

Memorandum of Understanding

between

**the Secretary of State for the Home Department acting through
Immigration Enforcement**

and

the London Borough of [Insert name of Borough]

in respect of the provision of Immigration Enforcement's Checking and Advice Service (IECAS)

For the period [insert contract start date] to [insert contract end date]

Official Sensitive

This **Memorandum of Understanding** (MoU) is made this [insert day of month] day of [insert month and year] between **THE SECRETARY OF STATE FOR THE HOME DEPARTMENT** of 2 Marsham Street, London, SW1P 4DF acting through Immigration Enforcement (**"The Authority"**)

and

THE LONDON BOROUGH OF [insert name of London Borough] of [insert address of London Borough] (**"The Customer"**)

1. BACKGROUND

- 1.1 This MoU outlines the agreement between the Authority and the Customer regarding the provision of IECAS, specifically the utilisation of a member of Home Office staff ("Officer") as defined in Schedule 2.
- 1.2 The Customer wishes to receive the Service as described in Schedule 2.
- 1.3 The Authority agrees to provide the Service, as described in Schedule 2, subject to the Customer making the payments, as described in Schedule 3, and complying with its other obligations as set out in this MoU.

2. STATUS OF THIS MOU

- 2.1 This MoU is not intended to be legally binding. It does not create any rights or obligations enforceable in law, whether in partnership, agency, joint venture or otherwise.
- 2.2 For the avoidance of doubt:
 - 2.2.1 Except where explicitly stated, this MoU shall not affect any of the existing contractual relationships between the Parties.
 - 2.2.2 Nothing in this MoU shall act to prevent the Parties entering into binding legal agreements in relation to other projects in the future.

3. COMMENCEMENT AND TERMINATION

- 3.1 This MoU shall commence on the date of signature of this MoU, by each Party, and shall expire when the MoU is terminated in accordance with clause 3.2 unless the Parties agree in writing to extend the duration of the MoU.
- 3.2 Should the Customer no longer require the Service, the Customer may terminate this MoU on provision of three (3) months notice in writing. Should the Authority breach the terms of this MoU the Customer may terminate the MoU immediately.
- 3.3 Should the Authority wish to cease providing the Service, the Authority may terminate this MoU on provision of three (3) months notice in writing. Should the Customer breach the terms of this MoU the Authority may terminate the MoU immediately.
- 3.4 Should the Customer fail to pay for the Services provided then the Authority may seek to end the provision of the Services immediately.

4. DEFINITIONS AND INTERPRETATION

Official Sensitive

- 4.1 In this MoU the words and phrases listed in Schedule 1 have the corresponding meanings.
- 4.2 The headings in this MoU are for ease of reference only and shall not affect the interpretation or construction of this MoU.
- 4.3 Where the context permits, the use of the singular shall be construed to include the plural; the use of plural the singular; and the use of any gender shall include all genders.
- 4.4 References to an Act of Parliament shall be deemed to include any subordinate legislation of any sort made from time to time under the Act.
- 4.5 References to any statute, enactment, order, regulation code or similar instrument shall be construed as a reference to the statute, enactment, order, regulation, code or similar instrument as subsequently amended or re-enacted.
- 4.6 References to “Clauses”, “Recitals” and “Schedules” are to the clauses and recitals of and schedules to this MoU, as the same may be amended from time to time.

5. OBLIGATIONS AND RESPONSIBILITIES

- 5.1 Each Party agrees to nominate an Appointed Official, within one (1) calendar month of signing this MoU, to oversee the implementation, management and operation of the provisions within this MoU. Unless otherwise stated the Appointed Officials will have the authority to agree matters, as required in this MoU, on behalf of the Authority and the Customer.
- 5.2 A Party's Appointed Official can change as and when required but the other Party must be informed of the change within three (3) working days.
- 5.3 The Appointed Officials, at least seven (7) calendar days before the commencement of each calendar month, will agree a working pattern for the coming month detailing the days and hours the Officer will deliver the Services. The work pattern will also set out any agreement for the Officer to deliver the Services away from the Premises. When agreeing monthly work patterns the Appointed Officials will aim for a consistent provision of Service whilst accepting sporadic variation over the length of the MoU.
- 5.4 The Appointed Officials will meet on dates to be agreed (at least quarterly), to discuss the monitoring of this MoU, the Officer's performance, the delivery of the Services, the payment for the Services, production of Agreed Monthly Work Pattern documents, potential revisions to the MoU and wider strategic issues.
- 5.5 The day-to-day management of the Services will be led by the Customer but the Authority will retain substantive management of the Officer.
- 5.6 In the event of exceptional operational circumstances (including, but without limitation to, circumstances arising from an emergency or from a material disruption to the Authority processes or a Force Majeure Event) the Authority may temporarily suspend or reduce provision of the Service in part or in whole immediately.
- 5.7 Where the Authority and Customer agree to reduce or amend the provision of the Service, the Customer shall only be liable for the cost of the Service provided.

6. THE AUTHORITY'S OBLIGATIONS

Immigration Enforcement Checking and Advice Service – December 2019

Official Sensitive

6.1 For the duration of this MoU, the Authority shall:

- 6.1.1 Provide the Service described in Schedule 2 at the premises of the Customer and in line with the Agreed Monthly Work Pattern;
- 6.1.2 Be responsible for the recruitment, employment, and training of those Officers required to deliver the Service;
- 6.1.3 Ensure that the Officer has access to relevant Home Office databases, information, systems and to communicate information derived from these to effectively carry out the Service;
- 6.1.4 Provide the Officer with the appropriate Laptop, Mobile Phone, and Uniform to effectively carry out the Service;
- 6.1.5 Provide a mobile Wi-Fi device if the Customer is unable to deliver its obligations under Clause 7.1.9.

7. THE CUSTOMER'S OBLIGATIONS

7.1 For the duration of this MoU, the Customer shall:

- 7.1.1 Cooperate with the Authority in all matters relating to the Service;
- 7.1.2 Ensure that the Officer is provided with a host manager, who will oversee and support the Officer, act as the primary point of contact for the Officer. The host manager does not have to be the same person as the Appointed Official;
- 7.1.3 Provide the Authority with immediate feedback on any performance, conduct or attendance issues that come to light in order that they can be appropriately addressed and rectified by the Authority without delay to maintain the Service;
- 7.1.4 Ensure that the Appointed Official or host manager monitors and authorises the Officer's Time Sheets on a monthly basis as set out in Schedule 3, Clause 3;
- 7.1.5 Provide a safe and effective working environment for the Officer including induction in appropriate Health and Safety and Fire Evacuation procedures;
- 7.1.6 Provide the Officer with access to; a desk, a chair, a phone, building pass, desk space that will not contravene data protection principles, secure personal storage facilities, changing facilities, relevant employees or contractors and customers;
- 7.1.7 Provide the Officer with secure internet and/or Wi-Fi facilities to enable them to effectively provide the Service;
- 7.1.8 Provide relevant training to the Officer in relation to the Customer's business, including but not limited to job-shadowing, to enable the Officer to fulfil the Service requirements;
- 7.1.9 Agree to the provision of management information, as set out within the MoU Update Meeting document contained at Schedule 5, at each meeting (minimum of quarterly) between the Appointed Officials;

Official Sensitive

7.1.10 Provide management information and feedback on Time Sheets and Agreed Monthly Work Patterns at the meetings between the Appointed Officials in accordance with the parameters set out within the MoU Update Meeting document contained at Schedule 5;

7.1.11 With their express permission, agree to the Authority publishing management information pertaining to the services provided, specifically changes to caseload figures and financial savings made to further promote the Service to prospective partner organisations.

7.2 Payment for the Service will be made in accordance with Schedule 3.

8. STATUTORY OBLIGATIONS

8.1 This MoU, and the provision of the Service, does not relieve the Customer from any of its statutory obligations, nor can it form the basis of a defence or excuse where a law has been breached. For the avoidance of doubt this means this MoU does not:

8.1.1 limit, exclude or otherwise protect the Customer from any civil court action or criminal prosecution; or

8.1.2 limit, exclude or otherwise restrict the Customer from its obligation to comply with the law; or

8.1.3 limit or exclude the liability of either Party for death or personal injury caused by its negligence, or for fraudulent misrepresentation or fraudulent concealment.

9. CHARGES, LIABILITIES AND PAYMENT FOR THE SERVICES

9.1 The Parties agree that the provisions of Schedule 3 will apply to the financial arrangements between them for the provision of the Service

9.2 The provisions in Schedule 3 will apply only for the Service provided between the date of commencement of this MOU and the date of its termination

9.3 In consideration for the Service provided by the Authority, the Customer shall make payments to the Authority in accordance with the terms of Schedule 3.

9.4 The Authority's charges for the Service are set out in Schedule 3. The Authority reserves the right to vary from time to time any of its charges in any way it sees fit. Any variation will be subject to further Parliamentary approval. The Authority will provide the Customer with such notice as is reasonable in the circumstances of any variation in charges.

9.5 The Authority will give to the Customer such notice as is reasonable in all the circumstances of any variation in charges.

9.6 For the avoidance of doubt, charges incurred by the Authority that have been invoiced in accordance with Schedule 3 of this MoU are not refundable.

9.7 Except as otherwise provided, the Parties shall each bear their own costs, expenses, losses or liabilities incurred in complying with their obligations under this MoU.

10. SERVICES CONTINUITY

Official Sensitive

- 10.1 Unplanned absences: The Officer will be instructed to contact their host manager and their Authority manager if they are unable to attend work in accordance with the agreed monthly working pattern document, for example because of illness. The Authority will attempt to provide an alternative Officer. However, if no Officer is available the Service will not be provided. If no Officer can be provided to fulfil the Service, the Customer shall not be liable for any costs for the time that the Service is unavailable.
- 10.2 Exceptional circumstance: Both the Authority and Customer agree the monthly work pattern document can be altered, by agreement of both parties, with three working day's notice where circumstance requires such amendments. Furthermore, in the event of exceptional operational circumstances the Authority may temporarily suspend or reduce the provision of the Service. In these circumstances the Customer will only be liable to pay for the Service based on the reduced number of hours provided.
- 10.3 The Customer's host manager will contact the Authority's Appointed Official if the Officer takes any unauthorised absences.
- 10.4 The Agreed Monthly Work Pattern will detail planned absences.

11. STATUS OF THE OFFICER

- 11.1 For the avoidance of doubt, the Officer remains the employee of the Authority and shall not become, or be regarded as, the employee, consultant, agent, sub-contractor or representative of the Customer. This MoU is not a contract of employment.

12. CONDUCT, DISCIPLINE AND SECURITY

- 12.1 The Officer will be subject to the provisions of the Official Secrets Act(s) 1911-1989 and section 182 of the Finance Act 1989 and the conditions and rules governing the conduct of civil servants. In particular, they will be required to observe rules governing political activities and the need to avoid situations that may lead to conflicts of interest.
- 12.2 The Officer will also remain subject to the Authority's conduct, discipline and grievance procedures, Authority policies and the standards of work and behaviour set out in the Civil Service Code. The Officer will be instructed additionally to observe the standards of work and behaviour set out in the Customer's Staff Handbook. In the event of any breach of these standards the Customer shall inform the Authority. In the event of any conflict between these documents the Civil Services Code and Authority policies will take precedence.

13. HEALTH AND SAFETY

- 13.1 The Customer has a Health and Safety Policy in which it accepts its responsibility under health and safety legislation and, so far as is reasonably practicable, the health, safety and welfare of all employees and other persons at its premises. The Customer therefore accepts its responsibility to ensure the health, safety and welfare of the Officer whilst providing the Service.
- 13.2 The Authority retains its obligations to the Officer as required by the Health and Safety at Work Act etc. 1974 and any subordinate legislation to that Act.

14. VARIATION

- 14.1 This MoU may be varied by written agreement between the Parties.
Immigration Enforcement Checking and Advice Service – December 2019

Official Sensitive

- 14.2 In the event that the Customer requires any variation to this MoU, the Authority shall provide on request details of the effect of such proposed variation on the Services and what adjustment(s), if any, would be required to the Hourly Rate or any other charges that may be applicable.

15. RIGHTS AND LIABILITIES

- 15.1 Any additional costs incurred should be agreed prior to commitment by the Parties.

16. LIMITATION OF LIABILITY AND INDEMNITY

- 16.1 Subject to Clauses 16.2 and 16.3 the Customer shall, during and after the term of the MoU, indemnify and keep indemnified and hold the Authority harmless from and against all actions, suits, claims, demands, damages, expenses, legal costs and other liabilities arising from or incurred as a result of or in connection with any breach of this MoU, except where any such claim arises from any act or omission of the Authority.
- 16.2 Nothing in this MoU shall operate to limit or exclude the liability of either Party for death or personal injury caused by its negligence, or for fraudulent misrepresentation or fraudulent concealment.
- 16.3 For the avoidance of doubt, the Customer shall not be liable to the Authority or its contractors or its employees or any other third party for any indirect costs incurred by the Authority unless such the costs are caused or contributed to by any act or omission or by the negligence or default of the Customer, its employees, agents, consultants or sub-contractors, or by any circumstances within the Customer or its employees, agents, consultants or sub-contractors control

17. FREEDOM OF INFORMATION REQUESTS

- 17.1 For the purposes of this clause:
- 17.1.1 "FOI Act" means the Freedom of Information Act 2000 and any subordinate legislation made under that Act or any guidance issued by the Information Commissioner;
- 17.1.2 "Information" means all records and information of any sort obtained, created, collected or held by the Authority and Customer in relation to this MoU; and
- 17.1.3 "Information Request" means a request for Information within the meaning of section 8 of the FOI Act.
- 17.2 Each Party accepts the other is subject to the FOI Act and agrees to assist and co-operate to enable each Party to comply with its obligations under the FOI Act.
- 17.3 Each Party may be obliged to comply with its obligations under the FOI Act without informing or consulting the other.
- 17.4 Notwithstanding Clause 17.3 above, each Party shall take all reasonable steps to inform and consult before responding to an information request and shall take into account any views expressed by the other Party. Where it was not possible to inform and/or consult the other Party in advance of a disclosure, it shall draw the disclosure to the other Party's attention after the event.

Official Sensitive

- 17.5 Without prejudice to Clause 17.2, each Party shall use reasonable endeavours to provide each other with any information necessary to enable them to answer an information request.
- 17.6 Should the Customer receive an Information Request which ought to have been addressed to the Authority it shall not attempt to process the request itself but shall within three (3) days return the request to the originator and instruct them to send it to:

Direct Communications Unit
2 Marsham Street
London
SW1P 4DF
e-mail: foirequests@homeoffice.gov.uk
copied to: IEChecking&AdviceService@homeoffice.gov.uk

18. DATA PROTECTION LEGISLATION

- 18.1 Both parties agree that they will comply with all the requirements of Data Protection Legislation in relation to their obligations under this MoU.

19. DATA SHARING AND INFORMATION SECURITY

- 19.1 The parties shall comply with all their respective duties and responsibilities in relation to information sharing, data security and confidentiality as set out within this agreement.
- 19.2 The full data sharing and information security protocols are as described in Schedule 4.

20. CONFIDENTIALITY

- 20.1 Each Party on receiving information obtained in the course of the MoU or which may come into the possession of any of its employees, agents, consultants or sub-contractors as a result of or in connection with this MoU undertakes:
- 20.1.1 to treat as confidential all information which is specifically designated as such by the disclosing Party, except to the extent the receiving Party:
 - 20.1.1.1 can show that such information is already in the public domain (other than by a breach of this MoU);
 - 20.1.1.2 can show that such information was received without restriction on disclosure or use from a third Party lawfully entitled to make the disclosure to the receiving Party;
 - 20.1.1.3 is authorised to disclose such information by any written agreement between the Parties;
 - 20.1.1.4 is required by law to disclose such information; or
 - 20.1.1.5 without limiting the application of Clause 20.1.1.4 is required to disclose information under the Freedom of Information Act 2000 and any subordinate legislation made under that Act from time to time or the Environmental Information Regulations 2004.

Official Sensitive

- 20.1.2 to take all necessary precautions to ensure that all information is treated as confidential by its employees, agents, consultants or sub-contractors.

21. DIFFERENCES OF OPINION

- 21.1 Any difference of opinion between the Parties under this MoU will be referred in the first instance to the respective Appointed Officials for discussion within seven (7) days.
- 21.2 In the event that such discussions fail to reach a conclusion, then the issue will be referred to the relevant Director of each Party with fourteen (14) days.

Official Sensitive

Signed on behalf of the Authority

By

Name

Position

Date

Signed on behalf of the Customer

By

Name

Position

Date

SCHEDULE 1 – DEFINITIONS

“Agreed Monthly Work Pattern” means a working pattern for the coming month detailing the days and hours the Officer will deliver the Services as agreed by the Appointed Officials;

“Appointed Officials” means officials named by each the Authority and the Customer respectively to oversee the implementation, management and operation of the provisions within this MoU. Unless otherwise stated, the officials will have the authority to agree matters, as required in this MoU. Replacement officials will be appointed by the Authority and the Customer as and when required;

“Controller” means the person who determines the manner in which and purposes for which personal data are to be processed either alone or jointly in common with other persons as defined in the Data Protection Legislation;

“Data Protection Legislation” means the General Data Protection Regulation and the Data Protection Act 2018;

“Data Subject” has the same meaning as defined in the Data Protection Legislation, being an identified or identifiable natural person who is the subject of personal data;

“Force Majeure” means in the event that either Party is prevented from carrying out its obligations under the MoU as a result of any cause beyond its control (such as - but not limited to - acts of God, war and/or floods), that Party shall be relieved of its obligations and liabilities under the MoU for as long as such cause persists PROVIDED THAT both Parties shall undertake to resume normal performance of the affected obligations as soon as reasonably practicable;

“Hourly Rate” means the rate set out in clause Schedule 3;

“IECAS” means Immigration Enforcement’s Checking and Advice Service;

“MoU” means this Memorandum of Understanding;

“Officer” shall mean an appropriately trained Home Office member of staff provided by the Authority for the express purpose of providing the Services detailed at Schedule 2;

“Party” means the Authority or the Customer;

“Personal Data” means any information relating to a data subject who can be identified from it or data that can be put together with other information to identify a living individual. It covers data held in any format;

“Premises” means the Customer’s premises;

“Privacy Information Notice” means a publically available statement or document that sets out some or all of the ways a party gathers, uses, discloses, and manages a customer or client’s data. It fulfils a legal requirement to protect a customer or client’s privacy

“Process” has the same meaning as defined in the Data Protection Legislation and includes collecting, recording, storing, retrieving, amending or altering, disclosing, deleting, archiving and destroying personal data

“Processor” means any person who processes personal data on behalf of the Controller (other than an employee) as defined by the Data Protection Legislation;

Official Sensitive

“Service” shall have the meaning set out in Schedule 2;

“Time Sheets” mean excel documents used by the Officer to accurately record their hours of service at the Premises.

SCHEDULE 2 – SERVICES

1. The Services provided by the Officer, and charged for under this MOU, will be based on the Customer's corporate requirements at any given time in respect of an individual's eligibility to access benefits and services.
2. The Officer will work the following teams within the Customer's organisation; (Housing Needs; Homelessness and Immigration Team; Children's Services Leaving Care; Adult Social Care; Adult Mental Health services,
3. The services provided by the Officer will consist of the following functions:

3.1 Where individuals or families approach the Customer for support or benefits under the following legislation:

- 3.1.1 No Recourse to Public Funds assessments in respect of Section 17 Children Act 1989;
- 3.1.2 Housing assessments and allocations under Part VI Housing Act 1996;
- 3.1.3 Homelessness assessments and support under Homelessness Reduction Act 2017 and part VI Housing Act 1996.
- 3.1.4 Section 117 (Mental Health Act);
- 3.1.5 Section 9 (Care Act) or Sections 6 and 7 (Housing Act);
- 3.1.6 Other relevant legislation;

the Officer will conduct real-time immigration status checks to support the Customer's decision-making in relation to the individual's or family's eligibility for support or benefits and advise on the implications of those status checks. This includes:

- 3.1.7 Maintaining effective front-line processes for families and individuals seeking support or benefits, primarily by providing immigration status information which aids the Customer to determine an individual's or family's eligibility to support, services, or benefits.
 - 3.1.8 Inspecting immigration and nationality documentation provided by individuals and families seeking support, services or benefits to enable the Customer to determine whether an individual or a family is entitled to support or benefits.
 - 3.1.9 Providing the Customer with an overview of voluntary returns information if appropriate.
- 3.2 The Officer will assist the Customer's teams listed in paragraph 2 of this schedule to periodically review its stock of cases by conducting immigration status checks on those individuals and families receiving support or benefits and advising on those checks. These checks will be used by the Customer in determining whether individuals and families remain eligible for support or benefits.

Official Sensitive

- 3.3 The Officer will establish processes to enable the Customer to effectively manage, audit and review the Customer's team's cohort of cases on a periodic basis in relation to immigration status checking. The Officer will provide an audit report making appropriate recommendations for improvements.
- 3.4 The Officer will assist the Customer to use the NRPF Connect system effectively to maximise the resolution of outstanding queries and cases.
- 3.5 The Officer will assist the Customer in evaluating the effectiveness of the service at regular update meetings to be determined by the Customer.
- 3.6 The Officer will act as a single point of contact between the Customer and Authority teams to ensure expedient case progression on the part of the Customer and the Authority and thus mitigating the potential for delay through an active involvement in the diary management of the Customer's teams (listed in paragraph 2 of this schedule) cohort of cases.
- 3.7 In order to enable the Customer to be able to confidently understand and conduct immigration status checks themselves, as part of their service provision, the Officer will deliver appropriate immigration training to the Customer's employees and provide appropriate support to embed knowledge in response to recommendations set out in the audit report detailed in Schedule 2 paragraph 3.3. Where the Officer is unable to deliver specific training, themselves they will work with the Customer to secure it. The Officer will deliver any training or support within their usual working pattern as agreed in Schedule 2 paragraphs 4, 5 and 6.
- 3.8 Where appropriate, the Officer will help facilitate the broader relationship between Customer and other Authority teams.
- 4 the Services will be provided at the Premises of the Customer for 200 days over the length of the MOU. (Specify days and times)
- 5 A days Service will constitute the Officer providing the Services for 7 hours 12 minutes per day, although fractions of days maybe agreed and charged at a proportional rate.
- 6 The Agreed Monthly Work Pattern can be altered, as required, by agreement of both Appointed Officials.
- 7 Subject to Schedule 2 Clauses 4 to 6 the Services will only be provided Monday to Friday, excluding public holidays. Number

SCHEDULE 3 – FINANCE

1. The Customer will be provided with [insert number of days required] Higher Officer (or equivalent) days for the duration of the MoU at an estimated cost of [insert estimated cost].
2. Based on the fees defined in the Immigration and Nationality (Fees) Regulations 2016, the hourly rate for the Services will be £58.20 at Higher Executive Officer rate/ £52.80 Executive Officer rate.
3. In reference to the Agreed Monthly Work Pattern document, as detailed at Schedule 2 Paragraph 4, the Officer will keep an accurate record of the hours they provided the Services to the Customer. These are recorded on the Time Sheet. On the second working day of each calendar month the Officer will e-mail the completed Time Sheet for the previous calendar month to the Customer's Appointed Official or host manager for authorisation. Once authorised and on the same day the Customer's Appointed Official or host manager shall e-mail the Time Sheet to the Authority's Appointed Official. This will be treated as confirmation and authorisation of the hours worked. The Time Sheet will be utilised by the Authority to raise an invoice.
4. Based on the hours of service provided by the Officer an invoice for payment will be raised and provided to the Customer by the Authority quarterly from the commencement of the MoU. The invoice will be sent to [insert Customer address for submission of the invoice]. This will be calculated by multiplying the number of hours used by £58.20/£52.80. The invoice will be paid by the Customer within 30 days of the receipt of the invoice.
5. In the event that other extraordinary costs are likely to be incurred, these will be agreed between the Appointed Officials.
6. The Customer is required to provide a PO number and invoicing details within seven (7) days of the MoU being signed. The PO number and invoicing details should be e-mailed to: IE-CAS@homeoffice.gov.uk

SCHEDULE 4 – PERSONAL DATA SHARING AND INFORMATION SECURITY

1. Introduction

- 1.1 Given the nature of the service provided this schedule combines the requirements of an umbrella memorandum of understanding and a process level memorandum of understanding in respect of the information sharing that will take place between the Parties.
- 1.2 Where anonymised information, pseudonymised information or non-personal information is shared, the recipient of that information will not attempt to re-identify any individual by analysing or combining it with other information which is in its possession at the time of receipt or subsequently comes into its possession.
- 1.3 This Schedule sets out the Personal Data sharing arrangement between the Authority and the Customer. It governs the exchange of information between the two Parties.
- 1.4 It ensures that information is shared with appropriate safeguards and in accordance with the law. Organisations which share information, particularly information that involves the sharing of Personal Data have a legal responsibility to ensure that the disclosure of information is both lawful and subject to adequate controls.
- 1.5 This Schedule aims to:
 - 1.5.1 set out the principles that will govern the sharing of information between the Parties including the onward disclosure of Personal Data to third parties;
 - 1.5.2 describe the processes, structures and roles that will support the exchange of information between the Authority and the Customer;
 - 1.5.3 set out the legal responsibilities which apply to disclosure and use of personal data having regard to the Data Protection Legislation;
 - 1.5.4 describe the data security protocols necessary to ensure compliance with Data Protection Legislation and any other specific security requirements;
 - 1.5.5 describe the process for managing Personal Data breaches.

2. Powers to Share Personal Data between the Parties

- 2.1 All information sharing must be compliant with legal obligations under Data Protection Legislation, any statutory data sharing powers and where relevant the Common Law Duty of Confidentiality.
- 2.2 The relevant legal bases to share information involving Personal Data between the Parties are set out below.
- 2.3 In addition to satisfying the conditions for processing data under the Data Protection Legislation there are a number of express powers and implied powers for sharing data between the Authority and the Customer:

Official Sensitive

- 2.3.1 Section 36 of the Immigration Act 2006 and Section 21 of the Immigration Act 1999 both allow for the sharing of information held by the Home Office in connection with the exercise of functions under any of the Immigration Acts.
- 2.3.2 Schedule 3, Nationality, Immigration and Asylum Act 2002 (NIAA) provides an express power for data sharing between the Authority and the Customer specifically within Paragraph 14;
- 2.3.3 Section 20 (as amended by sec. 55 of the IA 2016) of the Immigration Act 1999 provides for these bodies to share Personal Data with Home Office for 'immigration purposes' as listed in the legislation;
- 2.3.4 Immigration legislation will impact on NRPF assessments undertaken, the nature of said assessments and the level of support that can be provided. Cases such as N v Coventry (2008) provides an example of a situation where the immigration status of a NRPF family or individual is a prerequisite for the assessment process;
- 2.3.5 Housing support is granted under Section 193 of the Housing Act 1996, Part VII as amended by the Homelessness Act 2002 and the Localism Act 2011. Following review checks, which include immigration status checks, entitlement to public funds would end under Section 184 of the Housing Act 1996, Part VII as amended by the Homelessness Act 2002 and the Localism Act 2011;
- 2.3.6 Section 47 of the Children Act 1989 places a duty on local authorities to make enquiries where they have reasonable cause to suspect that a child may be at risk of suffering significant harm. It states that the following authorities must assist with these enquiries if requested to do so; any local authority; any local education authority; any housing authority; any health authority; any person authorised by the Secretary of State;
- 2.3.7 Part 3 of the Children Act 1989 allows for local authorities to provide various types of support for children and families. Section 17 provides a general duty of local authorities to provide services for children in need in their area;
- 2.3.8 Section 10 of the Children Act 2004 places a duty on each children's services authority to make arrangements to promote co-operation between itself and relevant partner agencies to improve the well-being of children in their area. The statutory guidance states that good information sharing is key to successful collaborative working and that arrangements under this section should ensure that information is shared for strategic planning purposes and to support effective service delivery. It also states that these arrangements should cover issues such as improving the understanding of the legal framework and developing better information sharing practice between and within organisations;
- 2.3.9 The Children (Leaving Care) Act 2000 aims to help young people who have been looked after by a local authority move from care to independent living. In regards to those with NRPF this duties can continue until 21 or 24 years of age.

Data sharing between the Authority and the Customer within the period of leaving care duties is essential for the Customer to establish eligibility for support specifically in respect of the current immigration status of a former looked-after child;

2.3.10 Section 55 of the Borders, Citizenship and Immigration Act 2009 stipulates that immigration functions are discharged having regards to the need to safeguard and promote the welfare of children. It is vital that the Authority is informed of instances where there are safeguarding concerns for children or any relevant circumstances where children are supported financially by the Customer whilst carrying out its duties;

2.3.11 In the judgement of *Clue v Birmingham City Council* (2010) the need for data sharing between local authorities and the Home Office was recognised as a condition for resolving cases expediently.

3. Lawful Bases for Processing Personal Data in Accordance with Article 6 of the GDPR

3.1 In accordance with Article 6 of the General Data Protection Regulation a lawful basis is required for disclosing, receiving and further processing the information for each Party.

3.2 The lawful bases for the processing of Personal Data are:

3.2.1 legal obligation;

3.2.2 public interest;

3.2.3 legitimate interest.

4. Privacy Information Notices

4.1 Each Party will ensure that their respective Privacy Information Notice is sufficiently detailed to cover the information sharing activity including the purpose of the processing and the lawful basis for the processing.

4.2 Once individuals engage with the Authority, they will receive a Personal Information Notice (PIN) when either applying for a visa, leave to remain, Asylum or when being served with a Red1 notice. Individuals also provide consent when first engaging with the Customer through a Conditions of Service (CoS) document

5. Third Party Processing

5.1 Should third parties be used to process any Personal Data the relevant Party must confirm that there are arrangements in place to ensure that the third party is compliant with Data Protection Legislation.

6. Data Protection Impact Assessment

6.1 The Parties will ensure that before any information sharing takes place in respect of this agreement that consideration is given as to whether a Data Protection Impact Assessment is required. This will help identify the relevant legal powers and assess the

benefits of the information sharing as well as identifying any privacy risks and how these might be mitigated.

- 6.2 The Authority has completed a Data Protection Impact Assessment in respect of the services provided by an on-site immigration official. The Authority has also completed a Data Protection Impact Assessment in respect of the utilisation of Connect.

7. Controller Status of the Receiving Parties

- 7.1 The Authority and the Customer will be joint controllers.

8. Purpose and Benefit of the Information Sharing

- 8.1 The purpose of data sharing between the Authority and the Customer is to facilitate the lawful exchange of data relating to the Customer's support provisions to individuals and families with no recourse to public funds (NRPF).
- 8.2 Joint working between the Authority and Customer is essential for resolving NRPF cases expediently. It is necessary to minimise the impact these cases have on the budgets of the Customer and the taxpayer.
- 8.3 The Customer's assessments and services for NRPF clients are dependent on knowing in detail a person's immigration status.
- 8.4 The sharing of data between the Authority and the Customer will ensure that outstanding immigration cases will be progressed as expediently as possible thus ensuring that the Customer can account for the associated costs to the taxpayer.
- 8.5 The information to be shared by the Authority and the Customer will be personal information about individuals with no recourse to public funds, including information about their dependants and will include sensitive personal data held by the Authority.
- 8.6 The sharing of information between the Authority and the Customer will enable the speedier resolution of cases thus saving the taxpayer money. It will help identify fraudulent claims. It will reduce the risk of poor case-working decisions being made where information is not being shared between the Authority and the Customer.
- 8.7 The Customer aims to reduce the timescales that NRPF cases remain supported by engaging with the Authority to resolve cases. The Authority can triage and prioritise cases based on factors such as the cost to the Customer or length of residence in the UK. The Customer can access real-time immigration status information from the Authority to ensure that cases are not being supported unlawfully or unnecessarily. The process will be expedited therefore saving time and money. The decision-making process will become more robust therefore ensuring the correct decision is made at the earliest opportunity. It will enable the identification of safeguarding issues.

9. Information to be Shared and the Systems the Information will be Derived from

- 9.1 The following type of Personal Data to be disclosed:

- 9.1.1 Name;

- 9.1.2 Date of Birth;
 - 9.1.3 Nationality;
 - 9.1.4 Address;
 - 9.1.5 Immigration Status;
 - 9.1.6 Family Details;
 - 9.1.7 Evidence of employment;
 - 9.1.8 Immigration history;
 - 9.1.9 Health concerns.
- 9.2 The Personal Data will be drawn from the following sources available to the Authority:
- 9.2.1 Case Information Database (CID);
 - 9.2.2 CRS;
 - 9.2.3 DVA;
 - 9.2.4 Home Office files;
 - 9.2.5 Atlas
- 9.3 The information is necessary, appropriate and relevant as an individual's personal circumstances are a prerequisite for the Customer to undertake assessments and thus comply with their legal obligations. The Authority must also be informed of cases where child protection proceedings are in place as this will be highly relevant to any immigration decision. The Authority will also advise the Customer when casework decisions have been made as this will impact upon decision-making processes in respect of the issuance of services.
- 9.4 The sharing of Personal Data will take place on a daily basis in accordance with the requirements of the Customer.

10. Type of Information Sharing Activity

- 10.1 The Authority and the Customer will partake in a regular information sharing activity.

11. FOIA Requests

- 11.1 Freedom of Information Requests are covered at Clause 17 in the main body of this agreement.

12. Subject Access Requests (SAR)

- 12.1 Individuals can request a copy of all the information that either Party holds on them, by making a SAR. This may include information that was disclosed to that Party under this

agreement. Where this is the case, as a matter of good practice, the Parties will liaise with each other to endeavour to ensure that the release of the information to the individual will not prejudice any ongoing investigation/proceedings.

13. Handling of Personal Data and Personal Data Security

- 13.1 Parties will be deemed to be Controllers (as defined in the Data Protection legislation) and as such must ensure that information shared that involves the sharing of personal data is handled and processed in accordance with the Data Protection legislation. Additionally, the Parties must process the information being shared in compliance with the mandatory requirements set by Her Majesty's Government Security Policy Framework ("HMG SPF") guidance issued by the Cabinet Office when handling, transferring, storing, accessing or destroying information assets.
- 13.2 The Parties will ensure effective measures are in place to protect information in their care and manage potential or actual incidents of loss of information. By way of example without limitation, such measures may include:
- 13.2.1 information not being transferred or stored on any type of portable device unless absolutely necessary, and if so, it must be encrypted and password protected to an approved standard;
 - 13.2.2 taking steps to ensure that all relevant staff are adequately trained and are aware of their responsibilities under the Data Protection legislation and this agreement;
 - 13.2.3 access to information received by the Parties pursuant to this MoU must be restricted to employees on a legitimate need-to-know basis, and with security clearance at the appropriate level; and
 - 13.2.4 the Parties will comply with the Government Security Classifications Policy (GSCP) where applicable:
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251480/Government-Security-Classifications-April-2014.pdf

14. Accuracy of the Shared Data

- 14.1 The parties will make reasonable endeavours to ensure that the information being shared is checked before disclosure for accuracy and relevance. The disclosing party will ensure data integrity. In the event that a party becomes aware of any inaccuracy or other defect in the information which has been disclosed it will notify the parties which disclosed the information.

15. Data Subject's Rights

- 15.1 Technical capability and procedures are in place to sufficiently comply with all the data subject's rights under the Data Protection Legislation. This includes the capability to identify, provide and erase personal data should either Party be legally required to do so.

16. Method of Information Sharing

- 16.1 Information will be exchanged between Parties in a secure approved format, as approved by all Parties.
- 16.2 Parties will ensure that all information they transmit to each other will be marked with the appropriate security classification in accordance with the GSCP.
- 16.3 The method of exchange will be in accordance with the standards and benchmarks relating to the security of that transfer and in accordance with any applicable provisions of the Data Protection legislation, Cabinet Office and other HMG guidance.
- 16.4 The movement of information must be captured and collated through the use of the NRPF Connect application which is accessible on the GCSX network. This ensures that data classified as Official can be shared securely. The Authority already has a separate data-sharing agreement with the NRPF network.
- 16.5 Should the NRPF Connect network not be available or not appropriate to the type of case, the sharing of data is subject to further data protection protocols. The Authority utilises the secure GSI Network to share data. The Customer should ensure the provision of GSI or GSX e-mail addresses to enable personal data to be shared securely.
- 16.6 If this is not feasible the Authority and the Customer should agree on a platform to ensure the secure sharing of data. Other options include the anonymising of data or if personal data has to be shared it should be encrypted using a secure data transfer method such as MoveIT.

17. Retention and Destruction Schedule

- 17.1 Information will be held in line with existing Authority retention and disposal policies.
- 17.2 Parties undertake to keep information being shared securely stored with access restricted to personnel authorised to access the information.
- 17.3 Parties will have documented policies on the retention and destruction of shared information in accordance with the requirements of the Data Protection legislation and HMG Security Policy Framework. Where specific information sharing activities are entered into by the Parties; the retention period should be jointly decided and set out in the respective agreement for that information sharing activity.
- 17.4 Where an agreement has been terminated, the Parties will follow any procedure set out in the agreement in relation to the handling of information. If no specific provisions are decided, the Parties will co-operate to determine how the information shared between the Parties is handled.
- 17.5 Parties will retain and securely destroy shared information according to their own internal retention/destruction program/schedule in line with the Data Protection legislation and in accordance with HMG Security Policy Framework guidance.

18. Permitted uses of the Information

18.1 Access to information will be restricted to authorised personnel from the Customer and the Authority who have:

18.1.1 the appropriate security clearance determined by their own organisation to handle the data (CTC for Authority employees), and

18.1.2 a genuine business need to access the information

19. Onward Disclosure to Third Parties

19.1 Parties will respect the confidentiality of the information being shared and will not disclose to third parties unless required to do so by law, or with the explicit consent of the other Party or as stipulated.

19.2 Unless otherwise stipulated within this agreement, any information shared as a result of this agreement, which then forms part of the permanent record of the receiving Party(s) becomes the responsibility of the receiving Party (s) under the terms of the Data Protection legislation.

19.2.1 Parties accept that the information shared as a result of this agreement may also be used to update their respective internal records. As Controller for that data, the receiving Party can onwardly disclose the information to third parties (this includes the sharing of Information with external contractors who are acting as Processors as on behalf of the Controller) subject to the following conditions being met

19.2.2 the Party wishing to make the onward disclosure must be satisfied that the information is only shared where it is necessary to carry out one of its own legitimate business functions and due regard must be had to any legal restrictions which may apply;

19.2.3 the Party wishing to make onward disclosure must be satisfied that the information is being shared lawfully and in accordance with any legal obligations that may apply, including those set out in the Data Protection legislation;

19.2.4 the Party wishing to make the onward disclosure must be satisfied that adequate security arrangements are in place for the transmission of the data to the receiving Party and that the receiving Party has adequate security arrangements in place for the secure storage of the information, and

19.2.5 where necessary a separate information sharing agreement should be put in place with the third-party organisation setting out all of the above.

20. Personal Data Breaches

20.1 A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss alteration, unauthorised disclosure of, or access to personal data transmitted stored or otherwise processed.

- 20.2 Examples of serious personal data breaches may include:
- 20.2.1 accidental loss or damage to the personal data;
 - 20.2.2 damage or loss of personal data by means of malicious software/hacking;
 - 20.2.3 deliberate or knowingly disclosure of personal data to a person not entitled to receive the data;
 - 20.2.4 emailing classified/sensitive information containing personal data to personal email accounts;
 - 20.2.5 leaving classified/sensitive papers containing personal data in a unsecure or publicly accessible area;
 - 20.2.6 using social networking sites to publish information containing personal data which may bring either Party's organisations into disrepute.
- 20.3 The designated points of contact (Appointed Officials) are responsible for notifying the other Party in writing in the event of personal data breach within 24 hours of the event.
- 20.4 The designated points of contact will discuss and jointly decide the next steps relating to the incident, taking specialist advice where appropriate. Such arrangements will include (but will not be limited to) containment of the incident and mitigation of any ongoing risk, recovery of the personal data, and assessing whether the Information Commissioner and/or the data subjects will be notified. The arrangements may vary in each case, depending on the sensitivity of the personal data and the nature of the loss or unauthorised disclosure.
- 20.5 Where appropriate, and if relevant to the incident, disciplinary misconduct action and/or criminal proceedings may be considered.

SCHEDULE 5 – MANAGEMENT INFORMATION AND PERFORMANCE

1. The template below will be utilised at the review meetings between the Appointed Officials to assess the performance of the Officer.

IE Checking and Advice Service – MoU Update Meeting

Date / Time of Meeting	
Partner Organisation	
Attendees	

MoU Monitoring – Delivery of Services

<p>OSIO Performance¹</p> <ul style="list-style-type: none"> • Current Caseload (+ / - since commencement of agreement or last meeting (whichever is more recent)) • Savings incurred (since commencement of agreement or last meeting (whichever is more recent)) • OSIO attendance and time-keeping • Strategic Influence 	
IT & Equipment ²	

¹ Provide update on Key Performance Indicators for period since last meeting and YtD update. Also provide update on OSIO behaviours

² Observations on IT in accordance with MoU monitoring

Official Sensitive

Actions to Take Forward	
-------------------------	--

Monthly Work Patterns ³	
OSIO Attendance Update ⁴	

Invoicing and Fees ⁵	
Signed Timesheets – Action Taken ⁶	

Contract Update ⁷	
Overall MoU Adherence – Y/N	

AOB	
-----	--

³ Update on Monthly Work Patterns – submission and adherence

⁴ Provide running total of days attendance v. MoU

⁵ Are fees and invoices up to date?

⁶ Timesheets to be signed and returned to IE Office for scan / e-mail

⁷ If meeting takes place within 3 months of contract expiry date discuss renewal and make form plans