THIS AGREEMENT is dated day of 2024

BETWEEN:

(1) NOTTINGHAM CITY COUNCIL of Loxley House, Station Street, Nottingham NG2 3NG (the “Council”); and

(2) [PROVIDER NAME] of [ADDRESS] being a company registered in England and Wales under Company Number [INSERT Co No] (the “Provider”)

WHEREAS:

(A) The Data Protection Legislation requires that where a Data Controller uses a Data Processor it must have a written contract (or other legal act) in place to evidence and govern their relationship.

(B) The Council has engaged the Provider to carry out the processing activities as set out in Annex 1.

(C) The Parties agree to comply with the provisions of this Agreement in respect of the Personal Data and the processing activities.

NOW IT IS AGREED AS FOLLOWS:

1. In this Agreement unless the context requires the following will have the meanings set out below:

|  |  |
| --- | --- |
| **“Controller”** | has the meaning given in the Data Protection Legislation |
| **“Data Protection Impact Assessment”** | An assessment by the Controller of the impact of the envisaged processing on the protection of the Personal Data |
| **“Data Protection Legislation”** | For the periods in which they are in force in the United Kingdom, the Data Protection Act 1998, the EU Data Protection Directive 95/46/EC, the Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practices)(Interception of Communications) Regulations 2000, the Electronic Communications Data Protection Directive 2002/58/EC, the Privacy and Electronic Communications (EC Directive) Regulations 2003, DPA 2018, the GDPR and all applicable laws and regulations relating to processing of personal data and privacy including all applicable guidance, codes of practice issued by the Information Commissioner, in each case as amended or substituted from time to time. |
| **“Data Subject”** | Means an individual who is the subject of Personal Data |
| **“DPA 2018”** | Means the Data Protection Act 2018 which subject to Royal Assent comes into force on 25th May 2018 and any equivalent legislation amending or replacing the DPA 2018 |
| **“GDPR”** | Means (a) the general Data Protection Regulations (Regulation (EU) 2016/679) which comes into force on 28 May 2018 and (b) any equivalent legislation amending or replacing the General Data Protection Regulations (Regulation (EU) 2016/679) |
| **“Law”** | means any applicable Act of Parliament, sub-ordinate legislation within the meaning of section 21(1) of the Interpretation Act 1978, exercise of the Royal Prerogative, enforceable Community right within the meaning of section 2 of the European Communities Act 1972, bye-laws, regulatory policy, guidance or industry code, judgment of a relevant Court of Law, or directives or requirements of any regulatory body of which the Provider or its Staff are bound to comply. |
| **“Personal Data”** | has the meaning given in the Data Protection Legislation |
| **“Personal Data Breach”** | Has the meaning as set out in the Data Protection Legislation |
| **“Processor”** | has the meaning given in the Data Protection Legislation |
| **“Protective Measures”** | Appropriate technical and organisation 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 measures adopted by it |
| **“Staff”** | means all persons employed by the Provider (including volunteers, agency, locum, casual or seconded personnel) in the provision of any services or any activity related to or connected with the provision of any services |

2. The Parties acknowledge that for the purpose of this Agreement and the Data Protection Legislation, the Council is the Controller and the Provider is the Processor.

3. The Provider is only authorised by the Council and shall only process Personal Data in accordance with the Council’s instructions as set out in Annex 1 (which may be amended from time to time), unless the Provider is otherwise required to do so by Law. Where the Processor is relying on Law with regard to the processing of Personal Data it shall notify the Council of this prior to any processing taking place.

4. The Council will ensure that it has all necessary and appropriate consents and notices in place to enable lawful transfer of the Personal Data to the Provider for the duration and purposes of this Agreement.

5. If required the Provider shall, prior to the commencement of any processing, provide all reasonable assistance to the Council in the preparation of any Data Protection Impact Assessment. Such assistance may include:

5.1 a systematic description of the envisaged processing operations and the purpose of the processing;

5.2 an assessment of the necessity and proportionality of the processing operations in relation to the Services being provided by the Provider;

5.3 an assessment of the risks to the rights and freedoms of Data Subjects; and

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

6. The Provider shall notify the Council immediately if it considers any instructions from the Council to be in breach of Data Protection Legislation.

7. The Provider, in respect of any processing of Personal Data under this Agreement shall:

7.1 have in place, and maintain, Protective Measures, reviewed and approved by the Council from time to time to ensure levels of security. Such measures to protect against unauthorised or unlawful processing of Personal Data and against accidental loss or destruction of or damage to Personal Data (such measures having taken into regard the nature of the data to be protected, the state of technological development and the cost of implementation);

7.2 not transfer Personal Data outside of the European Economic Area unless with the prior written consent of the Council, and subject to the Council and Processor being satisfied that sufficient safeguards are in place in respect of the transfer of the Personal Data and to protect the rights of the Data Subject;

7.3 delete or return all Personal Data (including copies of it) to the Council when the retention period expires or on termination of this Agreement(whichever takes place first) unless the Provider is required by Law to retain the same.

8. The Provider shall ensure that its Staff:

8.1 only process Personal Data in accordance with this Agreement;

8.2 are aware of and comply with the Provider’s duties under this Agreement;

8.3 enter into and be subject to, as appropriate, confidentiality agreements with the Provider or any sub-contractor;

8.4 are made fully aware of the confidential nature of the Personal Data and not to publish, disclose or divulge any of the Personal Data to a third party unless directed to do so under this Agreement;

8.5 have undergone appropriate training in the use, care, protection and handling of Personal Data.

9. The Provider shall notify the Council within two (2) working days and shall

provide full assistance and further information if it receives:

9.1 a request for Personal Data from a Data Subject;

9.2 a request to rectify, block or erase any Personal Data;

9.3 any other request in relation to the Council or Provider’s

obligations under Data Protection Legislation;

9.4 any communication from the Information Commissioner, or

regulations authority in connection with Personal Data being

processed under this Agreement;

9.5 a request from any third party for disclosure of Personal Data which

disclosure is required by Law.

10. The Provider shall notify the Council without delay and in any event within 24

hours upon becoming aware of a Personal Data Breach or loss of Personal Data processed under this Agreement in order to enable the Council to report the breach to the Information Commissioners Office within the 72 hour deadline imposed by the GDPR and to assist the Council, as directed, in the investigation, mitigation and remediation of any Personal data Breach.

11. In the event of any personal data breach the Provider shall assist the Council in issuing any notifications to data subjects.

12. The Provider shall keep and maintain accurate records and information to

demonstrate compliance with its obligations under this Agreement and any

additional Data Protection Legislation obligations.

13. It shall be at the Council’s sole discretion as to whether it consents to any

processing being conducted by a third party Sub-Processor. If the Provider

requires any processing to be undertaken by a sub-contracted third party it must

first seek the written agreement of the Council and the Provider shall enter into

an appropriate written agreement with the Sub-Processor with processing obligations no less onerous than as set out in this Agreement. For the avoidance of doubt the Provider shall remain fully liable to the Council in respect of all acts or omissions of the Sub-Processor.

AS WITNESS the hands of the parties

SIGNED for and on behalf

of the Council

Authorised signatory

SIGNED for and on behalf

of the Provider

Authorised signatory

**ANNEX 1**

**Data Processing Instructions**

Here you must include and clearly set out the following if there will be any processing of data:

|  |  |
| --- | --- |
| **Description:** | **Scope:** |
| Subject Matter | *High level short description of what the processing is about* |
| Duration: | *This is likely to be the Contract Period but if different insert the specific dates*  *Also set out any retention periods that may apply* |
| Nature and Purpose of the Processing | *Be as specific as possible including all intended purposes so e.g.*  *Nature could be = collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data.*  *Purpose could be = employment processing, statutory obligation, data transfer etc* |
| Type of Personal Data | *e.g. name, address, d.o.b, NI number, pay, images etc* |
| Categories of Data Subject | *e.g. Staff (including volunteers, agents, and temporary workers), customers/clients, suppliers, students, members of the public, website users etc* |
| Plan for return and destruction of the data once processing complete | *e.g. how long will data be retained for, how will it be returned or destroyed* |