

Secure Data Environment (SDE) Registration Agreement

Between:

- (1) **Sussex Partnership NHS Foundation Trust**, whose registered office is at Swandean, Arundel Road, Worthing, West Sussex, BN13 3EP (the **Registration Organisation**) and
 - (2) **[FULL NAME OF USER ORGANISATION]** whose registered office is at **[INSERT REGISTERED OFFICE ADDRESS]** (the **User Organisation**)
- (each 'Party' and together 'Parties')

Registration for:

SECURE DATA ENVIRONMENT (SDE) NETWORK

Scope

This Agreement is intended for use where a User Organisation wishes to be registered to gain access to the Secure Data Environment (**SDE**) Network, pending submission of a successful project specific data access request. Once a User Organisation is registered by the Registration Organisation for one SDE, it will be registered across all of the SDE Network, and will be entered onto the SDE Network Registered User Register. This Agreement identifies the minimum requirements for registration and entry onto the Registered User Register. The SDE Network has entered into a collaboration agreement and formed a registration committee to guide and facilitate the registration process. The Registration Organisation exercises its functions under this Agreement pursuant to, and subject to, the SDE Network-wide Registration governance arrangements and nothing in this Agreement is intended to undermine or contradict the operation of those arrangements.

Purpose and benefits of Registration:

The User Organisation Registration Process benefits User Organisations by allowing them to submit certain information to the SDE Network once only. By completing Registration and being entered onto the Registered User Register, User Organisations reduce the administrative burden at the point of making a project specific data access request to any SDE within the SDE Network. The SDEs within the SDE Network are reliant on User Organisations being registered when a project specific data access request is made and during the period of access. They therefore have an interest in ensuring that User Organisations remain compliant with this Agreement. The process also enables User Organisations to vouch for users who, once approved via the Approved User Registration Process, can then submit data access request forms in respect of potential projects and, pending a successful project specific data access request, be granted access to data within an SDE. The terms applicable to Registration are set out in Part A of the Terms below.

Registration also allows User Organisations and Approved Users access to the discovery tool (**Discovery Tool**), to permit high level feasibility questions to be submitted to individual SDEs. The terms applicable to the Discovery Tool access are set out in Part B of the Terms below. It should be noted that:

- a) the Data made available to the User Organisation in the Discovery Tool does not include Personal Data when in the hands of the User Organisation, however this Agreement is part of the SDE's overall "Five Safes" implementation and the contractual controls contained herein help to render the Data as anonymised. While Data is to be treated as anonymised for access purposes, it may still give rise to information governance and re-identification risk; and
- b) any subsequent access to data in the SDE shall be conditional on the User Organisation entering into a separate Data Access Agreement (**DAA**) on a project-specific basis, and the parties must enter into a project-specific DAA before any work on any project can be commenced.

Registration requirements:

This Agreement therefore sets out specific obligations on User Organisations to:

- Complete the User Organisation Registration Process, which will require the User Organisation to confirm that it has suitable policies in place to enable good practice, for example in the areas of confidentiality, data protection, and staff training. User Organisations will be required to confirm that all information provided as part of the User Organisation Registration Process is correct.
- Once the User Organisation has been registered, it will be entered onto the Registered User Register. There are ongoing obligations on the User Organisation to keep the SDE Network up to date and to notify it of any significant changes. The User Organisation will have to

undertake subsequent reconfirmation activities as required by the SDE Network from time to time and at least annually.

- Procure that proposed Approved Users complete the Approved User Registration Process, and be accountable for the accuracy of all information provided. This includes providing assurance that minimum requirements have been met in relation to those Approved Users and periodically auditing those users.
- Take responsibility for all information provided by the User Organisation and the Approved Users during the respective Registration processes and accept liability for any discrepancies found.
- Comply, and procure that (where applicable), any Approved Users comply, with the terms governing access to the Discovery Tool.

Terms

In consideration of £1, of which the Registration Organisation hereby acknowledges receipt:


- (1) the User Organisation shall comply with the Registration Terms at Part A below and any additional terms applicable to Registration in this Agreement;
- (2) where the User Organisation wishes to procure access to the Discovery Tool for its Approved Users, it shall comply and shall ensure that the Approved Users comply with the Discovery Tool access Terms at Part B below, and any additional terms applicable to access to and use of the Discovery Tool in this Agreement; and
- (3) the User Organisation acknowledges that the Registration Organisation's rights under this Agreement may be enforced by any organisation hosting an SDE within the SDE Network as constituted from time to time pursuant to the Contracts (Rights of Third Parties) Act 1999. If the Registration Organisation is replaced by another SDE which assumes responsibility for Registration, the User Organisation acknowledges that this Agreement may be novated to the new organisation but otherwise the Agreement shall continue in full force and effect and may be enforced by the new organisation pursuant to the Contracts (Rights of Third Parties) Act 1999.

Part A: Registration Terms

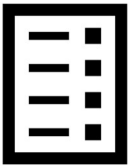
1. Registration	<p>1.1 The User Organisation shall:</p> <p>1.1.1 Complete the User Organisation Registration Process; and</p> <p>1.1.2 ensure Approved User(s) complete the Approved User Registration Process and vouch for each Approved User.</p> <p>1.2 The User Organisation shall be responsible for reviewing, ensuring the completeness and accuracy of and submitting the Application on behalf of (i) itself and (ii) each Approved User.</p> <p>1.3 The User Organisation warrants that:</p> <p>1.3.1 all answers provided in response to the User Organisation Registration Process and the Approved User Registration Process are true and complete and, without prejudice to the provisions at clauses 1.3.2 and 1.3.3, shall remain so for the duration of this Agreement;</p>
------------------------	---



	<p>1.3.2 it shall notify the Registration Organisation promptly, and in any event within 5 working days, of any changes to answers submitted in response to (i) the User Organisation Registration Process and (ii) the Approved User Registration Process;</p> <p>1.3.3 it shall notify the Registration Organisation promptly, and in any event within 5 working days, of changes to Approved User(s), including where an Approved User has left the User Organisation or is no longer authorised by the User Organisation.</p> <p>1.3.4 it shall ensure Approved Users have passed all mandatory assessments communicated to it by the Registration Organisation, and further ensure that any such assessments are re-taken at intervals confirmed by the Registration Organisation.</p> <p>1.4 The Registration Organisation shall review each Application in line with the Registration Policy, and where an Application is approved, enter the User Organisation and/or the Approved User onto the Registered User Register. The Registration Organisation may, in its absolute discretion, remove the User Organisation and/or any Approved User from the Registered User Register if the User Organisation breaches any provision of this Agreement.</p>
--	--


Part B: Discovery Tool access Terms

<p>2. Safe People</p> 	<p>2.1 Subject to (i) the User Organisation complying with the Registration Terms at Part A above, and (ii) the User Organisation and the applicable Approved User(s) being entered onto the Registered User Register, the Registration Organisation agrees to authorise access to and use of the Discovery Tool for the Approved Access for applicable Approved User(s) who have accepted the Terms of Use in Annex 1. Approved Users are not required to sign this Agreement but must complete the Approved User Registration Process and accept the Terms of Use before Approved Access is granted.</p> <p>2.2 The User Organisation shall:</p> <p>2.2.2 ensure Approved User(s) are aware of, and comply with, the Terms of Use, and the User Organisation acknowledges and agrees that any breach by</p>
--	---

	<p>an Approved User of the Terms of Use shall be a breach of the User Organisation of this Agreement;</p> <p>2.2.3 notify the Registration Organisation within 5 Working Days of where an Approved User is no longer authorised by the User Organisation for the Approved Access;</p> <p>2.2.4 ensure that Approved Users do not share login details or access credentials to the Discovery Tool with any other person and do not attempt to access the Data or the Discovery Tool after they have been notified that they are no longer authorised to do so;</p> <p>2.3 The User Organisation warrants that the Approved User(s) are appropriately trained and skilled in respect of their use of the Data and the Discovery Tool and in relation to data protection, confidentiality, governance and security, and to the standard specified in Annex 2 or as issued by the Registration Organisation in connection with the Data and the Discovery Tool (as updated from time to time).</p> <p>2.4 In the event of a breach or suspected breach of this Agreement, including the Terms of Use, the User Organisation acknowledges and agrees that the Registration Organisation may immediately suspend access to the Discovery Tool and the Data for one or more Approved User(s) (as notified by the Registration Organisation) and fully investigate the breach or suspected breach and may also apply the remedies and/or require remediations as set out in Annex 3 and Annex 9:</p> <p>2.5 The User Organisation acknowledges and agrees that the Registration Organisation shall:</p> <p>2.5.1 terminate access to the Discovery Tool and the Data on termination or expiry of the Agreement;</p> <p>2.5.2 following notification in accordance with clause 2.2.3 above, terminate access to the Discovery Tool and the Data for the relevant Approved Users.</p> <p>2.6 If there is any conflict between the Terms of Use and this Agreement, this Agreement shall prevail.</p>
--	--

<p>3. Safe Access</p> 	<p>3.1 The User Organisation shall access and use the Data and the Discovery Tool:</p> <p>3.1.1 in accordance with Applicable Laws;</p> <p>3.1.2 for the Approved Purpose only, and not for any other purposes; and</p> <p>3.1.3 in accordance with all applicable ethical standards and approvals.</p>
<p>4. Safe Settings</p>	<p>4.1 The Registration Organisation shall ensure that the Registration arrangements implement appropriate technical and organisational measures in compliance with Data Protection Laws.</p> <p>4.2 The Registration Organisation shall ensure that the Data does not contain personal data under Data Protection Laws.</p>

	<p>4.3 The User Organisation shall:</p> <p>4.3.1 keep the Data, Access Outputs and any access credentials to the Discovery Tool confidential in accordance with Applicable Laws and with at least the same degree of care used to protect its own confidential information, and shall ensure that the Approved Users do the same;</p> <p>4.3.2 not access, use, or disclose the Data and/or the Access Outputs other than as permitted by this Agreement or as required by Applicable Laws, and shall ensure that the Approved Users comply with this obligation; and</p> <p>4.3.3 use up to date software on machines with access to the Data and Discovery Tool, access the Data and Discovery Tool in secure environments only, receive regular training on security and data protection, and use maintained anti-malware and anti-virus software so as to avoid and prevent the introducing or permitting the introduction of any Virus into the Discovery Tool or the Registration Organisation's network and information systems, and shall ensure that the Approved Users comply with this obligation ; and</p> <p>4.3.4 shall ensure that the confidentiality requirements set out in Annex 5 are followed by the Approved User(s).</p> <p>4.4 The User Organisation acknowledges and agrees that the Registration Organisation may monitor and audit the access to or use of the Discovery Tool and the Data by the User Organisation and its Approved User(s) to ensure compliance with the terms of this Agreement in accordance with the protocol set out in Annex 6.</p>
<p>5. Safe Data</p> 	<p>5.1 The User Organisation shall not, and shall not attempt to:</p> <p>5.1.1 identify individuals from the Data:</p> <p>5.1.2 contact any individual whose data forms part of the Data; or</p> <p>5.1.3 link or combine the Data with other information or data relating to an identified or identifiable natural person available to the User Organisation,</p> <p>and shall ensure that the Approved Users do not, and do not attempt to, do the same.</p> <p>5.2 The User Organisation acknowledges and agrees that it has sole responsibility, and the Registration Organisation takes no responsibility, for interpretation or further analysis of the Data to the extent permitted under this Agreement.</p> <p>5.3 The User Organisation acknowledges and agrees that the Registration Organisation can delete any Data at any time without terminating the Agreement including (without limitation) if:</p> <p>5.3.1 the Data is no longer available to the Registration Organisation; or</p> <p>5.3.2 the Registration Organisation has reasonable concerns that the use of the Data for the Approved Purpose may not comply with Applicable Laws or poses an organisational or reputational risk, or a risk to the public trust in the Registration requirements, SDE or use of health data (to be determined by the Registration Organisation at its sole discretion); or</p>

	<p>5.3.3 The Registration Organisation no longer has sufficient funding to support the provision of the relevant Data.</p> <p>5.4 The User Organisation will inform the Registration Organisation without delay, and in any event within 48 hours of becoming aware of:</p> <p>5.4.1 any unauthorised access, disclosure, loss damage or alteration of the Data;</p> <p>5.4.2 any element within the Data that might permit the identification of an individual whose data forms part of the Data;</p> <p>5.4.3 any event which may impact the confidentiality, integrity or availability of the Data including cyber security incidents;</p> <p>5.4.4 any complaints in relation to the Data including complaints from an individual or supervisory authority; and</p> <p>5.4.5 any request from an individual to exercise their rights in respect of the Data.</p> <p>5.5 To the extent required by Data Protection Laws, the Registration Organisation shall notify data protection supervisory authorities and – where applicable – notify affected data subjects in the event of a personal data breach (provided that the User Organisation shall not be restricted from making such notifications in cases where such notifications are required by Data Protection Legislation. The parties will collaborate in this regard as appropriate.</p> <p>5.6 The Registration Organisation shall be responsible for responding to data subject rights requests submitted to either Party in an appropriate and lawful manner. The User Organisation shall provide reasonable assistance to the Registration Organisation where this is necessary in order to respond.</p> <p>5.7 For the avoidance of doubt, the Data to which the User Organisation has access shall be anonymised prior to access.</p> <p>5.8 Where, to the extent permitted under this Agreement, the Approved Access involves access to third party Data, the User Organisation acknowledges and agrees that further third-party terms may apply in addition to this Agreement.</p>
<p>6 Safe Outputs</p> 	<p>6.1 The User Organisation shall ensure that Access Outputs do not include Personal Data.</p> <p>6.2 The User Organisation shall not:</p> <p>6.2.1 use any Access Output for any purpose contrary to Applicable Laws or outside of the Approved Purpose; or</p> <p>6.2.2 download, extract, transmit, transfer, remove, share, copy, or publish any of the Data from the Discovery Tool without permission from the Registration Organisation.</p> <p>6.3 The User Organisation shall not commercialise any Access Outputs without entering into a project-specific DAA.</p>

<p>7 Intellectual Property</p>	<p>7.1 This Agreement is not intended to constitute any transfer of Intellectual Property Rights in the Data or the Discovery Tool.</p> <p>7.2 Ownership of Intellectual Property Rights is set out in Annex 7.</p> <p>7.3 The Registration Organisation hereby grants to the User Organisation a non-exclusive licence under the Registration Organisation's and its licensors' Intellectual Property Rights in the Data to use the Data for the Approved Purpose for the Term in the Territory.</p> <p>7.4 Unless otherwise specified in Annex 7, Intellectual Property Rights in the Access Outputs shall belong to the User Organisation, but the User Organisation may not use the Access Outputs for any purpose other than as permitted under this agreement.</p>
<p>8 Outcomes uncertainty / no warranty</p>	<p>8.1 To the fullest extent permitted under Applicable Laws, the Registration Organisation:</p> <p>8.1.1 makes no warranty, express or implied as to the quality of the Data or its suitability for the Approved Purpose; and</p> <p>8.1.2 excludes all liability for actions, claims, proceedings, demands, losses, costs, awards, damages, and payments suffered or made by the User Organisation that may arise from their use of the Data or unavailability of the Data for whatever reason.</p> <p>8.2 The User Organisation acknowledges and agrees that the liability provisions in Annex 9 apply.</p>
<p>9 Compliance with Laws etc</p>	<p>9.1 Each Party shall comply with their respective obligations under all Applicable Laws, including Data Protection Laws.</p> <p>9.2 If a Party who is obliged to respond to requests under the Freedom of Information Act 2000 ("FOIA"¹¹), receives a request regarding the Data, it shall endeavour to inform the other Party within 5 Working Days and the other Party shall provide reasonable assistance to the Party in receipt of the request to comply with its obligations under FOIA. The Party subject to any request under FOIA retains sole discretion for responding to requests made under FOIA.</p> <p>9.3 The User Organisation shall:</p> <p>9.3.1 comply with any policy, conditions or guidance issued by the Registration Organisation in connection with the Discovery Tool or the SDE Network (as updated from time to time); and</p> <p>9.3.2 provide the Registration Organisation in a timely manner with such information and materials as the Registration Organisation may reasonably require in order to perform its obligations under this Agreement and ensure that all such information and materials it provides to the Registration Organisation are complete and accurate.</p>

<p>10 Anti-Corruption and Sanctions</p>	<p>10.1 The User Organisation warrants that, to the best of its knowledge and belief, neither it nor any member of its group or any Approved User:</p> <p>10.1.1. has, at any stage, violated the Anti-Corruption Laws;</p> <p>10.1.2 is being, or will be, investigated, in respect of any breach of the Anti-Corruption Laws; and/or</p> <p>10.1.3 is, or will be, subject to sanctions, (an "Infringement/Investigation").</p> <p>10.2 Save where such disclosure would constitute a breach of any Applicable Law, the User Organisation further warrants that it shall immediately, and in any event within 24 hours of becoming aware, notify the Registration Organisation upon becoming aware of any Infringement/Investigation.</p> <p>10.3 The User Organisation will not allow sanctioned persons or entities to access, directly or indirectly, the Discovery Tool and the Data. For the avoidance of doubt, the User Organisation is solely responsible for ensuring that its Approved Users are not sanctioned. The User Organisation must notify the Registration Organisation immediately, and in any event within 24 hours of becoming aware, of any use of the SDE and/or the Data by a sanctioned person or entity.</p> <p>10.4 Any breach of clauses 10.1 to 10.3 above by the User Organisation shall be considered a material breach of this Agreement which cannot be remedied.</p>
<p>11 Further provisions</p>	<p>11.1. This Agreement is drafted in the English language. If this Agreement is translated into any other language, the English language version shall prevail. All other documents provided under or in connection with this Agreement shall be in English or accompanied by a certified English translation.</p> <p>11.2. This Agreement constitutes the entire agreement between the Parties and supersedes all previous understandings and negotiations in respect of the Parties' obligations as provided in this Agreement. Each of the Parties acknowledges and agrees that, in entering into this Agreement, it has not relied on, and shall have no remedy in respect of, any statement, representation, warranty or understanding (whether negligently or innocently made) of any person (whether a party to this Agreement or not) other than as expressly set out in this Agreement.</p> <p>11.3. The delay or failure by a Party to insist upon the strict performance of any provision, term or condition of this Agreement or to exercise any right or remedy consequent upon the breach thereof shall not constitute a waiver of any such breach or any subsequent breach of such provision, term or condition.</p> <p>11.4. If any provision of this Agreement is agreed or held to be invalid or unenforceable, such provision shall not have the effect of invalidating or rendering unenforceable the remainder of this</p>

Agreement and the Parties agree that they shall immediately commence in good faith negotiations to vary the terms of this Agreement in order to remedy such invalidity or unenforceability.

11.5. No variation of this Agreement shall be effective unless it is agreed in writing and signed by the Parties or their authorised representatives.

11.6. Any notices under this Agreement shall be in writing, sent to the Parties at their address above or their registered address or sent by email: for Registration Organisation: england.data.healthresearch@nhs.net; and for the User Organisation [**insert email address**]. A notice shall be deemed to have been received:

11.6.1. if delivered by hand, at the time of delivery;

11.6.2. if posted, at the expiration of 48 hours after the envelope containing the same was delivered into the custody of the postal authorities; or

11.6.3. if sent by email, at the time of transmission, or if this time falls outside business hours in the place of receipt, when business hours resume.

11.7. Subject to clause 11.8, no person other than a Party to this Agreement shall have any rights to enforce any term of this Agreement.

11.8. An organisation that is the host of an SDE within the SDE Network as constituted from time to time, including NHS England or its successor, has rights under the Contracts (Rights of Third Parties) Act 1999 to enforce any or all of the rights of the Registration Organisation under this Agreement.

11.9. The Registration Organisation may:

11.9.1. subcontract its obligations under this Agreement;

11.9.2. assign, novate or transfer this Agreement, or any or all of its rights or obligations under this Agreement, to any public or private sector body which performs the functions of the Registration Organisation.

11.10. The User Organisation shall not assign, novate or deal in any other manner with any or all of its rights and obligations under this Agreement without the prior written consent of the Registration Organisation.

11.11. This Agreement, its subject matter, or its formation (including non-contractual disputes or claims) shall be governed and construed in accordance with the laws of England and Wales. Each Party irrevocably agrees that the courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with this Agreement or its subject matter or formation.

11.12. The Registration Organisation may notify updates and changes to these Terms and Conditions at any time by giving notice

	<p>to the User Organisation. The User Organisation’s continued access to Data and the Discovery Tool constitutes acceptance of the updated/changed terms unless the User Organisation notifies the Registration Organisation that it does not wish to accept such terms within 30 days of the notice of updates/changes being given, in which case, this Agreement shall terminate on the Registration Organisation’s receipt of such notice from the User Organisation.</p> <p>11.13. This Agreement is effective for the duration of the Term.</p> <p>11.14. This Agreement may be executed in counterparts and both of those counterparts taken together will be deemed to constitute one and the same instrument.</p> <p>11.15. The Parties agree that this Agreement may be signed by electronic signature and that this method of signature is as conclusive of our intention to be bound by this Agreement as if signed by each Party’s manuscript signature.</p>
--	--

Signatories:

<p>Signed by an authorised representative for and on behalf of the User Organisation:</p>	<p>NAME:</p> <p>SIGNATURE.....</p> <p>JOB ROLE.....</p> <p>DATE:</p>
<p>Signed by an authorised representative for and on behalf of the Registration Organisation:</p>	<p>NAME:</p> <p>DATE:</p>

The following definitions apply in the Agreement:

“Agreement” means this Secure Data Environment (SDE) Data Registration Agreement including the Annexes hereto and the Terms of Use.

“Access Output” means the potential use cases arising from the Data.

"Anti-Corruption Laws" means all Applicable Laws including official guidance issued pursuant to such legislation or regulations, related to financial crime, including without limitation the Bribery Act 2010, the Criminal Finances Act 2017, The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, the Proceeds of Crime Act 2002 and the Terrorist Asset Freezing etc. Act 2010 or other applicable money laundering, terrorist financing legislation or sanctions legislation.

"Applicable Laws" means all applicable laws, statutes, regulations, and codes from time to time in force including Data Protection Laws and Anti-Corruption Laws.

"Application" means an application for verification of a User Organisation or an Approved User, in accordance with the User Organisation or the Approved User Registration Process.

"Approved Access" means access to and use of the Discovery Tool for the Approved Purpose.

"Approved Purpose" means the evaluation of Access Outputs.

"Approved User(s)" means those employees, agents and independent contractors of the User Organisation whose access to and use of the Data and the Discovery Tool for the Approved Purpose has been authorised by the User Organisation subject to the terms of this Agreement, and who have completed the Approved User Registration Process and entered into the Terms of Use, prior to such access or use.

"Approved User Registration Process" means the SDE Network defined process to enable the checks undertaken by the Registration Organisation to confirm that a user meets requirements to be an Approved User who can access the Discovery Tool and submit data access requests.

"Control" means the ability of a person to direct the affairs of another whether through ownership of share or equity interests, the exercise of management control, powers of appointment of directors or officers, contract or any other means.

"Data" means the data accessible through the Discovery Tool, excluding additional data available under a DAA .

"Data Protection Laws" means any Applicable Laws with respect to data protection and privacy, including the General Data Protection Regulation ((EU) 2016/679) ("**GDPR**"), the UK GDPR (as defined in the UK Data Protection Act 2018) and/or Data Protection Act 2018, as applicable to either Party and or the activities under this Agreement.

"Group" means a person and any other person Controlling, Controlled by or under common Control with them.

"Insolvency Event" means the occurrence of any of the following events in respect of a Party:

- a) that Party suspending, or threatening to suspend payment of its debts, being unable to pay its debts as they fall due, admitting inability to pay its debts or being deemed unable to pay its debts within the meaning of section 123 of the Insolvency Act 1986 as if the words "it is proved to the satisfaction of the court" did not appear in sections 123(1)(e) or 123(2) of the Insolvency Act 1986;
- b) that Party commencing negotiations with all, or any class of, its creditors with a view to rescheduling any of its debts, or making a proposal for, or entering into any compromise or arrangement with its creditors other than for the sole purpose of a scheme for a solvent amalgamation of that Party with one or more other companies, or the solvent reconstruction of that Party;
- c) that Party applying to court for, or obtaining, a moratorium under Part A1 of the Insolvency Act 1986
- d) a petition is filed, a notice is given or a resolution is passed or an order is made, for or in connection with the winding up of that Party other than for the sole purpose of a scheme for a solvent amalgamation of that Party with one or more other companies, or the solvent reconstruction of that Party;
- e) an application is made to court, or an order is made, for the appointment of an administrator, or a notice of intention to appoint an administrator is given or if an administrator is appointed, over that Party (being a company, partnership or limited liability partnership);

- f) the holder of a qualifying floating charge over the assets of that Party (being a company or limited liability partnership) has become entitled to appoint or has appointed an administrative receiver;
- g) a person becomes entitled to appoint a receiver over all or any of the assets of that Party or a receiver is appointed over all or any of the assets of that Party;
- h) a creditor or encumbrancer of that Party attaches or takes possession of, or a distress, execution, sequestration or other such process is levied or enforced on or sued against, the whole or any part of that Party's assets and such attachment or process is not discharged within 14 days;
- i) any event occurs, or proceeding is taken, with respect to that Party in any jurisdiction to which it is subject that has an effect equivalent or similar to any of the events mentioned in paragraphs a) to h) above (inclusive).

"Intellectual Property Rights" means the patents, rights to inventions, copyright and related rights, moral rights, trademarks and service marks, business names and domain names, rights in get-up, goodwill and the right to sue for passing off, rights in designs, rights in computer software, database rights, rights to use, and protect the confidentiality of, confidential information (including know-how and trade secrets) and all other intellectual property rights including the right to sublicense such rights owned by third parties, in each case whether registered or unregistered and including all applications and rights to apply for and be granted, renewals or extensions of, and rights to claim priority from, such rights and all similar or equivalent rights or forms of protection which subsist or will subsist now or in the future in any part of the world.

"Personal Data" has the meaning given to it in Data Protection Laws.

"Sanctioned Countries" means any country, administration, or terrorist group against which sanctions are imposed by the UK Government (including those sanctions imposed by the United Nations), a list of which can be found here as at the date of this Agreement:

<https://www.gov.uk/government/collections/financial-sanctions-regime-specific-consolidated-lists-and-releases>); and here:

<https://www.un.org/securitycouncil/sanctions/information>).

"SDE" means a Secure Data Environment.

"SDE Network" means the NHS Research Secure Data Environment Network.

"Term" means five years from the date of this Agreement.

"Terms of Use" means the Terms of Use, which will be accepted individually by Approved Users as required for the Approved Access, as set out in Annex 1.

"Territory" means worldwide excluding Sanctioned Countries.

"User Organisation" means the organisation identified on page 1 of the Agreement.

"User Organisation Registration Process" means the SDE Network defined process to enable the checks undertaken by the Registration Organisation to confirm that an organisation meets requirements to be approved as a User Organisation who can access the Discovery Tool and submit data access requests.

"Registration Organisation" means the organisation identified on page 1 of the Agreement.

"Registered User Register" means the SDE Network register of registered Approved Users and registered User Organisations.

"Registration Policy" means the NHS SDE Research Network User and Organisation Policy.

"Virus" means any thing or device (including any software, code, file or programme) which may:

- a) prevent, impair or otherwise adversely affect the operation of any computer software, hardware or network, any telecommunications service, equipment or network or any other service or device;
- b) prevent, impair or otherwise adversely affect access to or the operation of any programme or data, including the reliability of any programme or data (whether by re-arranging, altering or erasing the programme or data in whole or part or otherwise);
- c) adversely affect the user experience; or
- d) compromise the security of the Discovery Tool or the Data,
including worms, trojan horses, viruses and other similar things or devices.

“Working Day” means any day other than a Saturday, Sunday, or public holiday in the UK country in which the Registration Organisation is based.

1. In this Agreement, unless the context otherwise requires:
 - 1.1 capitalised words and expressions shall have the meanings set out in the above definitions;
 - 1.2 words in the singular shall include the plural and in the plural shall include the singular; and
 - 1.3 references to clauses and annexes are to the clauses and annexes of this Agreement.
2. Clause and annex headings shall not affect the interpretation of this Agreement.
3. A reference to a statute or statutory provision is a reference to it as amended, extended or re-enacted from time to time.
4. A reference to a person includes any legal or natural person whether incorporated or not.
5. Any references following words: including, include, in particular, for example or any similar expression shall be interpreted as illustrative and shall not limit the sense of those words or references.

Annexes

ANNEX 1 – TERMS OF USE

NHS Research SDE Network User and Registration Organisation

USER TERMS OF USE

Part A: Cohort Discovery tool

Scope

These Part A Terms of Use (“Terms”) constitute an agreement made between Approved Users and [Sussex Partnership NHS Foundation Trust] (“Registration Organisation”), concerning access to and use of high-level descriptions and categories of anonymised data sets (“Data”) held within the Cohort Discovery tool (“Discovery Tool”). Please read these Terms carefully before accessing Data held within the Discovery Tool. The Discovery Tool contains Data submitted by individual Secure Data Environments (SDEs) within the SDE Network and therefore they have an interest in ensuring that Approved Users remain compliant with the Terms. The Terms may be enforced against an Approved User by any SDE within the SDE Network as constituted from time to time.

Any other data within the SDE Network may only be accessed by submitting a data access request and entering into a Data Access Agreement.

For the purpose of this Part A, and unless defined below, capitalised terms shall have the following meanings:

"Access Output" means the potential use cases arising from the Data.

"Approved User" means you and any other users approved under the Approved User Registration Process.

"Approved User Registration Process" means the SDE Network defined process to enable the checks undertaken by the Registration Organisation to confirm that a user meets requirements to be an Approved User.

"Approved Purpose" means the evaluation of Access Outputs.

"User Organisation" means a user organisation under the Agreement.

The Approved User agrees that they:

1. Have completed the Approved User Registration Process honestly and accurately.
2. Have taken appropriate training in data protection and data security to the standards of the Secure Data Environment (SDE) Data Registration Agreement (**"Agreement"**) and have completed such training prior to accessing the Data.
3. Have read and agree to comply with the terms of the Approved Access (**"Registration Documentation"**), as signed by the User Organisation.

4. Shall adhere to all relevant data protection legislation, including the UK General Data Protection Regulation (GDPR) and the UK Data Protection Act (2018).
5. Shall always preserve the confidentiality of the Data.
6. Shall use the Data for the benefit of the public, patients, and the NHS and only for the Approved Purpose.
7. Shall access the Discovery Tool or the Data in a secure physical location only, where inadvertent disclosure can be prevented (for example not in a public place where they can be overlooked).
8. Shall use only IT equipment provided by the User Organisation which has up to date antivirus and firewall software and complies with any security requirements notified by the Registration Organisation from time to time including the National Cyber Security Centre 10 Steps to Cyber Security.
9. Keep login details confidential and adhere to secure password guidelines.
10. Shall view and analyse Data only within the Discovery Tool.
11. Shall only save code and not datasets, other than as permitted for the Approved Purpose.
12. Understand that Data is provided with no guarantee of data quality.
13. Understand that activity in the Discovery Tool may be logged and recorded; this includes but is not limited to access to Data.
14. Shall notify the Registration Organisation immediately of any breach of Data (being the accidental or unauthorised destruction, loss, alteration, disclosure of or access to Data by an unauthorised person), or potential breach of Data in the Discovery Tool or incident that may have compromised the security of the Data or the Discovery Tool.
15. Agree to follow all Registration Documentation, and any documentation governing the use of the Discovery Tool.
16. Shall comply with the requirements of the User Organisation's Cyber Essentials certification (or any equivalent which is reasonably satisfactory to the Registration Organisation) and can provide evidence of the same if requested.

The Approved User agrees that they shall not:

1. Share access credentials to the Discovery Tool.
2. Give access to Data in the Discovery Tool to any other person.
3. Leave their device unattended while accessing the Discovery Tool.
4. Link Data to any other dataset without the consent of the Registration Organisation.
5. Download, extract, replicate, alter or otherwise interfere with the Data or the proper operation of the Discovery Tool.
6. Attempt to copy or remove analyses of the Data or other Access Output from the Discovery Tool without complying with the terms of the SDE Access Output Checking policy (as set out below).
7. Use the Discovery Tool for any purpose other than the Approved Purpose.
8. Show/share contents of the Discovery Tool with any unauthorised users.
9. Take and share screenshots of content within the Discovery Tool.
10. Save or duplicate Data within the Discovery Tool, other than as permitted for the Approved Purpose.
11. Attempt to identify or contact any individual using Data in the Discovery Tool.

SDE Access Output Checking policy

The Approved User shall ensure that any Access Output does not contain any unauthorised Data or Confidential Information of the Registration Organisation.

Third Party Rights

The Approved User acknowledges and agrees that an organisation that hosts an SDE within the SDE Network as constituted from time to time, including NHS England or its successor, has rights pursuant to the Contracts (Rights of Third Parties) Act 1999 to enforce any or all of the rights of the Registration Organisation under this Agreement.

Part B: SDE Access

Scope

These Part B Terms of Use ("Terms") constitute an agreement made between Approved Users and the SDE Host which has entered into the corresponding DAA ("Host Organisation"), concerning access to and use of data held within the Secure Data Environment ("SDE") Network. Please read these Terms carefully before accessing data held within the SDE.

For the purpose of this Part B, and unless defined below, capitalised terms shall have the following meanings:

"**Analysis Output**" means any data (excluding, for the avoidance of doubt, the Data itself), learning, discovery, insight, paper, publication, or other results arising out of an Approved Project.

"**Approved Project**" means the project(s) identified in an applicable SDE Data Access Agreement.

"**Approved Purpose(s)**" means the purpose(s) identified in an applicable SDE Data Access Agreement.

"**Data**" means the data fields and datasets to which the User Organisation has been approved access under an applicable SDE Data Access Agreement.

"**SDE Analysis Output Checking Policy**" means the policy set out in an applicable SDE Data Access Agreement.

"**SDE Data Access Agreement**" means the agreement permitting access to the SDE Environment for a User Organisation.

"**SDE Documentation**" means the documentation that an SDE and User Organisation will complete for a project specific data access. This will include the Data Access Agreement and other documents such as non-disclosure agreements and technical specifications.

"**User Organisation**" means a user organisation under a SDE Data Access Agreement.

The Approved User agrees that they:

1. Have taken appropriate training in data protection and data security to the standards of the SDE Data Access Agreement and have completed such training prior to accessing the Data.

2. Have read and agree to comply with the terms of the Approved Purposes and Approved Project(s) (together "SDE Documentation"), as signed by the User Organisation.
3. Shall adhere to all relevant data protection legislation, including the UK General Data Protection Regulation (GDPR) and the UK Data Protection Act (2018).
4. Shall always preserve the confidentiality of the Data.
5. Shall use the Data for the benefit of the public, patients, and the NHS and only within the Approved Project scope and purposes (as defined in Annex 2 of the SDE Data Access Agreement).
6. Shall access the SDE in a secure physical location where inadvertent disclosure can be prevented (for example not in a public place where they can be overlooked).
7. Shall use only IT equipment provided by the User Organisation which has up to date antivirus and firewall software and complies with any security requirements notified by the Host Organisation from time to time including the National Cyber Security Centre 10 Steps to Cyber Security.
8. Keep login details confidential and adhere to secure password guidelines.
9. Shall view and analyse Data only within the SDE.
10. Shall only save code and not datasets, other than as permitted for the Approved Purpose.
11. Understand that Data is provided with no guarantee of data quality.
12. Understand that activity in the environment may be logged and recorded; this includes but is not limited to access to Data and any code submitted.
13. Shall notify the Host Organisation immediately of any breach of Data (being the accidental or unauthorised destruction, loss, alteration, disclosure of or access to Data by an unauthorised person), or potential breach of Data in the SDE or incident that may have compromised the security of the Data.
14. Shall notify the Host Organisation should their information, pertinent to the SDE Data Access Agreement, change including their employment status or relationship with the User Organisation.
15. Agree to follow all SDE Documentation.
16. Shall comply with the requirements of the User Organisation's Cyber Essentials certification (or any equivalent which is reasonably satisfactory to the Host Organisation) and can provide evidence of the same if requested.

The Approved User agrees that they shall not:

12. Share access credentials or give access to Data in the SDE to any other person.
13. Leave their device unattended while accessing the SDE.
14. Link data to any other dataset other than those defined in the Approved Project.
15. Download, extract, replicate, alter or otherwise interfere with the Data or the proper operation of the SDE.
16. Attempt to copy or remove analyses of the Data or other Analysis Output from the SDE without following the SDE Analysis Output Checking Policy below.
17. Use the database for any purpose other than that agreed in the Approved Project scope.
18. Show/share contents of the SDE with any unauthorised users.
19. Take and share screenshots of content within the SDE.
20. Save or duplicate datasets within the SDE, other than as permitted for the Approved Purpose.
21. Attempt to identify or contact any individual using Data in the SDE.

SDE Analysis Output Checking policy

The Approved User shall ensure that any Analysis Output complies with the terms of the SDE Analysis Output Checking Policy (as detailed in Annex 10 of the SDE Data Access Agreement) and does not contain any unauthorised Data or Confidential Information of the Host Organisation.

Contact

If users have any queries regarding the SDE or these Terms please contact england.data.healthresearch@nhs.net.

THE USER UNDERSTANDS THAT ANY BREACH OF THESE TERMS OF USE WILL RESULT IN ACCESS TO DATA, THE DISCOVERY TOOL AND /OR THE SDE BEING REVOKED AND POSSIBLE DISCIPLINARY ACTION . THE USER RECOGNISES THEIR RESPONSIBILITY TO ENSURE COMPLIANCE WITH ALL REQUIREMENTS UNDER THE DATA PROTECTION LEGISLATION .

By checking the relevant box and submitting your user application online, you are agreeing that you have fully read and understood the Secure Data Environment (SDE) Data Registration Agreement and the Terms of Use.

ANNEX 2 - APPROVED USER TRAINING REQUIREMENTS

Sufficient training or accreditation for accessing and processing data as would be expected from a leading company within the field including in respect of:

- Data Protection Laws
- information security and the safeguarding of Personal Data
- The concepts of Legal basis of processing, confidentiality, consent, anonymisation and de-identification as applied to data in the UK
- The Registration Organisation's policies regarding the SDE and relevant NHS policies, including the Five Safes
- the terms of this Agreement.

For the avoidance of doubt, the training requirements under this Annex 2 shall include as a minimum modules covering:

- Confidentiality and Data Protection
 - Common law duty of confidence
 - Personal data definition and context (incl. anonymisation)
 - Individuals' rights (subject access, objections etc.)
 - Sharing and disclosures
 - Caldicott Principles
- Information Security
 - Good practice (password management; email security; systems and devices etc.)
 - Threat recognition (e.g. social media; phishing; software warnings)
 - Incident reporting
 - Information risk management
- Records Management
 - Freedom of Information (rights and) responsibilities
 - Corporate records management (incl. retention and disposal)
 - Health records management
 - Data quality (incl. clinical record-keeping standards)

Approved Users shall be required to complete or refresh the training annually.

Data security level one training on the E-learning for health site is acceptable to the SDE Network to achieve the above training requirements.

The User Organisation will provide details of such training and accreditation to the Registration Organisation:

- (i) within 10 Working Days of the date of this Agreement, in respect of each Approved User as at the date of this Agreement;

- (ii) within 2 Working Days of any further Approved User being added, in respect of that Approved User; and/or
- (iii) on request from the Registration Organisation at any time.

ANNEX 3— TERM, TERMINATION AND SUSPENSION

1. This Agreement shall come into force on the date it is signed by both Parties and expire at the end of the Term unless terminated earlier.
2. The Registration Organisation may terminate this Agreement by giving the User Organisation thirty (30) Working Days' written notice:
 - a. in the event that it is directed to do so by the UK Department of Health and Social Care or NHS England.
 - b. The Registration Organisation ceases to have the right to use the Discovery Tool or the Data as envisaged under this Agreement.
 - c. the Registration Organisation has reasonable concerns that the use of the Data for the Approved Purposes may not comply with Applicable Laws or poses an organisational or reputational risk, or a risk to the public trust in the Registration or the SDE (to be determined by the Registration Organisation at its sole discretion); or
 - d. the Registration Organisation reasonably considers that the User Organisation is in breach of this Agreement, another DAA or Applicable Laws relating to use of the Data and where either this is a breach which is not capable or remedy by the User Organisation or, if the breach is capable of remedy, where the User Organisation has not demonstrated that it has cured this breach within 7 days of notice from the Registration Organisation.
3. Either Party may terminate this Agreement for any reason by giving the other Party at least three (3) months' written notice.
4. Neither Party shall be in breach of this Agreement nor liable for delay in performing, or failure to perform, any of its obligations under this Agreement if such delay or failure result from events, circumstances or causes beyond its reasonable control including, without limitation, acts of God, flood, drought, earthquake or other natural disaster; epidemic or pandemic; terrorist attack, cyber attack, civil war, civil commotion or riots, war, threat of or preparation for war, armed conflict, imposition of sanctions, embargo, or breaking off of diplomatic relations; nuclear, chemical or biological contamination or sonic boom; any law or action taken by a government or public authority, including imposing an export or import restriction, quota or prohibition, or failing to grant a necessary licence or consent; collapse of buildings, fire, explosion or accident; and any labour or trade dispute, strikes, industrial action or lockouts; non-performance by suppliers or subcontractors; and interruption or failure of utility service ("**Force Majeure**"). In such circumstances the affected Party shall be entitled to a reasonable extension of the time for performing such obligations. If the period of delay or non-performance continues for 3 months, the Party not affected may terminate this Agreement by giving 30 days' written notice to the affected Party.
5. Without affecting any other right or remedy available to it, either Party may terminate this Agreement with immediate effect by giving written notice to the other Party if:
 - a. the other Party commits a material breach of any term of this Agreement which cannot be remedied or which the other Party fails to remedy within 30 days' notice in writing to do so;

- b. an Insolvency Event occurs in respect of the other Party; or
 - c. the other Party suspends or ceases, or threatens to suspend or cease, carrying on all or a substantial part of its business.
6. Termination or expiry of this Agreement shall not affect any rights, remedies, obligations, or liabilities of the Parties that have accrued up to the date of termination or expiry, including the right to claim damages in respect of any breach of the Agreement which existed at or before the date of termination or expiry. Any provision of this Agreement that expressly or by implication is intended to come into or continue in force on or after termination or expiry of this Agreement shall come into or continue in full force and effect.
7. On termination for any reason or expiry of this Agreement:
 - a. The User Organisation's access to the Data and the Discovery Tool shall cease; and
 - b. The provisions of Annex 5 shall continue to apply indefinitely.
8. The Registration Organisation may, at its sole discretion, suspend access to the Data and the Discovery Tool for the User Organisation, either in whole or in part, including but not limited to where:
 - a. the Discovery Tool is undergoing maintenance;
 - b. there are system outages which are outside of the Registration Organisation's control;
 - c. the Registration Organisation is investigating a breach or suspected breach of Applicable Law or this Agreement;
 - d. in any circumstances where the Registration Organisation is permitted to terminate this Agreement pursuant to this Annex 3; or
 - e. the Registration Organisation has otherwise deemed it reasonably necessary to suspend access to the Data and the Discovery Tool including but not limited to where a potential data security risk is being investigated.
9. The Registration Organisation's right to suspend access to the Data and the Discovery Tool under paragraph 8 of this Annex 3 does not affect or in any way limit any other right or remedy available to it.

ANNEX 4 - NOT USED

ANNEX 5 - CONFIDENTIALITY

1. **Confidential Information** means all confidential information (however recorded or preserved) disclosed by one Party (the "**Disclosing Party**") or its Representatives (as defined below) to the other Party (the "**Recipient**") and its Representatives whether before or after the date of this Agreement in connection with this Agreement, including:
 - a. the terms of this Agreement;
 - b. the Data;
 - c. login and access details for the Discovery Tool;
 - d. any information (whether or not technical) that would be regarded as confidential by a reasonable business person.
2. **Representatives** means, in relation to a Party, its employees, officers and professional advisers.
3. The provisions of this Annex 5 shall not apply to any Confidential Information that:
 - a. is or becomes generally available to the public (other than as a result of its disclosure by the Recipient in breach of this clause);
 - b. was available to the Recipient on a non-confidential basis before disclosure by the Disclosing Party;
 - c. was, is or becomes available to the Recipient on a non-confidential basis from a person who, to the Recipient's knowledge, is not bound by a confidentiality agreement with the Disclosing Party or otherwise prohibited from disclosing the information to the Recipient;
 - d. the parties agree in writing is not confidential or may be disclosed; or
 - e. is developed by or for the Recipient independently of the information disclosed by the Disclosing Party.
4. The Recipient shall use best endeavours to keep the Disclosing Party's Confidential Information confidential and shall not:
 - a. use such Confidential Information except for the purpose of exercising or performing its rights and obligations under or in connection with this Agreement (**Permitted Purpose**); or
 - b. disclose such Confidential Information in whole or in part to any third party, except as expressly permitted by this Annex 5.
5. The Recipient may disclose such parts of the Confidential Information to those of its Representatives who need to know such Confidential Information for the Permitted Purpose, provided that:
 - a. it informs such Representatives of the confidential nature of the Confidential Information before disclosure; and
 - b. it procures that its Representatives shall, in relation to any Confidential Information disclosed to them, comply with the obligations set out in this clause as if they were a party to this Agreement,

and at all times, it is liable for the failure of any Representatives to comply with the obligations set out in this Annex 5.

6. The Recipient may disclose Confidential Information to the extent such Confidential Information is required to be disclosed by law, by any governmental or other regulatory authority (including any necessary reporting to a supervisory or commissioning body or regulator) or by a court or other authority of competent jurisdiction provided that, to the extent it is legally permitted to do so, it gives the Disclosing Party as much notice of such disclosure as possible and, where notice of disclosure is not prohibited and is given in accordance with this Annex 5, it takes into account the reasonable requests of the Disclosing Party in relation to the content of such disclosure.
7. The Disclosing Party reserves all rights in its Confidential Information. No rights or obligations in respect of the Confidential Information other than those expressly stated in this Agreement are granted to the other Party, or to be implied from this Agreement.
8. On termination or expiry of this Agreement, the Recipient shall:
 - a. destroy or return to the Disclosing Party all documents and materials (and any copies) containing, reflecting, incorporating, or based on the Confidential Information;
 - b. erase all the Confidential Information from its computer and communications systems and devices used by it, including such systems and data storage services provided by third parties (to the extent technically and legally practicable); and
 - c. certify in writing to the Disclosing Party that it has complied with the requirements of this clause,

provided that the Recipient may retain documents and materials containing, reflecting, incorporating, or based on the Confidential Information to the extent required by law or any applicable governmental or regulatory authority.
9. The provisions of this Annex 5 shall continue to apply after the expiry or earlier termination of this Agreement.

ANNEX 6 - SDE PROTOCOL ON MONITORING USE /AUDIT/COMPLIANCE

The Registration Organisation shall be entitled at any time during the Term to audit User Organisation's access to or use of the Cohort Discovery Tool and/or the Data under this Agreement should the Registration Organisation have any concerns that the User Organisation and/or Approved Users are in breach of the terms of this Agreement. The User Organisation will provide the Registration Organisation with all reasonable assistance in order to enable it to undertake an audit pursuant to this Annex 6.

Without prejudice to the Registration Organisation's rights under Annex 3, the User Organisation shall comply with any corrective actions required by the Registration Organisation in order to ensure User Organisation's compliance with the terms of this Agreement.

ANNEX 7 - INTELLECTUAL PROPERTY RIGHTS

The Registration Organisation or its licensors is the owner/licensee of the Discovery Tool and the Intellectual property Rights in the Data within it. Intellectual Property Rights in the Discovery Tool and the Data shall remain the property of the Registration Organisation or its licensors and the User Organisation shall not acquire any title or any other Intellectual Property Rights in them under this Agreement.

Intellectual Property Rights in the Access Output shall belong to the User Organisation to the extent that any Intellectual Property Rights in them do not constitute or infringe Intellectual Property Rights in the Data.

The User Organisation may not create a database, including synthetic datasets, based on Data (except that for the avoidance of doubt the User Organisation may create a database from the Access Output) and may not remove, suppress or modify in any way any proprietary marking, including any trade mark or copyright or database right notice on or in the Data or other means by which the Data is made available to the User Organisation or which is visible during the access or use of the Data.

The User Organisation shall notify the Registration Organisation immediately if the User Organisation becomes aware of any infringement of or unauthorised access to, use or copying of any part of the Discovery Tool or the Data.

ANNEX 8- SERVICE LEVELS

Part A: Availability

The Registration Organisation shall use reasonable endeavours to provide access to the Discovery Tool and the Data to the Approved Users throughout the Term.

Any unavailability of the Discovery Tool or the Data is outside the control of the Registration Organisation.

The Registration Organisation or its licensors may effect maintenance, repairs or updates to the Discovery Tool and the Data from time to time.

Part B: Technical Support

The Registration Organisation will provide reasonable technical support to the Approved Users on Working Days throughout the Term.

The Approved User will use reasonable endeavours to provide the Registration Organisation with sufficient information required to answer any query submitted. The Registration Organisation will use reasonable endeavours to respond to the Approved User's queries within a reasonable timeframe.

ANNEX 9 - LIABILITY

1. Liability

- a. The Registration Organisation shall not in any circumstances have any liability for any losses or damages which may be suffered by the User Organisation (or any person claiming under or through the User Organisation), whether the same are suffered directly or indirectly or are immediate or consequential, and whether the same arise in contract, tort (including negligence) or otherwise howsoever, which fall within any of the following categories: (i) special damage, (ii) loss of profits; (iii) loss of anticipated savings; (iv) loss of business opportunity; (v) loss of or damage to goodwill; (vi) loss of use or corruption of software, information or data; (vii) indirect or consequential loss.
 - b. The Registration Organisation excludes all warranties in relation to the Discovery Tool and the Data to the fullest extent permitted by law.
 - c. The total aggregate liability of the Registration Organisation for any and all claims relating to (i) the User Organisation's access to the Discovery Tool and the Data under this Agreement whether in contract, tort (including negligence) or otherwise and whether in connection with this Agreement or any collateral contract, and (ii) any actions or omissions of the Registration Organisation under this Agreement, shall in no circumstances exceed £10,000 (ten thousand pounds).
 - d. The exclusions in this Agreement shall apply to the fullest extent permissible at law, but the Registration Organisation does not exclude or restrict liability for:
 - i. death or personal injury caused by the negligence of the Registration Organisation, its officers, employees, contractors, or agents;
 - ii. fraud or fraudulent misrepresentation;
 - iii. breach of the obligations implied by section 12 of the Sale of Goods Act 1979 or section 2 of the Supply of Goods and Services Act 1982; or
 - iv. any other liability which may not be excluded by law.
2. The Registration Organisation shall not be in breach of this Agreement to the extent that any neglect, default, act or omission of the User Organisation, its Approved Users, staff, agents, sub-licensees or subcontractors results in a breach of the Registration Organisation's obligations under this Agreement.
 3. The User Organisation shall indemnify the Registration Organisation against all liabilities, costs, expenses, damages, and losses (including any direct, indirect, or consequential losses, loss of profit, loss of reputation and all interest, penalties and legal costs (calculated on a full indemnity basis) and all other reasonable professional costs and expenses) suffered or incurred by the Registration Organisation arising out of or in connection with:
 - a. the User Organisation's exercise of the rights granted to it under this Agreement;
 - b. the User Organisation's breach or negligent performance or non-performance of this Agreement;
 - c. the User Organisation failing to comply with its obligations to complete the User Organisation Registration Process and/or to ensure Approved User(s) complete the

Approved User Registration Process and ensuring the completeness and accuracy of the same in accordance with clause 1 of the Agreement;

- d. the User Organisation introducing or permitting the introduction of any Virus into the Discovery Tool or the Registration Organisation's network and information systems, or failing to ensure that shall ensure that the Approved Users do not do the same;
- e. the enforcement of this Agreement; or
- f. any claim for infringement of third-party Intellectual Property Rights.