice indicates that it is an NRVC the Contractor shall implement the changes required as soon as reasonably practicable (and for the avoidance of doubt prior to any applicable alteration to the profile payment being determined in accordance with the provisions of this condition).
- O2.4. As soon as practicable and in any event within fifteen (15) working days after having received the Authority Change Notice, the Contractor shall deliver to the Authority the Estimate. The Estimate shall include the opinion of the Contractor on:

- O2.4.1. Any amendment required to the Contract or any ancillary document as a result of the Authority Change;
- O2.4.2. Any estimated change in the profile payment that results from the Authority Change;
- O2.4.3. Any regulatory approvals which are required; and
- O2.4.4. Any impact on the provision of the Services as a whole.
- O2.5. As soon as practicable after the Authority receives the Estimate, the parties shall discuss and agree the issues set out in the Estimate, including providing evidence that the Contractor has used reasonable endeavours to oblige its sub-contractors to minimise any increase in costs and maximise any reduction in costs. In such discussions the Authority may modify the Authority Change Notice, in which case the Contractor shall as soon as practicable (and in any event within ten (10) working days) after receipt of such modification, notify the Authority of any consequential changes to the Estimate.
- O2.6. If the parties cannot agree on the contents of the Estimate, then the dispute will be determined in accordance with the dispute resolution procedure set out at Clause 44 of the Contract.
- O2.7. As soon as practicable after the contents of the Estimate have been agreed the Authority shall:
  - O2.7.1. Confirm in writing to the Contractor the Estimate (as modified); or
  - O2.7.2. Withdraw the Authority Change Notice;
- O2.8. Provided that the Authority withdraws an Authority Change Notice expressed to be a NRVC the Authority shall indemnify the Contractor in respect of any costs incurred by the Contractor in implementing such change in accordance with the provisions of paragraph O2.2.3 above. Such indemnity is only given to the extent that such costs are reasonable, reasonably incurred and are supported by documentary evidence to the Authority's reasonable satisfaction. The Contractor shall also be under an obligation to mitigate any costs incurred as a result of the relevant Authority Change Notice.
- O2.9. Where an Estimate is confirmed the parties shall execute a variation in the form set out in Appendix A and shall enter into any such further documentation or agreements as may be necessary to give effect to the relevant change.

### **O3. Contractor Changes**

- O3.1. If the Contractor wishes to introduce a change (a “Contractor Change”) it must serve a notice (a “Contractor Change Notice”) on the Authority. The notice must be in the format specified by the Authority, as amended from time to time.
- O3.2. The Contractor Change Notice must:
  - O3.2.1. Set out the proposed change in sufficient detail to enable the Authority to evaluate it in full;
  - O3.2.2. Specify the Contractor’s reasons for proposing the change;
  - O3.2.3. Request the Authority to consult with the Contractor with a view to deciding whether to agree to the change and, if so, what consequential changes the Authority requires as a result;
  - O3.2.4. Indicate any implications of the change;
  - O3.2.5. Indicate whether a variation to profile payment is proposed; and
  - O3.2.6. Indicate if there are any dates by which a decision by the Authority is critical.
- O3.3. The Authority shall evaluate the Contractor’s proposed change in good faith, taking into account all relevant issues, including (without limitation) whether:
  - O3.3.1. A change to the profile payment will occur;
  - O3.3.2. The change affects the quality or the likelihood of successful delivery of Services;
  - O3.3.3. The change will interfere with the Authority’s business or the relationship of the Authority with third parties; and
  - O3.3.4. The change materially affects the risk or costs to which the Authority is exposed.
- O3.4. As soon as practicable after receiving the Contractor Change Notice, the parties shall meet and discuss the matter referred to in it. During their discussions the Authority may propose modifications or approve or reject the Contractor Change Notice.
- O3.5. If the Authority approves the Contractor Change Notice (with or without modification) the implementation of the relevant change shall be commenced within ten (10) working days of the Authority’s acceptance. Within this period, the parties shall consult and agree the remaining details as soon as practicable and shall execute a variation in the form set out in Appendix A and shall enter into any such further documentation or agreements as may be necessary to give effect to the relevant change.




- O3.6. If the Authority rejects the Contractor Change Notice, it shall not be obliged to give its reasons for such a rejection.
- O3.7. Unless the Authority specifically agrees to a change to any profile or to any payment, there shall be changes to profiles or to payments as a result of a change proposed by the Contractor.
- O3.8. If the change proposed by the Contractor causes or will cause the Contractor's costs to decrease then the profile payment shall be reduced to reflect a sharing in the decrease in costs in accordance with the Contract.

#### **O4. Change in Law**

- O4.1. The Contractor shall not be entitled to refuse to carry out a Change in Law Change.
- O4.2. For the purposes of this Agreement, "Change in Law" means the coming into force after the date of this Agreement of:
  - O4.2.1. Legislation other than Legislation which, at the date of this Agreement:
    - O4.2.1.1. has received Royal Assent but has not been commenced; or
    - O4.2.1.2. subject to Clause O4.3, has been published;
  - O4.2.2. any Directions; or
  - O4.2.3. any applicable judgment of a relevant court of law which creates or changes a binding precedent.
- O4.3. For the purposes of Clause O4.2.1.2, the parties agree that proposed Legislation which comes into force after the date of this Agreement which is different from that which was published before the date of this Agreement and where those differences require the Contractor to incur additional costs which it would not have had to incur had the relevant proposed Legislation come into force in the form published before the date of this Agreement, the coming into force of that proposed Legislation shall be a Change in Law for the purposes of this Agreement.
- O4.4. The Contractor shall provide to the Authority as part of the process set out in the Change Protocol, reasonably detailed evidence in writing of the additional costs that it will have to incur as a direct result of the coming into force of the proposed Legislation.
- O4.5. For the purposes of Clause O4.2.1.2, published means published:

- O4.5.1. in a draft Bill as part of a Government Departmental Consultation Paper;
- O4.5.2. in a Bill;
- O4.5.3. in a draft statutory instrument; or
- O4.5.4. as a proposal in the Official Journal of the European Union.

## Appendix A – Variation Template

<div style="display: flex; justify-content: space-between; align-items: center;"><div style="text-align: left;"><b>Ministry of JUSTICE</b>   Procurement</div><div style="text-align: right;"> <b>European Union</b> European Social Fund <small>Investing in jobs and skills</small></div></div> <div style="text-align: center; margin-top: 10px;"><b>Variation to Contract Form</b></div>		
<p>Contract Title :</p> <p>Contract Reference :</p> <p>Variation Number :</p> <p>Date Effective From :</p> <p>Between:</p> <div style="border: 1px solid black; padding: 5px; margin-top: 5px;"><p>The Secretary of State for the Authority, represented by The Ministry of Justice Commercial and Contract Management Directorate (hereinafter called "the Authority") &amp; XXXXX (hereinafter called "the Contractor").</p></div> <p>1. The Contract is varied as follows:</p> <div style="border: 1px solid black; height: 100px; margin-top: 10px;"></div> <p>2. Words and expressions in this Variation shall have the meanings given to them in the Contract.</p> <p>3. The Contract, including any previous Variations, shall remain effective and unaltered except as amended by this Variation.</p> <p>Signed:</p> <table style="width: 100%; border: none;"><tr><td style="width: 50%; vertical-align: top;"><p>For the Authority</p><p>Signature : .....</p><p>Name : .....</p><p>Title : .....</p><p>Date : .....</p></td><td style="width: 50%; vertical-align: top;"><p>For the Contractor</p><p>Signature : .....</p><p>Name : .....</p><p>Title : .....</p><p>Date : .....</p></td></tr></table>	<p>For the Authority</p> <p>Signature : .....</p> <p>Name : .....</p> <p>Title : .....</p> <p>Date : .....</p>	<p>For the Contractor</p> <p>Signature : .....</p> <p>Name : .....</p> <p>Title : .....</p> <p>Date : .....</p>
<p>For the Authority</p> <p>Signature : .....</p> <p>Name : .....</p> <p>Title : .....</p> <p>Date : .....</p>	<p>For the Contractor</p> <p>Signature : .....</p> <p>Name : .....</p> <p>Title : .....</p> <p>Date : .....</p>	
<b>Official - Sensitive</b>		
<p>Variation to Contract Form (10/09) Version 2.0</p>		

## **SCHEDULE P: MARKET STEWARDSHIP PRINCIPLES**

### **P1. Introduction**

- P1.1. The Market Stewardship Principles cover five key principles that must underpin the Contractor's provision of the Services and its engagement with all entities to which it subcontracts the provision of the Services.
- P1.2. Each of the principles is set out in this Schedule together with guidance as to how the Contractor should respond to its obligations against each of the principles.

### **P2. Adherence to appropriate management of risk in the supply chain**

- P2.1. All contractual and other risk should be appropriately managed. This should extend to not passing risk down supply chains disproportionately, the management of volume fluctuations and other events and the management of intellectual property rights.

#### **P2.2. Meaningful volume of work allocation**

P2.2.1. The Contractor should be able to evidence its approach in allocating work to supply chain partners in a manner which meets its obligations under this Agreement. Where a supplier is specified in the Contractor's Tender as a supply chain partner, the Contractor shall refer meaningful volumes of work to that supplier. These volumes should be set out in the Contractor's Tender.

P2.2.2. The Contractor shall record details of all issues arising out of complaints from suppliers that they have not received expected volumes of work and shall refer these complaints to the Authority.

#### **P2.3. Systems for allocation of work to the supplier**

The Contractor should have systems for allocation of specific work to the supplier where the delivery of the Service to a Participant is best served by calling on the particular expertise of the supplier. The allocations should ensure that the Participant receives services from a supply chain organisation that has the correct level of expertise. Examples would include suppliers who have the skills and experience required to work with Participant with a range of different needs such as protected characteristics, female offenders, ethnic minority offenders, BAME, and offenders with learning difficulties or dyslexia etc.

#### **P2.4. Volume Fluctuations**

The Contractor must demonstrate to the Authority's satisfaction how it manages any volume fluctuations in offender referrals and the reallocation of caseload to the supply chain. The potential impact of both increases and particularly reductions in work allocation and associated drop in income, and actions to mitigate these risks, must be set out in the Industry Standard Partnering Agreement.

**P2.5. Spot purchase arrangements**

Spot purchase arrangements may be entirely appropriate but can be detrimental to supply chain partners as opposed to more standard contracts that guarantee an income. Suppliers generally, but also in seeking funding or additional business, may be disadvantaged in only being able to reference spot purchase contracts. The Contractor should therefore ensure that wherever 'spot purchase' arrangements are utilised, options to transition to more stable contractual referral systems are reviewed at regular periods.

**P2.6. Payment terms**

The Contractor should detail a full exploration of payment terms and the impact of these on the supply chain including the requirement for any clawback/repayment if targets are not met. The implications of this should be worked through for each year of the Industry Standard Partnering Agreement.

**P2.7. Minimum contract term**

Consideration should be given to the needs of the supplier in relation to the contract term. The contract length, if inadequate, may damage the ability of the supplier in seeking new business or additional funding from elsewhere. Supporting statements around expected minimum term of contracts may be helpful for sub-contracting organisations to avoid this. A minimum three year term should be appropriate for most supply chain partnerships.

**P2.8. Intellectual Property Rights (IPR)**

The Contractor should set out in the Industry Standard Partnering Agreement an approach for the handling of intellectual property rights to be established as part of the supply chain selection process.

**P3. Alignment of ethos in the supply chain**

**P3.1.** The Authority envisages that a sustainable relationship is fostered throughout the contractual period, which meets the expectations of both parties according to the position established at contract inception. In entering into a contractual agreement, there should be an understanding of what is important

to both parties and this should go on to form part of the contractual agreement which will be reviewed throughout the contract term to ensure that expectations are being met. The Authority's market engagement has reinforced that this is an important expectation for many organisations and key to building trust, especially in the early stages of such business relationships.

**P3.2. Audit trail**

The Contractor must maintain an audit trail of engagement with suppliers that demonstrates compliance with the principles established at the outset of their working relationship and shall include any additional support the Contractor offers.

**P3.3. Support declared in the bid to supply chain organisations**

The Contractor must publish a statement with regard to the support that is being offered by the Contractor to suppliers. Each support element must be itemised.

**P3.4. Referrals of Applicable Persons to non-contracted partners**

The Contractor may wish to refer Applicable Persons to organisations in its ESF Contract Area who already deliver support services relevant to rehabilitation. The Contractor must not exploit the services delivered by these organisations, particularly those who do not enter into a formal contractual or grant funding arrangement with the Contractor. The Authority will require the Contractor to articulate how it is supporting and sustaining all organisations that the Contractor intends to refer a significant volume of Participants. In this context, 'significant' should be interpreted in proportion to the size of the organisation rather than the Contractor's caseload.

**P3.5. Meetings**

The Contractor must record details of the conduct of all meetings with members of its supply chain and review these records to ensure that they are timely and appropriate and reinforce good relationship management.

**P4. Visibility across the supply chain**

P4.1. The Authority expects that all parties have visibility of participation within the supply chain. This should include payment terms against contractual targets, the volume of business handled by supply chain partners, fair apportionment of referrals with regard to easier cases, and how the supply chain adjusts to

changing volumes or demographics within the Contractor's ESF Contract Area.

**P4.2. Supply chain sourcing, selection and refresh process**

The Contractor must ensure that the sourcing, selection and refresh process for supply chain partners is transparent. This information must be made freely available to both the Authority and each potential supplier on request.

**P5. Reward and recognition of good performance**

- P5.1. The Authority considers it important that organisations in the supply chain receive appropriate reward for good performance. Recognition of good performance should be shared across the chain and this should include the sharing of good practice. As industry forums are instigated, methods for sharing data other than through the data room will be developed.

**P6. Application of the principles of the Compact in work with Civil Society Organisations**

**P6.1. Evidence of compliance and other issues**

The Authority has an expectation that the Contractor and its supply chain follow the principles of the Compact when engaging with Civil Society Organisations (as that term is defined in the Compact).