Police and Crime Commissioner for Cleveland – accessing Cleveland Police systems

DATA PROCESSING CONTRACT

THIS AGREEMENT is made the (1st October 2021).

BETWEEN

1. The Parties

The Chief Constable of Cleveland Police, (herein after called the "Controller" or the "Force") Community Safety Hub, 1 Cliffland Way, Hemlington, TS8 9GL of the one part and

The Police and Crime Commissioner for Cleveland (herein after called the "Processor"), Community Safety Hub, 1 Cliffland Way, Hemlington, TS8 9GL of the second part.

1.1 With respect to the Parties' rights and obligations under the Contract and this Agreement, the Parties acknowledge and agree that:

1.1.1 the relevant Force is the Controller in respect of any Personal Data inputted to the Processor's Software and/or System, and the subsequent processing of any Personal Data contained within search results generated in response to the Personal Data inputted and subsequent processing thereof by or on behalf of the relevant Force;

1.1.2 the Processor is a Processor in respect of any Personal Data inputted to the Processor's Software and/or System, and any subsequent processing on behalf of the relevant Force of Personal Data contained within search results generated in response to the Personal Data inputted; and

1.1.3 the Processor may not determine the purposes and means of the processing of Personal Data to be undertaken by it under the Contract and this Agreement.

1.2 For the avoidance of doubt, the Processor is the Controller in its own right in respect of any Personal Data it gathers, stores and otherwise processes for the purpose of the provision of the Services, save as in relation to the processing activities detailed at 1.1.

1.3 The Processor acknowledges that the Controller may also engage other contractors to perform services for and on behalf of the Controller and the Processor shall cooperate and interface directly with such third parties as instructed by the Controller.

2. **Purpose**

2.1 This Agreement sets out the terms and conditions under which personal data held by the specified Controllers will be disclosed to the specified Processor. This Agreement is entered into with the purpose of ensuring compliance with the applicable "Data Protection Legislation". Any processing of personal data must comply with the provisions of this legislation.

2.2 The purpose of the processing is described at Schedule A (herein after called the Purpose).

2.3 The Processing of the Police Data for the Purpose will assist the relevant Controller to fulfil its obligations pursuant to the processing described at Schedule A.

3. Definitions

3.1 The following words and phrases used in this Agreement shall have the following meanings except where the context otherwise requires.

3.2 In this Agreement, the expressions **Data, Controller, Data Subject, Processor, Processing, Personal Data, Personal Data Breach, Pseudonymisation** and **Supervisory Authority Concerned** have the same meaning as in Article 4 of GDPR.

3.3 **Data Protection Legislation** means (i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time (ii) the Data Protection Act 2018 to the extent that it relates to processing of personal data and privacy and (iii) all applicable Law and guidance about the processing of personal data and privacy, including the Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699), the Electronic Communications Data Protection Directive 2002/58/EC, the Privacy and Electronic Communications (EC Directive) Regulations 2003 and all applicable Laws relating to processing of Personal Data and privacy, including where applicable the guidance and codes of practice issued by the Supervisory Authority Concerned.

3.4 **Special Categories of Personal Data** has the same meaning as in Article 9 of the GDPR.

3.5 **GDPR** means the UK General Data Protection Regulation.

3.6 **LED** means the Law Enforcement Directive.

3.7 **Data Loss Event** means any event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Contract, and/or actual or potential loss and/or destruction of Personal Data in breach of this Contract, including any Personal Data Breach.

3.8 **Data Subject Access Request** means a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation.

3.9 **Police Data** means any Data, including Personal Data and Special Categories of Personal Data and criminal conviction and offence data, to be provided to, or collected by, the Processor and processed on behalf of the Controller as identified in this Contract.

3.10 The **Designated Police Manager** means Head of DSE who has the day to day responsibility for the management of the Purpose on behalf of the Controllers, or other such person as shall be notified to the Processor from time to time.

3.11 The **Project Manager** means Resolution Team Manager within OPCC who has the day to day management on behalf of the Processor, or such other person as shall be notified to all the Controllers from time to time.

3.12 **Government Security Classification** means a scheme for the classification of information.

3.13 **Good Industry Practice** means the exercise by the Processor of that degree of skill, diligence, prudence, foresight and operating practice which, at the relevant time, would reasonably and ordinarily be expected from a skilled and experienced person engaged in the same or a similar business as the Contractor, seeking in good faith to comply with its contractual and other obligations and those Information Security practices as advised by ISO/IEC 27001:2013, or such other relevant guidance as may be in force from time to time.

3.14 **Agreement** means this Data Processing Agreement together with its schedules and all other documents attached to or referred to as forming part of this Agreement.

3.15 **Data Protection Impact Assessment** means an assessment by, or on behalf of, all the Controllers of the impact of the envisaged processing on the protection of personal data.

3.16 **Services** means the processing activities and services to be undertaken by the Processor on behalf of the Controllers, as identified.

3.17 **Protective Measures** means appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of such measures adopted.

3.18 **Law** means any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of Section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the Processor is bound to comply.

3.19 **Confidential Information** means all Police Data and any other information relating to the Controllers' customers and prospective customers, current or projected financial or trading situations, business plans, business strategies, developments and all other information relating to the Controllers' business affairs including any trade secrets, know-how and any information of a confidential nature imparted by the Controllers to the Processor during the term of this the Contract and this Agreement or coming into existence as a result of the Processor's obligations, whether existing in hard copy form or otherwise, and whether disclosed orally or in writing.

3.20 **Content** means the files, data, text and other materials that are transferred, stored, shared or hosted on or through the Services and Software by each Controller, Users and Recipients, including any Personal Data in it. It does not include CRM Information or System Data.

3.21 **CRM Information** means the databases, logs and other collections of Personal Data and/or Police Data about each Controller and its respective users that is provided to the Processor by the Controller or its Users, or that the Processor obtains in connection with: (a) the creation and administration of accounts; (b) how the Services, software and support are used, accessed and interacted with; (c) any permissions, consents or preferences; and (d) each of the Controllers being the Processor's customer, and information that the Processor obtains from third parties that may be linked to the Controllers.

3.22 **System Data** means (a) usage statistics, system logs, performance and security data, feedback data, records of support requests, and aggregated data about how the Processor's sites, Services, software, support and apps are used (e.g. performance counters, access logs, metrics and associated metadata, unique identifiers for devices, technical information about the devices used, the network, operating system and browsers); and (b) data identified on the Processor's sites, Services, software, support and apps as malicious (e.g. malware infections, cyberattacks, unsuccessful security incidents, or other threats). This may contain limited CRM Information where it appears, for example, in log records.

3.23 **Lead Controller** shall mean The Chief Constable of Cleveland Police, or such other Controller as may be notified to the Processor in writing from time to time.

3.24 **Interpretation**

3.25 Headings are inserted for convenience only and shall not affect the construction or interpretation of this Contract and, unless otherwise stated, references to clauses and schedules are references to the clauses of and schedules to this Contract;

3.26 Any reference to any enactment or statutory provision shall be deemed to include a reference to such enactment or statute as extended, re-enacted, consolidated, implemented or amended and to any subordinate legislation made under it.

3.27 The word 'including' shall mean including without limitation or prejudice to the generality of any description, definition, term or phrase preceding that word, and the word 'include' and its derivatives shall be construed accordingly.

4. Information provision

4.1 Details of the Police Data to be provided to or collected by the Processor and processed on behalf of the Controllers is set out at Schedule A:

(a) the subject matter and duration of the processing;

(b) the nature and purpose of the processing;

(c) the type of Personal Data and categories of Data Subject involved.

4.2 Ownership of the Police Data shall at all times remain with the relevant Controller.

5 Use, Disclosure and Publication

5.1 The Police Data will be used solely for the Purpose.

5.2 Subject to clause 5.7 below the Police Data shall not at any time be copied, broadcast or disseminated to any other third parties, except in accordance with the terms of this Data Processing Agreement or with the express written permission of the Controller.

5.3 The Police Data will NOT be matched by the Processor with any other Personal Data otherwise obtained from the Controller, or any other source, unless specifically authorised in writing by the relevant Controller.

5.4 Unless in accordance with the "Purpose", the Police Data will not be disclosed to any third party without the express written authority of the relevant Controller, and then only in accordance with the Controller's documented instructions.

5.5 Access to the Police Data will be restricted to those employees of the Processor as listed at Schedule B and approved by the Controller, directly involved in the processing of Police Data in pursuance of the Purpose.

5.6 No steps will be taken by the Processor to contact any Data Subject identified in the Police Data except where it is necessary for the Purpose and only when expressly authorised in writing by the relevant Controller.

5.7 The only exceptions to clauses 5.2 and 5.4 above are where the Processor is subject to an order issued by a Court of competent jurisdiction, or subject to any exemption under the Data Protection Act 2018, where disclosure is required by a law enforcement agency or regulatory body or authority, or the Processor is required to do so for the purposes of legal proceedings, in which case the Processor shall in so far as permitted to do so immediately notify the Controller in writing of any such requirement for disclosure of the Police Data in order to allow the Controller to make representations

to the person or body making the requirement save where the Processor is prohibited by law from so doing.

6 Data Protection and Human Rights

6.1 The use and disclosure of any Personal Data shall be in accordance with the obligations imposed upon the Parties to this Contract by the Data Protection Legislation and the Human Rights Act 2018.

6.2 The Parties agree and declare that the information processed pursuant to the Contract and this Agreement will be used and processed with regard to the rights and freedoms enshrined within the European Convention on Human Rights. Further, the Parties agree and declare that the processing of Personal Data as described at Schedule A is proportionate, having regard to the Purpose and the steps taken in respect of maintaining a high degree of security and confidentiality.

6.3 The Processor undertakes to comply with the provisions of the Data Protection Legislation, and in particular to notify as required any particulars as may be appropriate to the Information Commissioner and shall not perform its obligations under the Contract and this Agreement in such a way as to (or otherwise do or omit to do anything which might) cause the Controllers to breach any of their applicable obligations under Data Protection Legislation.

6.4 The Processor warrants, undertakes and represents that, in so far as it is a Processor in accordance with clause 1.1 above, it shall (and shall ensure that the Processor Personnel shall) only use or process the Police Data for the purpose set out in the Appendix to this Schedule and in accordance with instructions from the Force (as set out in the Agreement, the Appendix or as otherwise notified in writing by the Force to the Processor during the term of the Contract and Agreement) unless it is required to do otherwise by Law. If it is so required, the Processor shall promptly notify the Controllers before processing the Police Data unless prohibited by Law.

6.5 The Processor shall notify both the Data Protection Officer on behalf of the relevant Controller and the Designated Police Manager on behalf of the Lead Controller immediately if it considers that any of the Controllers' instructions infringe the Data Protection Legislation.

6.6 The Police Data shall be processed by the Processor without unreasonable delay.

6.7 The Processor shall provide training on a continuing basis for all Processor Personnel employed or engaged in the provision of the Services in compliance with Data Protection Legislation, Good Industry Practice, and the Security Plan.

6.8 The Processor shall provide the Controllers with full assistance in relation to either Party's obligations under Data Protection Law and any complaint, communication, request or event.

6.9 The Processor shall provide all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment prior to commencing any processing, and throughout the period of processing. Such assistance may, at the discretion of the Controller, include:

(a) a systematic description of the envisaged processing operations and the purpose of the processing;

(b) an assessment of the necessity and proportionality of the processing operations in relation to the Services;

(c) an assessment of the risks to the rights and freedoms of Data Subjects; and

(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

6.10 The Processor shall notify the both the Data Protection Officer on behalf of the relevant Controller(s) and the Designated Police Manager on behalf of the Lead Controller immediately if it:

(a) receives a Data Subject Access Request (or purported Data Subject Access Request), including a request to rectify, block or erase any Personal Data;

(b) receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;

(c) receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under the Contract and this Agreement;

(d) receives a request from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; and,

(e) becomes aware of a Data Loss Event.

6.11 Upon becoming aware of a Data Loss Event, the Processor shall immediately take all steps necessary to:

6.11.1 remedy such breach or protect the System against any such potential or attempted breach or threat; and

6.11.2 prevent an equivalent breach in the future.

6.12 The Processor shall provide the Data Protection Officer(s) on behalf of the relevant Controller(s) and the Designated Police Manager on behalf of the Lead Controller with full details and copies of the complaint, communication, request (including any information notice) or event detailed in clause 6.7 above and shall provide within two Business Days or such other period as may be agreed with the relevant Controller(s):

6.12.1 such assistance as is reasonably requested by or on behalf of the relevant Controller(s) and/or the Lead Controller to enable them to comply with a Data Subject Access Request within the relevant timescales set out in Data Protection Law;

6.12.2 the relevant Controller(s), at their request, with any Police Data it holds in relation to a Data Subject (within the timescales required by the relevant Controller(s));

6.12.3 assistance as requested by the or on behalf of the relevant Controller(s) and/or the Lead Controller following any Data Loss Event;

6.12.4 assistance as requested by or on behalf of the relevant Controller(s) and/or the Lead Controller with respect to any request from the Supervisory Authority Concerned or any consultation by any Controller with the Supervisory Authority Concerned;

6.12.5 assistance as requested by or on behalf of the relevant Controller(s) and/or the Lead Controller in relation to any other complaint or request made; and,

6.12.6 the relevant Controller(s) and/or the Lead Controller with any other information reasonably requested by them related to any complaint, communication or request (including any information notice), or event.

6.13 The Processor's obligation to notify and provide information to the relevant Controller(s) and/or the Lead Controller under the preceding clauses shall include the provision of further information in phases, as further details become available.

6.14 Taking into account the nature of the Processing, the Processor shall provide the relevant Controller with full assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under preceding clauses (and insofar as possible within the timescales reasonably required by the Controller) including by promptly providing:

(a) The relevant Controller with full details and copies of the complaint, communication or request;

(b) such assistance as is reasonably requested by the relevant Controller to enable the relevant Controller to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;

(c) the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;

(d) assistance as requested by the Controller following any Data Loss Event; and,

(e) assistance as requested by the Controller with respect to any request from the Information Commissioner's Office, or any consultation by the Controller with the Information Commissioner's Office.

6.15 It is acknowledged that where a Controller cannot comply with a request without disclosing information relating to another individual who can be identified from that information, he is not obliged to comply with the request, unless;

(a) the other individual has consented to the disclosure of the information to the person making the request; or

(b) it is reasonable in all the circumstances to comply with the request without the consent of the other individual. In determining whether it is reasonable, regard shall be had, in particular to: -

i. any duty of confidentiality owed to the other individual;

ii. any steps taken by the Controller with a view to seeking consent of the other individual;

iii. whether the other individual is capable of giving consent;

iv. any express refusal of consent by the other individual.

6.16 The Processor shall not transfer Police Data to, or process Police Data within, any country or territory outside the United Kingdom unless the prior written consent of the Force has been obtained, and any necessary notification(s) to the relevant supervisory authority(ies) have been has been complied with, and, if the transfer or processing is to be outside the European Economic Area, the following conditions have been fulfilled:

6.16.1 appropriate safeguards in relation to the transfer are in place, as determined by or on behalf of the Controller, or in exceptional circumstances and where explicitly stated in writing by or on behalf of the Controller one of the derogations at GDPR Article 49 applies;

6.16.2 the Data Subject shall retain enforceable rights and effective legal remedies;

6.16.3 the Processor complies with its obligations under Data Protection Law by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Force in meeting its obligations); and

6.16.4 the Processor complies with any reasonable instructions notified to it in advance by the Force with respect to the processing of the Personal Data;

6.17 The following personnel are authorised by the Parties to assume responsibility for Data Protection legislation compliance, notification, security, confidentiality, audit and co-ordination of Data Subject rights.

Nominated Post Holder	*Organisation*	*Contact Details*
Data Protection Officer	Cleveland Police	dataprotection@cleveland.pnn.police.uk
Data Protection Officer	OPCC	[redacted]@cleveland.police.uk

6.18 On reasonable notice, the Processor shall permit the Controllers or the Controllers' representative or designated auditor (subject to reasonable and appropriate confidentiality undertakings) to inspect and audit the Processor's data processing activities (and/or those of its agents, subsidiaries, Sub-processors and sub-contractors) and compliance with this Contract. The Processor shall comply with all reasonable requests or directions by the Controllers, their representative or designated auditor to enable the controllers to verify and/or procure that the Processor is in full compliance with its obligations under the Contract (including this Schedule).

6.19 The Processor shall designate a Data Protection Officer if required by the Data Protection Legislation.

6.20 Before allowing any Sub-processor to process any Personal Data related to the Contract and this Agreement, the Processor must:

(a) notify the Controller in writing of the intended Sub-processor and processing;

(b) obtain the written consent of the Controller;

(c) enter into a written contract with the Sub-processor which give effect to the terms set out in the Contract and this Agreement such that they apply to the Sub-processor; and

(d) provide the Controller with such information regarding the Sub-processor as the Controller may reasonably require.

6.21 The Processor shall remain fully liable for all acts or omissions of any Sub-processor.

6.22 The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Controller may on not less than 30 Working Days' notice to the Processor amend the Contract and this Agreement to ensure that it complies with any guidance issued by the Information Commissioner's Office.

6.23 The Processor shall maintain and make available to the Controller complete and accurate records to demonstrate compliance with the Processor's obligations under the Contract and this Agreement and/or under Articles 28 and 30 of the GDPR and or

Section 59 of the Data Protection Act 2018 as appropriate to the processing purpose under this Agreement.

6.24 The Processor shall at the written direction of the relevant Controller, delete in accordance with clause 8 below or return Police Data (and any copies of it) to the Controller on termination of the Contract and/or this Agreement unless the Processor is required by Law to retain the Police Data, at no additional cost to the Controller.

7 Confidentiality

7.1 Except as specified in clause 7.2 below, the Processor shall not use or divulge or communicate to any person (other than those whose province it is to know the same for the Purpose, or without the prior written authority of the Controller) any Police Data obtained from any Controller, which it shall treat as private and confidential and safeguard accordingly.

7.2 Clause 7.1 above shall not apply where disclosure of the Police Data is ordered by a Court of competent jurisdiction, or subject to any exemption under the Data Protection Act 2018, where disclosure is required by a law enforcement agency or regulatory body or authority, or is required for the purposes of legal proceedings, in which case the Processor shall immediately notify the Controller in writing of any such requirement for disclosure of the Police Data in order to allow the Controller to make representations to the person or body making the requirement.

7.3 The restrictions contained in clauses 7.1 and 7.2 shall cease to apply to any Data which may come into the public domain otherwise than through unauthorised disclosure by the Parties to the Contract or this Agreement.

7.4 The Processor shall ensure that any individuals who process Police Data under the Contract and this Agreement are aware of their responsibilities in connection with the use of that Police Data and have confirmed so in writing by completion of Schedule C: Undertaking of Confidentiality which will be provided to the Designated Police Manager as a pre-requisite for that individual to process Police Data.

7.5 For the avoidance of doubt, the obligations of confidentiality imposed on the Parties by the Contract and this Agreement shall continue in full force and effect after the expiry or termination of the Contract and this Agreement.

7.6 Respect for the privacy of individuals will be afforded at all stages of the Purpose.

8 Retention, Review and Deletion

8.1 The Processor shall process all Police Data in accordance with the normal policies and procedures of each Controller in relation to the retention, review and disposal, which will be notified to the Processor by the Designated Police Manager.

8.2 The Designated Police Manager, on behalf of the Controllers, shall be entitled ensure that the requirements of the Force Policies are met by the Processor, in accordance with paragraph 6.1.2.

8.3 Police Data shall only be retained by the Processor for such time as is necessary for the completion of the Purpose and thereafter it shall be promptly and securely deleted from the Processor's information systems in accordance with the arrangements identified at Schedule A.

8.4 The Processor shall act promptly to securely delete Police Data relating to a specific Data Subject at the request of any Controller.

8.5 The Processor's Project Manager will be responsible for ensuring the secure handling and subsequent deletion of the Police Data in accordance with the requirements of the Data Protection Legislation and any specific measures required by the Controller as identified at Schedule A.

8.6 Electronic copies of the data shall be securely destroyed by the Processor by either physical destruction of the storage media or secure deletion using an approved NCSC data cleansing product.

9 Security

9.1 The Processor recognises that the Controllers have obligations relating to the security of Data in their control, including under the Data Protection Legislation, ISO/IEC27001, ISO/IEC27002, PASF and equivalent standards, and the Information Community Security Policy for policing. The Designated Police Manager shall, on behalf of the Controllers, provide the Processor with copies of relevant policies, in so far as it is permitted to do so, and any amendments as may be made from time to time. In addition to complying with its own obligations under the Data Protection Legislation, the Processor shall continue to apply the obligations applicable to the Controller, including those detailed in this clause and the specific obligations detailed below, on behalf of the Controllers during the term of the Contract and this Agreement.

9.2 The Processor shall obtain independent certification of, or evidence that they are working towards ISO 27001, PASF or an equivalent standard as soon as reasonably practicable, and shall maintain such certification for the duration of the Contract and this Agreement.

9.3 Without prejudice to the generality of the requirements of clause 9.1 above, the Processor shall ensure for the duration of the Contract that, in respect of its System, and in accordance with Good Industry Practice and the Security Plan, it:

9.3.1 has appropriate network defence systems enabled;

9.3.2 maintains in place up to date patching and anti-virus policies and that performance against these is measured and monitored to ensure compliance;

9.3.3 has completed and shall comply with the terms of a Code of Connection Agreement which describes the minimum security requirements of the Processor System; and,

9.3.4 performs a risk assessment and that appropriate, prudent and cost-effective risk treatment measures have been applied.

9.4 Without prejudice to the generality of the requirements at clause 9.1 above, the measures imposed under clause 9.3 shall protect against:

9.4.1 the loss of integrity of Police Data;

9.4.2 the loss of confidentiality of Police Data;

9.4.3 the unauthorised access to, use of, or interference with Police Data by any person or organisation;

9.4.4 the unauthorised access to network elements, buildings, premises, sites and/or tools used by the Processor in the provision of the Services;

9.4.5 the use of the System or Services by any third party in order to gain unauthorised access to any computer resource or Police Data; and,

9.4.6 the loss of availability of Police Data due to any failure or compromise of the Services.

9.5 The Processor shall, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of Data Subjects having regard to the information detailed at Schedule A, implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a) the pseudonymisation and encryption of Personal Data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to Police Data in a timely manner in the event of a physical or technical incident;

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

9.6 The Processor shall in assessing the appropriate level of security take particular account of the risks that are presented by the processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Police Data transmitted, stored or otherwise processed.

9.7 The Processor shall, in accordance with its obligations under the Contract and this Agreement and in particular under clauses 9.1 – 9.5 above, develop a Security Plan detailing the technical and organisations measures it has imposed to ensure full compliance with its obligations and shall provide a copy of the Security Plan, together with documentation related to any other applicable security policies, practices and procedures, to the Designated Police Manager on behalf of the controllers within 20 Business Days of the commencement of this Agreement.

9.8 The Processor shall implement and maintain the Security Plan to apply during the term of the Contract and this Agreement and after the end of such term (as applicable) in accordance with an exit plan which shall be approved by the Controllers.

9.9 Incorporated as part of the Security Plan, the Processor warrants, represents and undertakes for the duration of the Contract and this Agreement that it shall have an up-to-date business continuity and disaster recovery plan in relation to the performance of the Services, availability of the System and Police Data, and compliance with its obligations under the Contract and this Agreement sufficient to enable it to maintain or promptly reinstate (within reasonable time periods) performance of the Services, availability of the System and Police Data and compliance with its obligations under the Contract and this Agreement in the event of a disaster or other business interruption ("Contractor BCDR Plan").

9.10 The Security Plan shall be written in plain English in language which is readily comprehensible to the staff of the Parties engaged in the Services and shall not reference any other documents which are not either in the possession of the Controllers or otherwise specified in the Contract or this Agreement.

9.11 In the event of any inconsistency in the provisions of the standards, guidance, policies and legislation detailed at clause 9.1 above, the Processor shall notify the Designated Police Manager on behalf of the Lead Controller of such inconsistency immediately upon becoming aware of the same, and the Designated Police Manager shall, as soon as practicable, advise the Processor which provision shall take precedence.

9.12 The Security Plan shall be fully reviewed and updated by the Contractor as necessary, and at least annually, to reflect:

9.12.1 emerging changes in Good Industry Practice;

9.12.2 any change or proposed change to the System, the Services and/or associated processes;

9.12.3 any new perceived or changed threats to the System; and

9.12.4 a reasonable request by the Controllers.

9.13 The Processor shall provide the Controllers with the results of such reviews as soon as reasonably practicable after their completion and shall make and implement appropriate amendments to the Security Plan at no additional cost to the Controllers.

9.14 Without prejudice to any other right of audit or access granted to the Controllers pursuant to the Contract and this Agreement, the Processor shall conduct tests of the processes and countermeasures contained in the Security Plan ("Security Tests") on an annual basis or as otherwise agreed by the Parties. The date, timing, content and conduct of such Security Tests shall be agreed in advance with the Designated Police Manager on behalf of the Lead Controller, at least 30 Business Days in advance. Security Tests shall be designed and implemented so as to minimise the impact on the Services. The Controllers shall be entitled to send a representative to witness the conduct of the Security Tests. In any event, the Processor shall provide the Controllers with the results of such tests as soon as practicable after completion of each Security Test.

9.15 Where any Security Test carried out pursuant to clauses 9.11 or 9.13 or audit performed pursuant to clause 6.17, reveals any actual or potential security failure or weaknesses, or any other breach by the Processor of its obligations under the Contract or this Agreement, the Processor shall promptly notify the Controllers of the changes to the Security Plan (and the implementation thereof) and/or other remedial action (as applicable) which the Processor proposes in order to correct such failure or weakness or remedy such breach, and shall implement and maintain such measures as soon as reasonably possible at no additional cost to the Controllers.

9.16 The Processor shall take all reasonable steps to ensure the reliability and integrity of any employees who have access to the Police Data and ensure that they:

(a) are aware of and comply with the Processor's obligations under the Contract and this Agreement;

(b) are subject to appropriate confidentiality undertakings with the Processor or any Sub-processor, as set out at Schedule C;

(c) are informed of the confidential nature of the Police Data and do not publish, disclose or divulge any of the Police Data to any third Party unless directed in writing to do so by the relevant Controller or as otherwise permitted by the Contract or this Agreement;

(d) have undergone adequate appropriate data protection training and specific instructions in respect of the secure handling of Police Data; and,

(e) do not transfer Personal Data outside of the European Economic Area unless the prior written consent of the relevant Controller has been obtained.

9.17 Access to the Police Data will be restricted to those employees of the Processor as listed at Schedule B and approved by the Controller, directly involved in the processing

of Police Data in pursuance of the Purpose and have appropriate confidentiality undertakings with the Controller and/or Processor in accordance with Schedule C.

9.18 The relevant Controller may wish to undertake suitability checks (including vetting) on any persons having access to the Police Data in accordance with Force Vetting Policy and further reserves the right to issue instructions that particular individuals shall not be able to participate in the Purpose without reasons being given for this decision. The Processor will ensure that each person who will participate in the Purpose understands this and provides their written consent as necessary.

9.19 The Processor will ensure that the Police Data accessed is not used other than as identified within this Agreement, and that the Contract and this Agreement are complied with.

9.20 The Controller reserves the right to undertake a review of security provided by the Processor and may request access to the Processor's premises for this purpose. Failure to provide sufficient guarantees to the Controller, in respect of adequate security policies, practices and procedures is likely to result in the suspension and/or termination of the Contract and this Agreement.

9.21 Without prejudice to the Processor's obligations under the Data Protection Legislation, this Contract and the Agreement, as to taking appropriate technical and organisational measures to ensure the integrity and security of the Police Data, the Processor hereto undertakes to comply with all or any reasonable requirements concerning the storage, access or use of any Police Data as may from time to time be made by the Controllers or by someone acting on their behalf.

9.22 Any access to the premises used to process the Police Data by maintenance or repair contractors, cleaners or other non-authorised persons must be closely supervised to ensure that there is no access to the Police Data and there is no breach of the agreed security arrangements. If in doubt, the Processor must consult with the relevant person appointed by the Controllers i.e. the Designated Police Manager.

9.23 During the term of this Contract, the Processor's Project Manager shall carry out such checks as are reasonably necessary to ensure that the above arrangements are not compromised.

10 Freedom of Information

10.1 The Processor acknowledges that the Controllers are subject to the requirements of the Code of Practice on Government Information, the Freedom of Information Act 2000 and the Environmental Information Regulations 2004 and shall assist and cooperate with the Controllers to enable them to comply with their Information disclosure obligations.

10.2 The Processor shall not respond directly to a Request for Information unless expressly authorised to do so by the relevant Controller(s).

10.3 Where the Processor receives a request for information under the provisions of the Freedom of Information Act 2000 or Environmental Information Regulations 2004 in respect of information provided by or relating to the Controller, the Contract or this Agreement, that request should be referred to the Designated Police Manager and/or the relevant Controller as soon as practicable and in any event within two Business Days of receipt.

10.4 The Processor shall and shall procure that any Sub-Processors shall:

10.4.1 provide the relevant Controller(s) and/or Designated Police Manager on behalf of the Lead Controller with a copy of all Information in its possession, or power in the form that the Controllers (acting reasonably) require within five Business

Days (or such other period as the Controllers may specify) of the Controller's request;

10.4.2 provide all necessary assistance as reasonably requested by the Controllers to enable them to respond to the Request for Information within the time for compliance set out in section 10 of the FOIA or regulation 5 of the EIR.

10.5 The Processor acknowledges that the Controllers may, acting in accordance with the Department of Constitutional Affairs' Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the Freedom of Information Act 2000, be obliged under the FOIA or the EIR to disclose information concerning the Processor or the Services:

10.5.1 in certain circumstances without consulting the Processor; or

10.5.2 following consultation with the Processor and having taken the Processor's views into account,

provided always that where clause 10.5.1 applies the relevant Controller shall, in accordance with any recommendations of the Code referred to above, take reasonable steps, where appropriate and without putting itself in breach of any applicable Law, to give the Processor advanced notice, or failing that, to draw the disclosure to the Processor's attention after any such disclosure.

10.6 Notwithstanding any other provision in the Contract, this Agreement or any other agreement between the Parties, the Processor acknowledges and agrees that the Controllers are responsible for determining in their absolute discretion whether any Commercially Sensitive Information and/or any other Information is exempt from disclosure in accordance with the provisions of the Code of Practice on Government Information, the FOIA or the EIR.

10.7 The Processor shall ensure that all Information is retained for disclosure as required by Law and shall permit the Controllers to inspect such records as requested from time to time.

10.8 This clause 10 shall survive termination of the Contract and this Agreement and continue in full force and effect.

11 **Deed of Indemnity**

11.1 In consideration of the provision of the Police Data for the "Purpose", the Processor shall, immediately on demand, fully indemnify each Controller and keep each Controller fully and effectively indemnified and hold it harmless from and against all costs, claims, demands, expenses (including legal costs and disbursements), losses, actions, damages, proceedings and liabilities of whatsoever nature suffered or incurred by the relevant Controller arising directly or indirectly as a result of any breach by the Processor of its obligations under the Contract or this Agreement.

11.2 Neither Party excludes or limits its liability to the other Party for:

(a) death or personal injury caused by its negligence, or that of its employees, agents or sub-contractors;

(b) bribery, fraud or fraudulent misrepresentation by it or its employees; or

(c) any other matter which, by Law, may not be excluded or limited.

11.3 The above indemnity shall have no effect on any criminal proceedings arising from any breach of the Data Protection Act 2018.

12 **Disputes**

12.1 In the event of any dispute or difference arising between the Parties out of the Contract or this Agreement, the persons appointed pursuant to clause 6.11 of this Agreement and those representing the Parties to the dispute or difference shall within 20 days of receipt of a written request from any party to the dispute addressed to one of the individuals described at clause 6.11 meet in an effort to resolve the dispute or difference in good faith.

13 Term Termination and Variation

13.1 This Agreement shall commence on signature and shall continue for the duration of the Contract, whichever is the earlier.

13.2 In the event that any Party wishes to exit from this Agreement, that Party shall serve a notice, in writing, to the offices of the other party of a date not less than 30 days from the date of the said notice, on which the Party proposes to exit this Agreement. However, the Controller may at any time by notice in writing terminate this Agreement forthwith if the Processor is in breach of any material obligation under this Agreement.

13.3 In the event that either Party wishes to vary any term of this Agreement that Party will give notice, in writing to the offices of the other party, explaining the effect of and reason for the proposed variation. The Parties shall within 30 days of receipt of such a notice meet to discuss the variation.

13.4 The Controller will have the final decision on any proposed variation to this Agreement. No variation of the Contract shall be effective unless it is contained in a written instrument signed by all Parties and annexed to this Agreement.

14 Miscellaneous

14.1 This Agreement acts in fulfilment of part of the responsibilities of the Controller as required by Articles 28 and 29 and Recital 81 of the GDPR and the Data Protection Act 2018.

14.2 This Agreement and the Contract constitute the entire agreement between the Parties as regards the subject matter hereof and supersedes all prior oral or written agreements regarding such subject matter.

14.3 If any provision of this Agreement is held by a Court of competent jurisdiction to be invalid or unenforceable, such invalidity or unenforceability shall not affect the remaining provisions of the Contract or this Agreement, which shall remain in full force and effect.

14.4 The validity, construction and interpretation of this Agreement and any determination of the performance which it requires shall be governed by the Laws of England and the Parties hereby submit to the exclusive jurisdiction of the English Courts.

Schedule A

DETAILS OF POLICE DATA TO BE PROCESSED BY THE PROCESSOR ON BEHALF OF THE CONTROLLER.

1. The Processor shall comply with any further written instructions with respect to processing from the Controller.

2. Any such further instructions shall be incorporated into this schedule.

Details of the Designated Police Manager (DPM)	[redacted]
Third Party details (if applicable)	OPCC, Complaints Resolution Team
Third Party Project Manager (if applicable)	[redacted], OPCC
Subject matter of the Processing	The OPCC Complaints Resolution Team will access Cleveland Police systems to obtain information required for the purposes of handling and resolving complaints.
Duration of the Processing	The processing shall commence on the data of this contract and shall expire at an indeterminate date, should the OPCC complaints handling model change format.
Purposes of the Processing	The purpose of the processing is to ensure timely access for the OPCC to obtain the information they need to handle and resolve complaints. The system access, retrieval and extraction of data are the data processing activities, to avoid the need to request the data from Cleveland Police employees and await receipt of said data.
Nature of the Processing	The OPCC Complaints Resolution Team will access the following systems: **Centurion** – includes consultation of previous complaints for the purposes of assisting the handling of new complaints, and creation of new complaint records. **Niche** – read only access to look up details that may be applicable to an event attended / handled by Cleveland Police for the purposes of handling a specific complaint. **Webstorm** - read only access to look up details that may be applicable to an event attended / handled by Cleveland Police for the purposes of handling a specific complaint. **Red Box** – to access call recordings that may be applicable to an event attended / handled by Cleveland Police for the purposes of handling a specific complaint. **BWV footage -** recordings that may be applicable to an event attended / handled by Cleveland Police for the purposes of handling a specific complaint. **E-Duty –** for consultation as to when Officers are on duty

	DMS Service and Duties – for consultation as to when Officers are on duty and their supervision chain. Information from all of the above systems may be copied and saved against the policy log to keep a record of team member activities undertaken in order to try and resolve the complaint. The Data Processor is not permitted to access any other records from these systems for any other purpose. The Information Sharing Agreement covers the OPCC's lawful basis for using the information once obtained.
Type of Personal Data	Complaints data will include: Names, DOB, address, and protected characteristics are recorded. PC data that is collected includes: sex, gender, sexual orientation, disability, ethnicity, faith/ religious belief, and pregnancy and maternity status. Data from the above mentioned systems. Criminal offence and employees related data will likely also be captured from the above mentioned systems.
Categories of Data Subject	The categories of data subject whose data will be processed include: Members of public, employees, suspects, victims, witnesses and potentially colleagues from partner organisations.
Arrangements for return or destruction of the data once processing is complete	Data extracted by the OPCC from Police systems will be saved to the Policy log within Centurion. The retention of this data will be covered by the OPCC Retention Schedule

Schedule B

INDIVIDUALS EMPLOYED BY THE PROCESSOR AUTHORISED TO PROCESS THE POLICE DATA FOR THE PURPOSE

1. Access to the Police Data will be restricted to only those employees of the Processor or sub Processor as listed below and approved by the Controller, as being directly involved in the processing of Police Data in pursuance of the purpose.

Name	Position	Organisation

Schedule C

UNDERTAKING OF CONFIDENTIALITY

I [INSERT NAME] as an employee of the Processor as defined in the Contract between the Controllers and [INSERT PROCESSOR] to which this Undertaking is appended, hereby acknowledge the responsibilities arising from this Contract.

I understand that my part in fulfilling the Purpose means that I may have access to the Police Data and that such access may include:

a) reading or viewing of information held on computer or displayed by some other electronic means; or

b) reading or viewing manually held information in written, printed or photographic form.

c) overhearing any radio, telephone or verbal communication

I undertake that:

1. I shall not communicate to nor discuss with any other person the contents of the Police Data except to those persons authorised by the Controller as is necessary to progress the agreed Purpose.

2. I shall not retain, extract, copy or in any way use any Police Data to which I have been afforded access during the course of my duties for any other purpose.

3. I will only operate computer applications or manual systems that I have been trained to use. This training has included the requirements of the Data Protection Legislation which prescribes the way in which personal data may be obtained, stored and processed.

4. I will comply with the appropriate physical and system security procedures made known to me by the Designated Police Manager.

5. I will act only under instruction from the Designated Police Manager or other relevant official in the processing of any Police Data.

I understand that the Police Data is subject to the provisions of the Data Protection Legislation and that by knowingly or recklessly acting outside the scope of this Contract I may incur criminal and/or civil liabilities.

I undertake to seek advice and guidance from the Designated Police Manager or other relevant official of the Controller in the event that I have any doubts or concerns about my responsibilities or the authorised use of the Police Data defined in the Contract.

I have read, understood and accept the above.

Name:

Processor company details:

Signed (Employee) ……..

Date ……..

Signed (Project Manager) ……..

Date ……..

Signed on behalf of the Chief Constable of Cleveland Police

Name: [redacted]

Position: [redacted]

Date: 18 November 21

Signed on behalf of the Office of the Police and Crime Commissioner for Cleveland

Name: [redacted]

Position: [redacted]

Date: 2 November 2021