Data Processing Agreement

1. Definitions and Interpretation

1.1 In this agreement, the following terms shall have the meaning set out below:

Authority means North Somerset Council

Authority Data means any 'information' provided by, obtained or created on behalf of North Somerset Council in delivering the services specified in this contract; and in the case of Personal Data, any data processed on behalf of North Somerset Council where North Somerset Council is the data controller.

Caldicott Principles (1997, 2012 & 2016) means the Caldicott principles which protect patient identifiable data. These principles are applicable to any processing of health or social care data.

Data Controller means the role as defined Article 4, paragraph 7 of the GDPR

Data Processor means the role as defined Article 4, paragraph 8 of the GDPR

Data Protection Act 2018 (DPA) means the Data Protection Act 2018 (DPA).

Data Protection Officer (DPO) means the role as defined under Chapter IV, Articles 37 – 39 of GDPR.

Environmental Information Regulations 2004 (EIR) means the Environmental Information Regulations 2004 (EIR) as amended or re-enacted from time to time and any Act substantially replacing the same.

Freedom of Information Act 2000 (FOIA) means the Freedom of Information Act 2000 (FOIA) as amended or re-enacted from time to time and any Act substantially replacing the same.

Good Industry Practice means the exercise of the degree of skill, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced Processor engaged in the same type of undertaking under the same or similar circumstances as are contemplated by this agreement.

General Data Protection Regulation (GDPR) means the European General Data Protection Regulation (2016), Regulation (EU) 2016/679, as amended or re-enacted from time to time and any United Kingdom Act or European Union Regulation recognised in UK law substantially replacing the same – see UK GDPR.

Information has the meaning given under Section 84 of the Freedom of Information Act 2000 (FOIA), which shall include (but is not limited to) information in any form whether relating to the past, present or future and may in particular consist of data, documentation, programs, (including the source code of any programs which the Authority has the right to use), computer output, voice transmissions, correspondence, calculations, plans, reports, graphs, charts, statistics, records, projections, maps, drawings, vouchers, receipts and accounting records and may consist of or be stored in any form including paper, microfilm, microfiche, photographic negative, computer software and any electronic medium and references herein to Information shall include reference to the medium in which it is stored.

Information Legislation means the DPA, FOIA, GDPR, UK GDPR and the EIR.

Information Governance Requirements means the documented set of additional information governance requirements which the Authority applies within itself and requires of its Processors and of which it has furnished a copy to the Processor via information governance.

Legislation for the avoidance of doubt includes all Law in particular the Information Legislation.

Personal Data means Personal Data as defined in Sections 3(2) and (3) of the DPA and Article 4(2) of the GDPR, which is supplied to the Processor by North Somerset Council or obtained by the Processor in the course of performing the services.

Processor means the Data Processor to which this agreement applies.

Subject Access Request means a request for Personal Data falling within the provisions of Articles 12 and 15 of the GDPR

UK GDPR: The GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland through operation of section 3 of the European Union (Withdrawal) Act 2018.

2. Resolution of Inconsistency

2.1 The Processor shall immediately upon becoming aware of the same, notify the Authority of any inconsistency between its practices and the provisions of Information Legislation, including related regulation, standards, guidance and policies applicable under this schedule and compliance statements made by the processor during the contract procurement process.

2.2 Where notified or it otherwise becomes aware of inconsistency, the Authority, as soon as practicable, shall advise the Processor with which provision the Processor shall be required to comply (but not so as to place the Processor in breach of any legislation) by means of an action plan which:

2.2.1 specifies the inconsistency and articulates the resulting risks posed to the Authority's compliance with the Legislation.

2.2.2 explains how the requirement to resolve the inconsistency meets the contractual requirements and the statements of compliance made during the contract procurement process.

2.2.3 specifies the time period which in the Authority's opinion is reasonable in which to resolve the inconsistency.

2.2.4 explains the means by which the Authority intends to satisfy itself that the inconsistency is resolved and specifies the steps the Processor is required to take to facilitate any assessment.

2.2.5 takes into account the opinion of the Processor on the level of resource required to resolve the inconsistency.

2.3 Where inconsistencies are not resolved within the expectations set out in paragraph 2.2, the Authority may use the dispute resolution provisions of this contract.

3. Protection of Information

3.1 The Processor acknowledges that the confidentiality, integrity and availability of information and on the security provided in relation to Information is a material element of this agreement.

3.2 The Processor shall and shall at all times provide a level of security which:

3.2.1 is in accordance with Legislation and this contract;

3.2.2 is in accordance with compliance regimes representing Good Industry Practice which the Authority may specify;

3.2.3 complies with the information governance requirements, and

3.2.3 meets any specific security threats identified from time to time by the Authority.

3.3 The Processor shall ensure that it provides comparable technical and policy coverage of security to information as if it were being processed directly by the Authority. This shall include but not limited to the following:

3.3.1 All mobile storage systems and hardware shall be encrypted to the standards laid out by the National Cyber Security Centre in its Device Security Guidance.

3.3.2 When data is to be sent out, every effort should be made to use electronic transfer methods via a secure email portal, or by encrypted email using native TLS v1.2 or other secure mechanism such as Egress.

3.3.3 When data is being emailed, every effort should be made to reply to an email, rather than free-typing an email address.

3.3.4 Where electronic transfer is not possible, Personal Data must be sent using Royal Mail recorded delivery, with the recipient address checked by at least two individuals prior to posting.

3.3.5 All employees shall be appropriately vetted before use in the services which are the subject of this agreement.

3.3.6 All employees shall receive adequate information governance training which shall be refreshed over a period of no longer than every twelve months, and assurances will be provided to the Authority in this regard.

3.3.7 The Authority reserves the right to see evidence of training completion for all employees subject to this agreement.

3.3.8 All buildings and physical environments shall be subject to appropriate physical security and protection.

3.3.9 When handling NHS data, the Processor shall apply safe haven usage to at least NHS standard and comply with the requirements of the Caldicott Principles.

3.3.10 The Processor shall only permit access to information by individuals as authorised by the Authority.

3.3.11 The Processor shall securely destroy all information provided or created under this agreement which is no longer required to be retained in accordance with this agreement and shall provide confirmation to the Authority that it has been destroyed.

3.4 The Processor will have in place fully tested and effective disaster recovery and business continuity plans.

3.5 The Processor shall observe the following principles when handling Personal Data for the purpose of carrying out the Processor's obligations under this agreement.

3.5.1 Every proposed processing of Personal Data within or outside the Processor's organisation should be clearly defined and regularly risk assessed and approved by an appropriate information governance role holder.

3.5.2. Personal data must not be processed unless it is absolutely necessary. Personal data should not be used unless there is no alternative.

3.5.3 The minimum necessary Personal Data is to be used. Where the use of Personal Data is considered necessary, each individual item of information should be justified with the aim of reducing the need for processing personally identifiable information.

3.5.4 Access to Personal Data should be on a strict need to know basis. Employees should only have access to the data that they need to see, and should only receive the access and functionality permissions required to undertake their roles.

3.5.5 The Processor must ensure that its employees are aware of their responsibility to comply with the common law duty of confidentiality.

3.5.6 All persons handling Personal Data must understand and comply with the Information Legislation. All processing of Personal Data must be lawful.

3.6 Any information received by the Processor from the Authority under this agreement or generated by the Processor pursuant to this agreement shall remain at all times the property of the Authority. It shall be identified, clearly marked and recorded as such by the Processor on all media and in all documentation.

3.7 The Processor shall not, save as required by this agreement, without the prior written consent of the Authority disclose to any other person any information provided by the Authority under this agreement unless required to do so by law.

3.8 Where processing Personal Data, the Processor shall not procure the services of any other agent or sub-Processor in connection with this agreement without the explicit written consent of the Authority.

3.9 The Processor shall observe and comply with the Authority's security classification/ protective marking scheme as defined within its information governance requirements. For clarity, the Authority observes the Government's Security Classifications Policy and only handles information classified up to a level of OFFICIAL.

3.10 The Processor shall take all necessary precautions to ensure that all information obtained from the Authority under or in connection with this agreement, is given only to such of the Processor's employees and professional advisors or consultants engaged to advise the Processor in connection with this agreement as is strictly necessary for the performance of this agreement, and is treated as confidential and not disclosed (without prior written approval) or used by any such employees or such professional advisors or consultants otherwise than for the purposes of this agreement.

3.11 The Processor shall not use any information it receives from the Authority otherwise than for the purposes of this agreement.

3.12 With regard to Authority data:

3.12.1 The Processor shall not delete or remove any proprietary notices contained within or relating to the Authority data.

3.12.2 The Processor shall not store, copy, disclose, or use the Authority data except as necessary for the performance by the Processor of its obligations under this agreement or as otherwise expressly authorised in writing by the Authority.

3.12.3. To the extent that Authority data is held and/or processed by the Processor, the Processor shall supply that Authority data to the Authority as requested by the Authority in the format it is held.

3.12.4. The Processor shall take responsibility for preserving the integrity of Authority data and preventing the corruption or loss of Authority data.

3.12.5 The Processor shall perform secure back-ups of all Authority data and shall ensure that up-to-date back-ups are stored offline and, where relevant, off-site, in accordance with the business continuity and disaster recovery plan. The Processor shall ensure that such backups are available from which to recover Authority data as and when necessary.

3.12.6 The Processor shall ensure that any system on which the Processor holds any Authority data, including back-up data, is a secure system that complies with the Authority's information governance requirements.

3.12.7 If the Authority data is corrupted, lost or sufficiently degraded as a result of the Processor's default so as to be unusable, the Authority may:

3.12.7.1 require the Processor (at the Processor's expense) to restore or procure the restoration of Authority data in full and in not later than three days (subject to any agreed business continuity and disaster recovery plan); and/or

3.12.7.2 in default thereof itself restore or procure the restoration of Authority data, and shall be repaid by the Processor any reasonable expenses incurred in doing so.

3.12.8 If at any time the Processor suspects or has reason to believe that Authority data has or may become corrupted, lost or sufficiently degraded in any way for any reason, then the Processor shall notify the Authority immediately and inform the Authority of the remedial action the Processor proposes to take.

4. Data Protection

4.1 The Authority is and will remain the Data Controller in relation to the personal information processed under this agreement, and that the Processor will act as Data Processor with respect to such personal information. As such, the Processor must follow the direction of the Authority as to how Personal Data is processed.

4.2 All Personal Data acquired by the Processor from the Authority shall only be used for the purposes of this agreement and shall not be further processed or disclosed without the prior written consent of the Authority.

4.3 The Processor shall comply with the GDPR requirements with regard to appointing a Data Protection Officer.

4.4 The Processor warrants that it has complied with its notification requirements under the DPA to undertake the subject matter of this agreement.

4.5 The Processor shall comply with all relevant codes of practice issued under the DPA and GDPR.

4.6 The Processor shall assist the Authority in safeguarding the legal rights of the data subject.

4.7 The Processor will have in place at all times appropriate technical and organisational security measures to safeguard Authority data in compliance with Information Legislation and National Cyber Security Centre (NCSC) guidance.

4.8 The Processor shall indemnify the Authority against loss, destruction or processing contrary to information legislation by itself, its employees, sub-Processors or agents.

4.9 The Processor shall ensure the reliability and ongoing training of all its relevant employees to ensure awareness of and compliance with the Processor's obligations under the Information Legislation.

4.10 The Authority shall respond to all Subject Access Requests (SAR), whether received by the Processor or the Authority.

4.10.1 On receipt of a SAR made directly to it, the Processor will forward the request immediately, and no later than two working days after receipt, to the council's Information Governance team (foi@n-somerset.gov.uk)

4.10.2 If requested by the council, the Processor shall provide to the Authority the Personal Data requested by the data subject (as defined in the DPA) within 10 working days of receipt of instruction by the Authority for supply of the data.

4.10.3 The information shall be supplied to the council in .xlsx, .docx or .pdf form in full, with any proposed redactions highlighted.

4.11 The Processor shall immediately and no later than two working days after receipt, forward to the council's Information Governance team (foi@n-somerset.gov.uk):

4.11.1 a request from any person whose Personal Data it holds to access his or her Personal Data; or

4.11.2 a written complaint or request relating to the Authority's obligations under the Information Legislation.

4.12 The Processor will assist and co-operate with the Authority in relation to any complaint or request received, including:

4.12.1 providing full details of the complaint or request;

4.12.2 providing the Authority with any information relating to a SAR within 10 working days of receipt of the request;

4.12.3 promptly providing the relevant service manager with any Personal Data and other information requested by them in writing.

4.12.4 respond to any further requests from the council's Data Protection Officer when investigating information security incidents.

4.13 In addition to the obligation undertaken in paragraph 3.8, the Processor shall not further process information outside of the UK as defined by DPA and GDPR without full prior written consent from the Authority.

4.14 The Processor shall cooperate with data protection compliance audits as and when requested by the Authority.

4.15 The Processor shall comply with Information Legislation requirements for maintaining accurate, current and comprehensive records of processing activities.

5. Caldicott Principles

The Processor must also observe the Caldicott Principles when processing health and/or social care data, which are set out below.

1. Justify the purpose(s)
Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

2. Don't use personal confidential data unless it is absolutely necessary

Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

3. Use the minimum necessary personal confidential data
Where use of personal confidential data is considered to be essential, the inclusion of each discrete item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function.

4. Access to personal confidential data should be on a strict need-to-know basis
Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

5. Everyone with access to personal confidential data should be aware of their responsibilities
Action should be taken to ensure that those handling personal confidential data, both clinical and non-clinical employees, are made fully aware of their responsibilities and obligations to respect patient confidentiality. **6. Comply with the law**
Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

7. The duty to share information can be as important as the duty to protect patient confidentiality.
Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

8. Inform patients and service users about how their confidential information is used.
A range of steps should be taken to ensure no surprises for patients and service users, so they can have clear expectations about how and why their confidential information is used, and what choices they have about this. These steps will vary depending on the use: as a minimum, this should include providing accessible, relevant and appropriate information - in some cases, greater engagement will be required.

6. The FOIA and the EIR

6.1 The Authority is subject to the provisions of the FOIA and the EIR and the Processor shall assist the Authority (at the Processor's expense) to enable the Authority to comply with these Acts. The Processor acknowledges that the Authority may be obliged to disclose information relating to this agreement. Notwithstanding any other term of this agreement, the Processor hereby gives its consent for the Authority to publish this agreement in its entirety, including from time-to-time agreed changes to the agreement, to the general public in whatever form the Authority decides.

6.2 The Processor must transfer any request for information under FOIA and EIR to the Authority as soon as practicable after receipt and in any event within two working days of receipt.

6.3 Where the Authority so requires for the purpose of compliance with the FOIA and EIR, the Processor shall provide the Authority with a copy of all Information in its possession or power, in the form that the Authority requires, within 10 working days (or such other reasonable period as the Authority may specify) of the Authority requesting the information.

6.4 Without prejudice to paragraph 6.6 and subject to paragraph 6.8 below, where the Processor believes the disclosure of information would prejudice its commercial interests or constitute an actionable breach of confidentiality, the Authority shall consider any case made where it is provided within 10 working days (or such other reasonable period as the Authority may specify) of the Authority requesting the information.

6.5 The Processor shall provide all necessary assistance as requested by the Authority under paragraph 6.3 above so as to enable the Authority to respond to a request for information within the time for compliance set out in section 10 of the FOIA or regulation 5 of the EIR.

6.6 As between the parties, the Authority will determine at its absolute discretion whether any information is exempt from disclosure in accordance with the provisions of the FOIA or the EIR.

6.7 In no event will the Processor respond directly to a request for information unless expressly authorised to do so by the Authority, save to acknowledge receipt (if so requested by the Authority).

6.8 The Processor acknowledges that the Authority may be obliged under the FOIA or the EIR to disclose information without consulting with the Processor, or following consultation with the Processor and having taken its views into account.

6.9 The Processor must ensure that all Information produced in the course of this agreement or relating to this agreement is retained for disclosure in line with the Authority's policy on information retention periods and must permit the Authority to inspect such records as requested from time to time.

6.10 The Processor acknowledges that any lists or schedules provided by it outlining confidential information are of indicative value only and that the Authority may nevertheless be obliged to disclose confidential Information.

7. Disclosures by the Authority

7.1 Nothing in this agreement shall prevent the Authority disclosing any Information:

7.1.1 for the purpose of the examination and certification of the Authority's accounts; or

7.1.2 any examination pursuant to Section 6 (1) of the National Audit Act 1983 of the economy, efficiency and effectiveness with which the Authority has used its resources; or

7.1.3 to any government department or any other contracting Authority (as defined in The Public Contracts Regulations 2006). All government departments or contracting authorities receiving such confidential information shall be entitled to further disclose the confidential information to other government departments or other contracting authorities on the basis that the information is confidential and is not to be disclosed to a Processor which is not part of any government department or any contracting Authority; or

8. Accessibility of data

Where the Processor is undertaking work on behalf of the Authority to develop new systems, practices or documentation in processing of data, the Processor shall ensure that there remains the ability to extract data in a format accessible to and useable by the Authority (with regard to paragraph 11.3) supported by an Impact Assessment which is approved by the Authority.

9. Know-how

Nothing in this agreement shall prevent either party from using any techniques, ideas or know-how gained during the performance of this agreement in the course of its normal business, to the extent that this does not result in a disclosure of Information the subject of this agreement.

10. Information breaches

10.1 The Processor shall ensure all losses or breaches of security or information are reported to the Authority (foi@n-somerset.gov.uk) within 24 hours whether actual, potential or attempted, in order for the Authority to notify the regulator and, where necessary, the data subjects, as required by Information Legislation.

10.2 The Processor will ensure all major breaches are internally investigated, and appropriate remedial action taken, along with supporting the Authority and the Information Commissioner's Office in any investigation by it. A copy of the investigation report must be provided to the Authority.

10.3 The Processor will immediately take all reasonable steps to remedy such breaches and to protect the integrity of both parties against any actual, potential or attempted breach or threat and any equivalent attempted breach in the future.

11. Breach, termination and continuance

11.1 The Processor shall indemnify the Authority for any breach of the requirements of this schedule which renders the Authority liable for any costs, fines, claims or expenses under legislation howsoever arising.

11.2 Failure on the part of the Processor to comply with the provisions of this schedule shall amount to a breach of this contract and shall give the Authority the right to exercise any and all of the remedies in this contract and recover all costs incurred as a consequence of the Processor's breach.

11.3 On termination of this agreement howsoever arising the Processor shall, when directed to do so by the Authority, and instruct all its agents and sub-Processors to:

11.3.1 transfer to the Authority the whole or any part of the Personal Data and other Information received or acquired by the Processor for the purposes of or in the course of the delivery of the services the subject of this agreement; and

11.3.2 ensure that such a transfer is made securely in a manner specified by the Authority and the data complies with the requirement at paragraph 7; and

11.3.3 securely destroy or erase the whole or any part of such Personal Data and other Information retained by the Processor and provide to the Authority such proof of destruction as the Authority may reasonably specify.

11.4 The provisions of this paragraph shall continue in effect notwithstanding termination of this agreement.

Appendix A: Data Processing Schedule

The Provider shall comply with any further written instructions with respect to processing by the Council. Any such further instructions shall be incorporated into this Schedule.

Description	Details
Names of Parties	1. North Somerset Council 2. Public Perspectives Ltd.
Purpose	To deliver a survey to households in North Somerset.
Subject matter of the processing	Personal data will be processed by Public Perspectives Ltd. for the specific purposes of administering a health and wellbeing survey for North Somerset Council
Duration of the processing	The contract term is 4 months
Nature and purposes of the processing	Purpose of the processing: Creating a random sample to distribute a household survey to 5000 homes across North Somerset. This will involve the use of mail files and the land gazetteer to create a mail list for the purposes of sending the survey and any follow up to encourage participation. Any PID will be shared via secure means and only with agreed third party suppliers that are supporting the survey distribution and data analysis.
Type of Personal Data	This will include *telephone number, religion, ethnicity, postcode, information about health conditions, behaviours. Protected characteristics demographics.*
Categories of Data Subject	This may include persons taking part in survey and family members
Plan for return and destruction of the data once the processing is complete unless a requirement under EU or member state law to preserve that type of data	The Processor shall retain such documents and records in accordance with its obligations under the Data Protection Act 2018. Subject to the legal obligations, upon termination of the contract the Personal Data shall be returned to the customer and any copies held by the Processor shall be securely destroyed.

Signed for and on behalf of **Data Controller** North Somerset Council	Signed for and on behalf of **Data Processor Public Perspectives Ltd.**

Authorised Signatory **Signature**___*Rebecca Keating*_____ **Name:** Rebecca Keating **Position:** Service Leader Public Health **Date:** 09/10/24	Authorised Signatory **Signature**__*Mark Yeadon* **Name:** Mark Yeadon **Position:** Director **Date:** 14/10/24