NUAR Data Distribution Agreement

This Agreement is made between:

(1) The Cabinet Office (acting through the independent committee being part of the Cabinet Office, the Geospatial Commission) (**GC**);

(2) Neath Port Talbot County Borough Council, a local authority in England and Wales registered address is at Civic Centre Port Talbot SA13 1PJ (the **Data Provider**),

(each a **party** and together the **parties**).

Background:

(A) The GC through its Board of Commissioners is an impartial commission established by charter with responsibility for setting the UK's geospatial strategy and promoting the best use of geospatial data to drive productivity, promote economic growth, and improve the delivery of public services, while safeguarding considerations such as national security and intellectual property rights.

(B) The GC intends to co-ordinate (including through appointment of one or more third party suppliers responsible for provision of the NUAR Platform, Data transformation services, and/or associated services) the collecting, transforming, storing, and making available to third parties (subject to appropriate end user terms and acceptable usage policies) of datasets provided by data providers, including the Data Provider, for use in the NUAR Platform.

(C) The parties wish to enter into this Agreement to govern the Data Provider's provision of its Data for use on the NUAR Platform and the GC's co-ordination of the NUAR Platform as it relates to the Data Provider, including the distribution of that Data through the NUAR Platform to Licensees under a pre-agreed set of terms and conditions.

(D) The parties intend that this Agreement can continue without requiring variation irrespective of the replacement of any third party supplier responsible for provision of the NUAR Platform, Data transformation services, and/or associated services.

1 Definitions & interpretations

1.1 Appendix 1 provides for the definition and interpretation of words used in this Agreement.

1.2 In this Agreement:

1.2.1 any obligation on the GC to do something is to be interpreted as an obligation on the GC to do or to arrange for that thing to be done, including through one or more third party providers of the NUAR Platform, Data transformation services, and/or associated services; and

1.2.2 any obligation on the Data Provider to do something to or for the benefit of the GC is to be interpreted as an obligation on the Data Provider to engage with one or more third party providers of the NUAR Platform or the GC itself, Data transformation services, and/or associated services, as instructed by the GC and/or as set out in Appendix 4.

2 Term of this Agreement

2.1 In consideration of the mutual rights and obligations contained herein, this Agreement shall commence on the Commencement Date and shall continue until its termination in accordance with Clause 10.

3 Access to the Data

3.1 The Data Provider or any Data Provider Party shall deliver or make available to the GC, or a GC Party, the Data promptly following the Commencement Date and shall, thereafter, deliver or make available to the GC and/or a GC Party Data Updates.

3.2 The responsibility for transformation and ingestion of the Data shall be as set out in Appendix 4 (Data format and delivery requirements), as supplemented from time to time by such specific additional transformation and ingestion arrangements as may be agreed between the Data Provider and relevant third party providers of the NUAR Platform, Data transformation services, and/or associated services. Following transformation in accordance with those arrangements, the Transformed Data shall be delivered by or made available by the Data Provider for inclusion in the NUAR Platform in accordance with the arrangements set out in Appendix 4 (Data format and delivery requirements), as supplemented from time to time by such specific additional transformation and ingestion arrangements as may be agreed between the Data Provider and relevant third party providers of the NUAR Platform, Data transformation services, and/or associated services(but the delivery or availability of any Transformed Data under this Clause 3.2 shall not create an obligation for the GC to upload such Transformed Data into the NUAR Platform).

3.3 The management of Data and Transformed Data on the NUAR Platform, including the uploading and distributing of any Data and Transformed Data is subject to a separate agreement between the GC and a third party engaged for the delivery of the NUAR Platform.

3.4 Save to the extent expressly set out in this Agreement, the Data and the Transformed Data is provided without warranty or condition express or implied, statutory or otherwise as to its quality or fitness for purpose. All conditions, warranties, terms and undertakings express or implied, statutory or otherwise, in respect of the Data and the Transformed Data other than those expressly set out in this Agreement are hereby excluded to the fullest extent permitted by law.

4 The parties' obligations to each other

4.1 **The GC obligations**

4.1.1 The GC shall (and shall, where the context permits, ensure that GC Parties and Licensees shall):

a) not use Data for any illegal, deceptive, misleading or unethical purpose;

b) not (except as expressly licensed in this Agreement) reverse engineer, decompile, adapt, disassemble, modify, separate or otherwise tamper with the Data so that Data can be extracted and used for any purpose outside the scope of this Agreement;

c) be responsible for costs that it may incur in the performance of its obligations under this Agreement and for complying with all applicable laws, codes of practice and regulations (save that the GC may introduce a cost recovery model from the start of the fourth year of its contract with the primary third party provider of the NUAR Platform) pursuant to which it shall be entitled to levy charges on the Data Provider, subject to giving the Data Provider a minimum sixty (60) days' notice of the introduction of such charges);

d) conform with all relevant laws, rules and regulations governing the holding of data and the processing of personal data and privacy, including the Data Protection Act 2018;

e) not hold itself out or describe itself as the agent of the Data Provider or any Data Provider Party;

f) put in place the technological and security measures described in Appendix 3 to protect all Data which the Data Provider or any Data Provider Party provides to the GC from unauthorised use or access;

g) notify the Data Provider as soon as it suspects any (i) infringement of the Data Provider's IPR, or (ii) unauthorised access to the Data has taken place, and give the Data Provider all reasonably required assistance in pursuing any potential infringement or remedying any unauthorised access or use and take into consideration any reasonable proposal made by the Data Provider for dealing with any security incident; and

h) not use the Data other than for the purposes of exercising its rights and performing its obligations under this Agreement;

i) provide to the Data Provider access to regular reports providing information in respect of access to that Data Provider's Data through the NUAR Platform in the period before each such report, the contents of that report to be as set out in Appendix 3 Part 1.3.

4.2 **Data Provider obligations**

4.2.1 The Data Provider shall (and shall, where the context permits, ensure that Data Provider Parties shall):

a) comply with the data format and delivery requirements set out in Appendix 4, as supplemented from time to time by such specific additional transformation and ingestion arrangements as may be agreed between the Data Provider and relevant third party providers of the NUAR Platform, Data transformation services, and/or associated services;

b) exercise reasonable skill and care to ensure that Data delivered pursuant to this Agreement is accurate and up to date (and, as a minimum, of the same accuracy and currency as any data it currently provides for 'safe digging' purposes pursuant to any statutory or contractual obligation to which it is subject);

4.2.2 Where the Data Provider:

a) provides to the GC details of any person to whom the GC is to grant authorised user rights for the purposes of the Data Provider delivering Data, the Data Provider shall be responsible for the accuracy of all the details provided and the GC shall have no liability as a result of any inaccuracy of any details provided to it;

b) provides correct details of such persons referred to in Clause 4.2.2a) and the GC incorrectly records those details the GC shall, as soon as reasonably practicable, correct the information when advised of the inaccuracy and the GC shall be responsible for the consequences of such incorrect recording of such data.

4.3 **Bribery, corrupt gifts or payments**

4.3.1 The parties each warrant and undertake that they have not committed and will not commit in connection with this Agreement any offence under the Bribery Act 2010 or any other law in force in any applicable jurisdiction creating offences in respect of bribery, corruption and fraudulent acts.

4.3.2 Any breach of this Clause 4.3 by any party shall entitle the other party, with no liability whatsoever, to terminate this Agreement with immediate effect by notice in writing and to recover from the defaulting party the amount of any loss resulting from such termination.

4.4 **End User Licence**

4.4.1 The GC shall only make Data available under Clause 5.1 to Licensees that have first entered into an End User Licence with the GC.

4.5 **Relationship between the parties**

4.5.1 Nothing in this Agreement or its performance is intended to or shall give rise to, or establish, any relationship of agency, partnership, joint venture or employer and employee between the parties, nor authorise a party to make or enter into any commitments for or on behalf of the other party.

5 Licence

5.1 Subject to the terms of this Agreement the Data Provider grants to the GC and the GC Parties:

5.1.1 a non-exclusive, revocable, licence to:

a) transform (or permit a third party provider to transform) the Data to create the Transformed Data and thereafter submit the Transformed Data for the purpose of inclusion of the Transformed Data in the NUAR Platform (including in any additional 'value add' services made available through the NUAR Platform);

b) promote its transformation and supply of the Data by including sample 'snap shot' images created using Data in promotional materials provided that:

i) each such image is a raster image;

ii) each such image has a coverage area which is reasonable in order for the GC to illustrate its transformation or supply of the Data;

ii) each such image is not capable of being used as a service or product in itself; and
iii) the Data Provider provides its written approval of the nature and use of such image.

c) use and to sub-license to a third party provider of the NUAR Platform the Trade Marks solely as shown in Appendix 2 and solely for the purposes set out in this Agreement;

d) include the Transformed Data in the NUAR Platform for access by Licensees (including on a commercial basis for the purposes of offsetting the GC's costs);

e) grant non-exclusive, revocable, non-transferable sub-licences for access to the Data (in whole or in part) solely to Licensees for their Licensed Use provided that:

i) the Licensees' use of the Data shall be limited to creating User Generated Points or User Generated Polygons define an area of interest for underground assets and related infrastructure for a Licensed Use;

ii) Licensees may only view and query Data and consume a data feed within the extent of the User Generated Points or User Generated Polygons;

iii) Licensees shall not be permitted to extract Data from the NUAR Platform other than through such technical mechanisms for the production, display and export of Data forming part of the NUAR Platform; and

iv) in accordance with the GC's arrangements for the development of the NUAR Platform, the GC may from time to time give the Data Provider a minimum of sixty (60) days' written notice of additional licensed uses and/or additional categories of licensees, and the same shall apply automatically as Licensees and Licensed Uses from the end of that notice period.

5.2 The Data Provider agrees that the licences granted under Clause 5.1 shall not prevent the GC from providing feedback to any relevant Government departments in respect of the NUAR Platform.

5.3 The GC shall, and shall procure that no GC Parties shall use Data or the Trade Marks in any way or for any purpose other than as set out in this Clause 5.

5.4 Apart from the GC, GC Parties, the Data Provider and Data Provider Parties, and any third party provider of the NUAR Platform, no person, firm, or organisation (including without limitation any group company or affiliate) is granted any rights under this Agreement.

5.5 This Agreement does not give the GC any right to sublicense, distribute, sell or otherwise make Data or the Trade Marks available to third parties other than as permitted by Clauses 5.1.

6 Trade Marks, rights acknowledgement and branding

6.1 The Data Provider (or, where applicable, its licensors) owns the IPR in the Data and the Trade Marks. All rights not expressly granted are reserved to the Data Provider and its licensors and no transfer of ownership of IPR arises or is implied.

6.2 The GC shall ensure that in the NUAR Platform an appropriate acknowledgement is shown regarding the ownership of the Data and the Trade Marks, in accordance with any arrangements agreed between the parties.

7 Royalties

7.1 No royalties or other payments are payable under this Agreement.

8 Variation

8.1 A variation to this Agreement may be effected by agreement but only where in writing and signed by an authorised representative of each of the parties (other than a variation of Licensees or Licensed Uses referred to in Clause 5.1.1(e)(iv) which may be effected by the GC giving written notice).

9 Auditing

9.1 The GC shall (and shall procure that any third party provider of the NUAR Platform shall) maintain accurate and complete records (**Data Provider Records**) related to all transactions and supplies of Data arising out of this Agreement.

9.2 The GC shall (and shall procure that any third party provider of the NUAR Platform shall) allow the Data Provider, any Data Provider Party, or an auditor appointed by the Data Provider to access the Data Provider Records for as long as this Agreement is in existence and for a period of 12 months thereafter, provided that:

9.2.1 the purpose of such an audit of the Data Provider Records is solely for the purpose of auditing compliance with the terms of this Agreement, regulatory compliance and/or for the prevention and/or detection of crime;

9.2.2 access for the purpose of inspecting the Data Provider Records:

a) in the case of suspected fraud shall be on not less than one day's written notice at any time during normal business hours; and

b) in any other case not less than thirty days' written notice at any time during normal business hours; and

9.2.3 The GC shall (and shall procure that any third party provider of the NUAR Platform shall) provide the Data Provider, any Data Provider Party, or an auditor appointed by the Data Provider with all reasonable assistance in the carrying out of such audit. The Data Provider, Data Provider Party, and the auditor will ensure that any information obtained in the course of the audit concerning the GC's business is, subject to Clauses 14 and 15, kept confidential and not used for any purpose other than the proper conduct of the audit.

9.2.4 Each party shall bear its own costs in relation to the carrying out of such audit.

10 Termination and expiry

10.1 **General termination rights**

10.1.1 Either party may terminate this Agreement with immediate effect by giving the other party notice in writing in the event that the other party:

a) is in material breach of any term of this Agreement and such breach is either incapable of being remedied or is not remedied within thirty (30) days of a written request to do so;

b) repeatedly breaches any term of this Agreement in such a manner as to reasonably justify the opinion that its conduct is inconsistent with it having the intention or ability to give effect to the terms of this Agreement;

c) ceases to carry on business (and, in the case of the GC, has not previously transferred and does not transfer this Agreement in accordance with Clause 16.1);

d) discloses Confidential Information of the terminating party otherwise than in accordance with this Agreement; or

e) materially alters the nature of its business.

10.2 **Mutual termination rights**

10.2.1 Any party may terminate this Agreement at any time by giving the other parties thirty (30) days' written notice.

10.3 **The Data Provider's termination rights**

10.3.1 The Data Provider may terminate this Agreement with immediate effect by giving the GC notice in the event that the GC, or a GC Party uses or authorises the use of the Data Provider's IPR in the Data outside the scope permitted by this Agreement.

10.4 **Effects of termination or expiry of this Agreement**

10.4.1 If this Agreement is terminated or expires:

a) any accrued rights and remedies will not be affected;

b) the GC shall and shall procure that the GC Parties and each Licensee shall (unless they are able to enter into a separate licence with the Data Provider) immediately cease to have access to any Data no longer available on the NUAR Platform as a result of that termination or expiry, other than to the extent in the case of the GC Parties that further access to that Data is necessary for effective audit of use of the NUAR Platform and compliance with this Agreement; and

c) the GC shall, and shall procure that the GC Parties shall (unless they are able to enter into a separate licence with the Data Provider) cease to make available the Data through the NUAR Platform within thirty (30) days.

10.4.2 The provisions of this Agreement intended to survive termination or expiry, including Clauses 1, 4.1.1(a), (c), (e) and (f), 4.3, 4.5, 8.1, 10.4, 12, 14 to 18, 20 and 21 shall continue in full force and effect, notwithstanding such termination or expiry.

11 Warranties and Indemnity

11.1 The Data Provider warrants to the GC that:

11.1.1 it has the authority to enter into this Agreement; and

11.1.2 it has the authority and power to grant the rights set out in this Agreement.

11.2 The Data Provider excludes, to the fullest extent permissible by law all implied or express warranties, except those stated in this Clause 11.

11.3 Subject to Clauses 11.4, 12.2, 12.3, and 12.4:

11.3.1 the GC shall indemnify the Data Provider and keep it indemnified against all costs, expenses, damages, losses or liabilities incurred or suffered by it arising from any breach by the GC of the Data Provider's IPR in the Data provided that the GC shall not have any liability for any infringing IPR in the Transformed Data or for any infringement arising from the presence of such infringing IPR, to the extent such infringing IPR was provided to the GC by the Data Provider;

11.3.2 the Data Provider shall indemnify the GC and keep it indemnified from and against all costs, expenses, damages, losses or liabilities incurred or suffered by it arising out of any claim that the GC has infringed the IPR of any third party by using the Data in accordance with this Agreement.

11.4 Wherever a party is indemnified under this Agreement, that party shall:

11.4.1 promptly notify the other party (**Indemnifier**) in writing as soon as it becomes aware of any matter which may be subject to the relevant indemnity;

11.4.2 make no admission relating to the matter which is the subject of the indemnity without the Indemnifier's prior written consent;

11.4.3 allow the Indemnifier to conduct and settle all negotiations and proceedings and give the Indemnifier all reasonable assistance (at the Indemnifier's reasonable expense); and

11.4.4 use reasonable endeavours to mitigate its losses.

12 Liabilities

12.1 Nothing in this Agreement shall exclude or limit either party's liability for:

12.1.1 death or personal injury to the extent it results from its negligence, or that of its employees or agents; or

12.1.2 fraud or fraudulent misrepresentation.

12.2 No party will be liable to the other in contract, tort (including negligence) or otherwise for any loss of profits, loss of business or loss of contracts (in each case whether direct or indirect) or for any special, indirect or consequential losses or damages.

12.3 Subject to Clauses 12.1 to 12.2, the GC's maximum aggregate liability, whether in contract, tort (including negligence), under any indemnity, or otherwise arising out of or in connection with this Agreement to all providers of data to the NUAR Platform (including the Data Provider) in the local authority / government, and transport sectors in any Financial Year will not exceed an amount equal to GBP one million five hundred thousand (£1,500,000).

12.4 Subject to Clauses 12.1 to 12.2, the Data Provider's maximum aggregate liability, whether in contract, tort (including negligence) or otherwise arising out of or in connection with this Agreement will not exceed GBP thirty five thousand (£35,000).

13 Events outside a party's control

13.1 Neither party will be responsible, nor in breach of this Agreement, for any delay or failure in carrying out obligations under this Agreement if the delay or failure is caused by circumstances beyond the reasonable control of the affected party. In such circumstances the affected party will notify the other party of any such likelihood as soon as possible and, where possible, indicate for how long that party is likely to be delayed. The affected party shall be allowed a reasonable extension of time to carry out its obligations in these circumstances.

14 Confidentiality

14.1 Subject to Clause 15, each party agrees:

14.1.1 to use Confidential Information of the other party only for the purposes of discussions between the parties relating to their business relationship, and for performing obligations and exercising rights granted under this Agreement;

14.1.2 to keep all Confidential Information secure, and to disclose it only to those employees, consultants, directors and professional advisers who need to know such Confidential Information and who are subject to at least the same obligations of confidentiality as those set out in this Clause 14;

14.1.3 to notify the other party without delay of any unauthorised use, copying or disclosure of the other party's Confidential Information of which it becomes aware and provide all reasonable assistance to the other party to stop such unauthorised use, copying and/or disclosure; and

14.1.4 except as required by law, any order of a court of competent jurisdiction or by governmental or regulatory requirements (which shall include any requirements for disclosure under the *Freedom of Information Act 2000* and/or the *Environmental Information Regulations 2004*), not to disclose Confidential Information to any third parties unless expressly permitted under this Clause 14 or with the other's prior written consent.

14.2 The obligations in this Clause 14 do not apply to any information which is in the public domain (other than through the breach of any obligation of confidentiality) or which a party can demonstrate was previously known to it (unless acquired directly from the other party or in breach of any obligation of confidentiality) or was independently developed by it without the use of any Confidential Information.

15 Freedom of Information

15.1 The parties acknowledge that each Impacted Party:

15.1.1 is subject to the requirements of the FOI Legislation and agrees to assist and cooperate with any Impacted Party to enable the Impacted Party to comply with its obligations under the FOI Legislation relevant to the NUAR Platform where applicable; and

15.1.2 may be obliged under the FOI Legislation to disclose Information without consulting or obtaining consent from the other party but that it shall take reasonable steps to notify the other party of the Information Access Request (in accordance with the Cabinet Office's Freedom of Information Code of Practice issued under section 45 of the Freedom of Information Act 2000) to the extent that it is permissible and reasonably practical for it to do so.

15.2 Without prejudice to the generality of the above, the parties shall, and shall procure that the GC Parties or Data Provider Parties (as relevant) shall:

15.2.1 transfer to the Impacted Party's project lead (or such other person as may be notified by the Impacted Party to the other party) each Information Access Request relevant to the NUAR Platform that it or they (as the case may be) receive as soon as practicable and in any event within five (5) Business Days of receiving such Information Access Request, where applicable; and

15.2.2 in relation to Information held by any party on behalf of an Impacted Party, provide the Impacted Party with details about and copies of all such Information that the Impacted Party requests and such details and copies shall be provided within five (5) Business Days of a request from the Impacted Party (or such other period as the Impacted Party may reasonably specify), and in such forms as the Impacted Party may reasonably specify.

15.3 Each Impacted Party shall be responsible for determining in its absolute discretion whether Information is exempt information under the FOI Legislation and for determining what Information will be disclosed in response to an Information Access Request made to it in accordance with the FOI Legislation. The parties shall not respond to any person making an Information Access Request, save to acknowledge receipt, unless expressly authorised to do so by the relevant Impacted Party.

16 Assignment, subcontracting and sublicensing

16.1 Except as provided in this Agreement, or as otherwise agreed from time to time, no party may assign, subcontract or sublicense their rights and obligations under this Agreement without the prior written consent of the other party, such consent not to be unreasonably withheld or delayed.

16.2 The GC may novate, assign, subcontract, sublicense or otherwise transfer its rights and obligations under this Agreement to any other public sector body (including any public corporation or other similar body) in the UK by giving at least sixty (60) days' notice in writing to the other party.

17 Entire agreement

17.1 This Agreement and any documents referred to in it constitute the entire agreement and understanding between the parties concerning its subject matter and replaces any previous such agreement (including any previously executed distribution agreement).

18 Waiver

18.1 The waiver on a particular occasion by either party of rights under this Agreement does not imply that other rights will be waived.

18.2 No delay in exercising any right under this Agreement shall constitute a waiver of such right.

19 Notices

19.1 Any Dispute Notice under this Agreement shall be in writing and delivered by hand or prepaid recorded delivery or first class post addressed to the recipient at its registered office (or such other address as notified to the other party in writing). Any other notice under this Agreement shall be in writing (including email) and shall be delivered by hand or prepaid recorded delivery or first class post addressed to the recipient at its registered office (or such other address as notified to the other party in writing) or by email to the following named individuals for each party at the email address set out below:

19.1.1 In the case of GC: [Onboarding Lead]

Email: [nuar-onboarding@cabinetoffice.gov.uk], cc'd to [nuar@cabinetoffice.gov.uk]

In the case of the Data Provider: [Head of Legal and Democratic Services]

Email: [c.griffiths2@npt.gov.uk, cc'd to m.roberts@npt.gov.uk]

or such other contact details as either party shall notify to the other in writing. Notices shall be deemed to have been received:

a) if delivered by recorded first class post, two (2) Business Days after the notice was posted;

b) if delivered by hand, on the next Business Day after delivery; or

c) if delivered by email (communications and invoices only), at the time of sending or if such email is sent after 17:00 on a Business Day, at 09:00 on the next Business Day.

20 Contracts (Rights of Third Parties) Act 1999

20.1 A person who is not a party to this Agreement has no right under the Contracts (Rights of Third Parties) Act 1999 to enforce or enjoy the benefit of any term of this Agreement.

21 Disputes, jurisdiction and governing law

21.1 The parties shall use all reasonable endeavours to negotiate in good faith and settle any dispute or difference that may arise out of or relate to the Agreement ("**Dispute**") before resorting to litigation.

21.2 If the Dispute is not settled through discussion between representatives of the parties within a period of seven (7) Business Days of the date on which the Dispute arose, the parties may refer the Dispute in writing to a director or chief executive (or equivalent) ("**Senior Personnel**") of each of the parties for resolution.

21.3 If the Dispute is not resolved within 14 Business Days of referral to the Senior Personnel, the parties in dispute shall attempt in good faith to resolve the Dispute through entry into a structured mediation or negotiation with the assistance of a mediator. Either relevant party may give notice to the other party ("**Dispute Notice**") to commence such process and the Notice shall identify one or more proposed mediators.

21.4 If the parties are unable to agree on a mediator, or if the agreed mediator is unable or unwilling to act within 28 Business Days of the service of the Dispute Notice, either of the parties may apply to the Centre for Effective Dispute Resolution ("**CEDR**") in London to appoint a mediator. The costs of that mediator shall be divided equally between the parties or as those parties may otherwise agree in writing.

21.5 Where a dispute is referred to mediation under Clause 21.3, the parties will attempt to settle such Dispute by mediation in accordance with the model mediation procedures published by CEDR or such other procedures as the mediator may recommend.

21.6 If the parties reach agreement on the resolution of the Dispute, such agreement shall be recorded in writing and once signed by the parties' authorised representatives, shall be final and binding on the relevant parties.

21.7 If either of the parties refuses at any time to participate in the mediation procedure and in any event if the parties fail to reach agreement on the Dispute within 40 Business Days of the service of the Dispute Notice either of the parties may commence proceedings in accordance with Clause 21.10.

21.8 The parties shall continue to perform their obligations under this Agreement without delay or disruption while any Dispute is being resolved pursuant to this Clause 21.

21.9 No party shall be prevented from, or delayed in, seeking any order for specific performance or for interim or final injunctive relief as a result of the provisions of this Clause 21 and the requirements of this Clause 21 shall not apply in respect of any circumstances where such remedies are sought.

21.10 This Agreement shall be governed by and construed in accordance with English law. Without prejudice to this Clause 21, the parties submit to the exclusive jurisdiction of the English courts.

22 Signing

Signed for and on behalf of **Geospatial Commission**

Signature

Name

Title

Date

Signed for and on behalf of [***insert name of Data Provider***]

Signature

Name Michael Roberts

Title Head of Streetcare

Date 25th April 2022

Appendix 1 Definitions & interpretation

1.1 In this Agreement:

Expression	Meaning
Agreement	means this agreement (as amended or replaced from time to time in accordance with its terms)
Business Day	means any day excluding Saturdays, Sundays and bank holidays when banks are open for business in England
CEDR	has the meaning given to it in Clause 21.4
Commencement Date	means the date upon which an authorised representative of the last party to sign this Agreement does so
Confidential Information	means any information that is marked or identified as confidential, or that would reasonably be considered to be confidential in nature, that relates to the affairs of a party and is acquired by the other party in anticipation of or as a result of this Agreement
Contractor	means a third party that is granted written permission by a Licensee to access the NUAR Platform solely for the purposes of that Licensee's Licensed Use;
Data	means any information or datasets provided by any Data Provider for the purposes of participation in the NUAR Platform project and includes, as the context permits, Transformed Data and Data Updates
Data Provider Party	means any party who provides any information or datasets on behalf of the Data Provider for the purposes of participating in the NUAR Platform project and is listed as such in Appendix 6.
Data Updates	means updates, revisions and modifications to the Data that the Data Provider may provide (or provide access to) from time to time
Dispute	has the meaning given to it in Clause 21.1
Dispute Notice	has the meaning given to it in Clause 21.3
End User Licence	means a written licence to be click-accepted via the NUAR Platform pursuant to which a Licensee agrees to use the Data for its Licensed Use
Financial Year	means the period from 01 April in one year to 31 March in the following year.
FOI Legislation	means the Freedom of Information Act 2000, all regulations made under it and the Environmental Information Regulations 2004 and any amendment or re-enactment of any of them; and any guidance or statutory codes of practice issued by the Information Commissioner, the Ministry for Justice, or the Department of Environment Food and Rural Affairs (including in each case its successors or assigns) in relation to such legislation
Geospatial Commission or **GC**	means the government body of that name with responsibility for commissioning the NUAR Platform
GC Party	means the GC's agents, contractors and sub-contractors of any tier and their directors, officers, employees and workers engaged in relation to the NUAR Platform project and the **GC Parties** shall be construed accordingly
Impacted Party	means a party which is affected by a claim under the FOI Legislation
Indemnifier	has the meaning given to it in Clause 11.4.1
Information	means information recorded in any form held by an Impacted Party or by the parties on behalf of an Impacted Party
Information Access Request	means a request for any Information under the FOI Legislation
IPR	means intellectual property rights, including copyright, patent, trade mark, design right, database rights, trade secrets, know how, rights of confidence and all other similar rights

anywhere in the world whether or not registered and including applications for registration of any of them

Landowner means the owner of land to which Data relates;

Licensed Use means a Licensee's use of the Data for the purposes of:

a) in respect of any Licensee other than the Data Provider and / or the GC:

i) safe digging, on-site efficiency, site planning, survey, ground investigation, data exchange, co-ordination, the avoidance of utility strikes and undertaking statutory duties in respect to the design, construction, maintenance, operation or improvement of underground assets under sections 79-82 of the New Roads and Street Works Act 1991; and / or

ii) carrying out safe working practices under the Health & Safety at Work etc. Act 1974; and / or

iii) any other rights that may be granted by the Data Provider to the Licensee in conjunction with the Licensee access to the NUAR Platform; and/or

iv) any other of the 'Licensed Use Examples' set out in Appendix 5; and/or

v) any use notified by the GC pursuant to Clause 5.1.1(e)(v);

b) in respect of the Data Provider and / or the GC only, informing the future roll-out of the NUAR Platform on a national basis

Licensee means:

a) any employee of a Statutory Undertaker that is authorised by such Statutory Undertaker to access Data for its Licensed Use;

b) any employee of a local authority that is authorised by that local authority to access Data for its Licensed Use;

c) any employee of a Data Provider that is authorised by that Data Provider to access Data for its Licensed Use;

d) any Contractor(s) engaged and authorised by a Statutory Undertaker, local authority, central government and central government agencies or Data Provider;

e) the GC and the GC Parties; who have agreed to the terms of access of the NUAR Platform;

NUAR Platform means National Underground Asset Register, a digital platform being developed by the GC that will allow Licensee's to view Data Providers' underground assets in accordance with an End User Licence

Senior Personnel has the meaning given to it in Clause 21.2

Statutory Undertaker means an organisation that operates within the United Kingdom, that is deemed to be a statutory undertaker under relevant legislation, which may include utility surveyors, landowners, water suppliers, electricity suppliers, gas suppliers, telecoms suppliers and authorities responsible for sewers

Trade Marks means the trade marks shown in Appendix 2

Transformed Data means Data that has been transformed into a form that can be uploaded onto the NUAR Platform

User Generated Points means a point selected by the Licensee within the Data with a buffer zone radius of up to 250 metres

User Generated Polygons means a polygon drawn by the Licensee within the Data

Utility Surveyor means a person holding an accreditation as a professional utility survey practitioner.

1.2 In this Agreement, unless the context otherwise requires:

1.2.1 headings are inserted for convenience only and shall not affect the interpretation of any provision of this Agreement;

1.2.2 words in the singular include the plural and vice versa;

1.2.3 references to:

a) a Clause or an Appendix are to a Clause or Appendix of these terms and conditions; and

b) a statute or statutory provision include any amendment, extension or re-enactment of such statute or provision;

1.2.4 reference to legislation or a legislative provision is a reference to it as amended, extended or re-enacted from time to time;

1.2.5 a reference to **writing** or **written** includes email but not fax;

1.2.6 any words following the terms **including**, **include**, **in particular**, **for example** or any other similar expression shall be construed as illustrative and shall not limit the sense of the words, description, definition, phrase or terms preceding those terms.

Appendix 2 The Data Provider's Trade Marks

[TRADE MARKS PROVIDED WILL BE INSERTED HERE]

Appendix 3 Technological and security measures

The GC shall put in place the following arrangements in respect of the NUAR Platform in order that its fundamental design is "Secure by Default"[1]

The GC shall have in place an appropriate security controls document with any third party supplier of the NUAR Platform covering the following topics at a minimum.

Any changes must align with best practice security guidelines and GC governance processes with Data Providers notified

1. Access Control

Access to the platform and underlying data shall be subject to access control, with access levels determined by the user's organisation, role and business needs.

1.1. Access to Services

- Access must be based on the principle of least privilege dictated by role
- Privileged access to the system must be subject to privileged access management processes to ensure that privileged access is secure, audited and role- and time-limited
- The system must only expose explicitly authorised data to authorised end users
- The system must not allow direct communication between end users and back-end resources
- The system must be able to restrict access to users from specific geographics locations

1.2. Password Management and Complexity

- Passwords must be distributed separately from their associated user ID
- Passwords must only be reset where the identity of the individual has been identified
- Initial password values and reset password values must be unique
- A password change must take place on first logon for initial or reset passwords
- Passwords must be changed at a minimum agreed interval, which may be shorter for accounts with privileged access
- Passwords must be stored using one-way encryption and separately from other system data
- Password storage access must be restricted to appropriately privileged users only
- The system must not display or output passwords in clear text at any time
- Autocomplete of password fields must be disabled
- Passwords must follow industry best practice for minimum length and complexity and for disallowed content

1.3. Account Management

- All login credentials must be unique to individual users
- User IDs must be a minimum length in line with industry best practice
- Any previously used user IDs must not be reused
- Login screens must only present the minimum amount of information required for access authentication
- User login validation must only take place once all of the user information has been input
- Authorised users must be authenticated using multi-factor authentication (MFA). It is desirable that the device used for MFA is not the same device on which the user is using the platform
- Login failures must not result in the disclosure of any detailed system or user information
- Accounts must be reviewed at agreed intervals to confirm their requirement is still valid
- Accounts must be disabled in a timely manner once they are no longer required and immediately if any misuse is suspected
- User audit trails must be retained even if the user account is disabled and organisations will have access to details of searches and enquiries, which contain their organisation's assets, and confirmation of acceptance of the Platform Terms and Conditions

1.4. Account Lockout

- User sessions must be terminated after an agreed period of inactivity and all protected information removed from the screen
- Users must be limited to a single session

[1] https://www.ncsc.gov.uk/information/secure-default

- User IDs must be locked out following a defined number of failed logon attempts, and failed logon attempts must be recorded.

2. Communication Security
   2.1. Information Transfer
   - All data in transit (including cookies) must be encrypted to a secure standard (TLS 1.2 minimum)
   - HTTPS content caching must be disabled
   - System responses must not include version information about the web server components
   - Any data transferred into the system must be validated for conformance against expected parameters

   2.2. Network Security
   - Any internet-facing services must be protected by at least a layer seven Web Application Firewall appropriately configured with Allow/Deny listings and port access rules
   - The system must be protected from a DDoS style attack with upstream protection and graceful degradation built in[2]
   - Any internet-facing forms must be protected by a server-side validated CAPTCHA and must validate expected input before submission
   - All servers must have host-based firewalls enabled and be configured for least privilege

   2.3. Ingestion of External APIs
   - Recommendations for the ingestion of external APIs, including additional Security Controls for the system, and security recommendations for the external element of any API ingestion subsystem are supplied in Appendix I[3]

3. Cryptography
   3.1. Cryptographic Controls
   - Cryptographic keys must be in line with industry best practice (minimum 256 bits for symmetric keys and 2048 bits for Asymmetric keys)
   - Cryptographic keys must be protected against modification and loss
   - Minimum standards must be defined for ciphers, protocols and hashing algorithms
   - A recognised library must be used for cryptography algorithms
   - Private keys must be transferred securely between components (minimum of AES 256)

   3.2. Certificate Management
   - Certificates used for redundancy must have different expiry dates
   - Internally signed certificates must be capable of being revoked
   - A cloud Hardware Security Module provisioned separately from the main system must be used for the storage of certificates

4. Operations
   4.1. Logging and Monitoring
   - All log events must:
     - include timestamps in a form that ensures consistency across time zones
     - be retained for an agreed minimum period
     - be generated at all levels of operation (e.g. operating system, database, application)
   - Logs must be stored separately to other system data and subject to regular monitoring (it must be possible to forward all logs to a central logging platform for security monitoring)
   - Logs must be protected by strong authentication and privileged access management controls. Privileged access management should be used to constrain privileged user access.
   - Logs should be centralised to allow for proficient security monitoring and response, and secured with appropriate security controls such as firewalls to stop attackers from pivoting into this part of the system.

[2] https://www.ncsc.gov.uk/collection/denial-service-dos-guidance-collection/preparing-denial-service-dos-attacks1

[3] https://docs.google.com/document/d/1qinRbpH3GBO1qt-wpH3QIa_Y-TqZxvASk7l16iBwEO8/edit?usp=sharing

4.2. Protection from Malware and Technical Vulnerability Management

- All components in the system must be protected against malware and malicious software[4]
- Any data received into the system must be scanned for malware and malicious code
- Subsystems allowing the import of new data into the system should be segregated from other components to allow separate, isolated scanning and diagnosis of incoming data
- Anti-malware software should be updated as soon as practicable after an update becomes available
- System components should be separated by firewalls and VLANs where practicable to restrict the spread of breaches or infections
- The system must be scanned for vulnerabilities on a monthly basis
- Critical and High rated patches must be applied as soon as practicable after the patch has been released by the vendor
- Application of patches should be managed to ensure that all patches are not applied at the same time to avoid negative impact on the system

4.3. Security Breaches and Near Misses

- Reporting processes must be defined
- Handling and investigation processes must be defined

4.4. End User Device Security

- Requirements and recommendations for end user device security must be defined and agreed with End User organisations
- Role-based access and principle of least privilege, as referenced elsewhere, should be used to mitigate end user device risks
- Security standards for end user devices should be defined as part of acceptable use terms

5. System Acquisition, Development and Maintenance

5.1. System Security Requirements

- All data at rest must be encrypted to an agreed secure standard in line with industry best practice
- All system data must be hosted within the United Kingdom
- Any operating system must be built to industry best practice methods and security configurations
- The system must not be vulnerable to the OWASP Top 10 vulnerabilities[5]

5.2. Assurance

- There must be regular reviews of security requirements, audit requirements and system architecture
- There must be regular penetration testing of the system by a CHECK approved provider. Penetration testing must be carried out at least annually, and after significant changes which may impact security.

6. Personnel Security

6.1. Personnel Security Requirements

- Role-based security clearance requirements will be defined for Supplier and End User personnel

6.2. Security training and awareness requirements will be defined, including recommendations and standards for security-minded communication in all project communications.

[4] https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks

[5] https://owasp.org/www-project-top-ten/

Appendix 4 Data Format and Delivery Requirements

Asset owners agree to provide as a minimum data format and delivery conformance requirement:

- 2D geometry information which allows each feature to be located and visualised on a map within the UK
- Metadata which allows the owner/operator of each feature to be identified and the coverage of their supplied data
- Data updated, or confirmed to be up to date, at least every 3 months

Appendix 5 Licensed Use Examples

These examples are for illustrative purposes only and do not constitute an exhaustive list of all future cases, nor are they complete or certain to feature in the NUAR Platform.

Use case	**User needs**	**Reason**	**Additional data required**
Coordination of streetworks	*Asset owners* / *local authorities* need to have access to all available underground asset data, maintenance plans and to integrate with street works registers	So to better coordinate streetworks for utility maintenance, leading to less overall disruption	Utility maintenance programmes referenced to XY coordinates (and other linked identifiers)
Aligning with street works notifications	*Asset owners* / *local authorities* need to make sure that the execution of works is a single process for the asset owners	So to remove duplication and rework in the process of notifying and agreeing execution for works particularly in complex environments	Street works notifications systems data
Emergency response	*Emergency responders* need to access up to date underground asset data live	So to better understand an emergency involving utility assets and can take immediate informed action	Risk assessments, environmental data, relevant above ground info (land use etc), UxO.
Flood risk planning	*Government planners* need to integrate location and condition of subsurface waterways (sewers, culverts) with environmental data and current flood protection	So to understand and have a holistic view of the entire urban environment to better plan for and mitigate flood events	Variety of data, including environmental (Met Office, EA, BGS, SUDS), government (Resilience Direct) and more
Subsurface Infrastructure development	*Designers and Engineers* need access to up-to-date buried infrastructure and geotechnical data to optimise routes of tunnels and design of basements/foundations	So to have the best available information to reduce construction costs and optimise site investigations	Data on housing stock, basement depths, foundation types (partly through the planning portals) BGS data (geology, hydrogeology, boreholes) other buried infrastructure (service tunnels)

Appendix 6 – Data Provider Parties

[Insert]