**DATED\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2021**

**(1) DERBYSHIRE COUNTY COUNCIL**

AND

(2) [TENDERER]

**CONFIDENTIALITY and DATA SHARING AGREEMENT**

**CCP085**

**SECURITY AT CHESTERFIELD LIBRARY**

**THIS AGREEMENT** is made\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2018

BETWEEN:

1. **DERBYSHIRE COUNTY COUNCIL**, whose principal place of business is at County Hall, Matlock, Derbyshire, DE4 3AG (the “**Council**”); and
2. **[NAME]** whose registered office is at [address] (the “**Recipient**”),

**WHEREAS:**

1. The Council wishes to provide certain confidential information to the Recipient which includes personal data (including sensitive personal data) of individuals engaged in the current delivery of services which are relevant to the procurement process for the CCP085 Security at Chesterfield Library (being “**Personal Data**”).
2. The Council and the Recipient each acknowledge that to enable the Recipient to consider whether to submit a tender and, if so, on what terms, it is necessary for the Recipient to receive Personal Data in relation to individuals engaged in the current delivery of services subject to the procurement process who may transfer to the successful tenderer under the Transfer of Undertakings (Protection of Employment) Regulations 2006 (as amended by the Collective Redundancies and Transfer of Undertakings (Protection of Employment) (Amendment) Regulations 2014) (the “**Purpose**”). The parties also acknowledge the need to fully protect such Personal Data with obligations of confidentiality, whilst recognising the importance of processing this Data within the procurement process.
3. This Agreement sets out the legal basis upon which such Personal Data may be disclosed by the Council to the Recipient for the Purpose.

**IT IS HEREBY AGREED:**

1. Use and Permitted Disclosures
   1. In return for the Council making the Personal Data available to the Recipient, the Recipient shall:
      1. keep the Personal Data secret and confidential and agrees to use the Personal Data only for the purposes of whether to submit a tender and, if so, on what terms within the procurement process and in accordance with the terms of this Agreement;
      2. not use or exploit the Personal Data in any way except for the Purpose;
      3. not directly or indirectly disclose or make available any Personal Data in whole or in part to any person, other than to its employees or professional advisers (the “**Staff**”) where it is deemed to be on a need to know basis for the Purpose, wherein the Recipient undertakes:
2. to notify such Staff of the Recipient’s obligations under this Agreement; and
3. to use its best endeavours to ensure that the Staff involved comply with such undertakings and obligations including entering into any further confidentiality agreements as the Recipient deems necessary;
   * 1. apply the same security measures and degree of care to the Personal Data as the Recipient applies to its own confidential information, which the Recipient warrants as providing adequate protection from unauthorised disclosure, copying or use; and
     2. establish and maintain adequate security measures (including any reasonable security measures proposed by the Council from time to time) to safeguard the Personal Data from unauthorised access or use.
   1. Nothing in this Agreement shall impose an obligation on the Council to continue discussions or negotiations in connection with the Purpose, or an obligation on the Council to disclose any information (whether Personal Data or otherwise) to the Recipient.
4. Data Protection
   1. For the purposes of this clause 2, the following definitions shall apply:

**Act:** the Data Protection Act 2018**;**

**Data Protection Impact Assessment**: an assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data.

**Controller**, **Processor**, **Data Subject**, **Personal Data**, **Personal Data Breach**, **Data Protection Officer** take the meaning given in the Act.

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

**Data Subject Request**: a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Act to access their Personal Data.

**GDPR**: the General Data Protection Regulation *(Regulation (EU) 2016/679).*

**Joint Controllers:** where two or more Controllers jointly determine the purposes and means of processing.

**LED**: Law Enforcement Directive *(Directive (EU) 2016/680)*.

**Protective Measures**: 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 the such measures adopted by it.

**Staff**: as defined in clause 1.1.3 above;

**Sub-processor**: any third Party appointed to process Personal Data on behalf of that Processor related to this Agreement.

* 1. The parties acknowledge that for the purposes of the Act, the Council is the Controller and the Recipient is the Processor. The only processing that the Processor is authorised to do is set out in this Agreement by the Controller and may not be determined by the Processor.
  2. The Processor shall notify the Controller immediately if it considers that any of the Controller's instructions infringe the Act.
  3. The Processor shall provide all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment prior to commencing any processing. Such assistance may, at the discretion of the Controller, include:
     1. a systematic description of the envisaged processing operations and the purpose of the processing;
     2. an assessment of the necessity and proportionality of the processing operations in relation to the Services;
     3. an assessment of the risks to the rights and freedoms of Data Subjects; and
     4. the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of the Personal Data.
  4. The Processor, in relation to any Personal Data processed in connection with its obligations under this Agreement, shall:
     1. process that Personal Data only in accordance with Annex A (below), unless the Processor is required to do otherwise by law. If it is so required, the Processor shall promptly notify the Controller before processing the Personal Data unless prohibited by law;
     2. ensure that it has in place Protective Measures, which are appropriate to protect against a Data Loss Event, which the Controller may reasonably reject (but failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures), having taken account of the:

1. nature of the data to be protected;
2. harm that might result from a Data Loss Event;
3. state of technological development; and
4. cost of implementing any measures;
   * 1. ensure that:
5. the Processor personnel do not process Personal Data except in accordance with this Agreement;
6. it takes all reasonable steps to ensure the reliability and integrity of any Staff who have access to the Personal Data and ensure that they:
7. are aware of and comply with the Processor’s duties under this clause;
8. are subject to appropriate confidentiality undertakings with the Processor or any Sub-processor;
9. are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third Party unless directed in writing to do so by the Controller or as otherwise permitted by this Agreement; and
10. have undergone adequate training in the use, care, protection and handling of Personal Data; and
    * 1. not transfer Personal Data outside of the EU unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:
11. the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with GDPR Article 46 or LED Article 37) as determined by the Controller;
12. the Data Subject has enforceable rights and effective legal remedies;
13. the Processor complies with its obligations under the Act 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 Controller in meeting its obligations); and
14. the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the processing of the Personal Data;
    * 1. at the written direction of the Controller, delete or return Personal Data (and any copies of it) to the Controller on termination of the Agreement unless the Processor is required by law to retain the Personal Data.
    1. Subject to clause 2.7, the Processor shall notify the Controller immediately if it:
       1. receives a Data Subject Request (or purported Data Subject Request);
       2. receives a request to rectify, block or erase any Personal Data;
       3. receives any other request, complaint or communication relating to either party's obligations under the Act;
       4. receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under this Agreement;
       5. 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; or
       6. becomes aware of a Data Loss Event.
    2. The Processor’s obligation to notify under clause 2.6 shall include the provision of further information to the Controller in phases, as details become available.
    3. Taking into account the nature of the processing, the Processor shall provide the Controller with full assistance in relation to either party's obligations under the Act and any complaint, communication or request made under clause 2.6 (and insofar as possible within the timescales reasonably required by the Controller) including by promptly providing:
       1. the Controller with full details and copies of the complaint, communication or request;
       2. such assistance as is reasonably requested by the Controller to enable the Controller to comply with a Data Subject Request within the relevant timescales set out in the Act;
       3. the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;
       4. assistance as requested by the Controller following any Data Loss Event; and/or
       5. 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.
    4. The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this clause. This requirement does not apply where the Processor employs fewer than 250 staff, unless:
       1. the Controller determines that the processing is not occasional;
       2. the Controller determines the processing includes special categories of data as referred to in Article 9(1) of the GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the GDPR; or
       3. the Controller determines that the processing is likely to result in a risk to the rights and freedoms of Data Subjects.
    5. The Processor shall allow for audits of its Data Processing activity by the Controller or the Controller’s designated auditor.
    6. Each party shall designate its own data protection officer if required by the Act.
    7. Before allowing any Sub-processor to process any Personal Data related to this Agreement, the Processor must:
       1. notify the Controller in writing of the intended Sub-processor and processing;
       2. obtain the written consent of the Controller;
       3. enter into a written agreement with the Sub-processor which give effect to the terms set out in this clause, such that they apply to the Sub-processor; and
       4. provide the Controller with such information regarding the Sub-processor as the Controller may reasonably require.
    8. The Processor shall remain fully liable for all acts or omissions of any of its Sub-processors.
    9. The Controller may, at any time on not less than 30 Working Days’ notice, revise this clause by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to this Agreement).
    10. 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 this Agreement to ensure that it complies with any guidance issued by the Information Commissioner’s Office.
    11. Where the parties include two or more Joint Controllers in accordance with GDPR Article 26, those parties shall enter into a Joint Controller Agreement as may be agreed between the parties.
15. Destruction of Confidential Information
    1. The Recipient will promptly and securely destroy all Personal Data together with any copies thereof on request by the Council.
    2. In the absence of such request, the Recipient will promptly and securely destroy all Personal Data together with any copies thereof as soon as:
       1. the tender submission deadline passes in the event that the Recipient has not submitted a tender;
       2. the Recipient is notified that its tender has not been successful or its involvement in the procurement process has otherwise ended;
       3. the Recipient is notified that it has not been awarded a contract by the Council; or
       4. the Council abandons or otherwise brings to an end the procurement process.
    3. In the circumstances in which a contract has been awarded to the Recipient by the Council, then the Recipient will continue to hold all Personal Data in accordance with the terms of this Agreement until it receives a request by the Council in accordance with clause 3.1, at which time the Recipient will promptly and securely destroy all Personal Data together with any copies thereof.
16. Termination and Suspension
    1. Without prejudice to the Council’s rights set out elsewhere in this Agreement, the Council may:
       1. suspend or terminate this Agreement in the case of a breach being notified to them in accordance with clause 2.6; or
       2. terminate this Agreement in the event of the procurement being aborted; or
       3. terminate this Agreement in the event that the Recipient notifies the Council that they will be withdrawing from the procurement process.
17. Liability
    1. Neither party excludes or limits liability to the other party for:
       1. fraud or fraudulent misrepresentation;
       2. death or personal injury caused by negligence;
       3. a breach of any obligations implied by section 12 of the Sale of Goods Act 1979 or section 2 of the Supply of Goods and Services Act 1982; or
       4. any matter for which it would be unlawful for the parties to exclude liability.
    2. Subject to clause 6.1, neither party shall in any circumstances be liable whether in contract, tort (including for negligence and breach of statutory duty howsoever arising), misrepresentation (whether innocent or negligent), restitution or otherwise, for:
       1. any loss (whether direct or indirect) of profits, business, business opportunities, revenue, turnover, reputation or goodwill;
       2. loss (whether direct or indirect) of anticipated savings or wasted expenditure (including management time); or
       3. any loss or liability (whether direct or indirect) under or in relation to any other contract.
    3. Clause 6.2 shall not prevent claims, for:
       1. direct financial loss that are not excluded under any of the categories set out in clause 6.2.1; or
       2. tangible property or physical damage.
    4. The Recipient shall indemnify and keep indemnified the Council against any liability, loss, damage, fines, costs, expenses (including legal expenses) which arise (directly or indirectly) from out of and/or in connection with the Recipient’s breach of this Agreement or the Act.
18. General
    1. The Contracts (Rights of Third Parties) Act 1999 shall not apply to this Agreement and no third party shall have the benefit of or the right to enforce any term of this Agreement.
    2. Any variation to this Agreement must be in writing and signed by the respective authorised signatories.
    3. This Agreement, and any issues or disputes arising out of or in connection with it (whether such disputes are contractual or non-contractual in nature, such as claims in tort, for breach of statute or regulation, or otherwise) shall be governed by and construed in accordance with English law and each of the parties submits to the exclusive jurisdiction of the Courts of England and Wales with regard to any such issues or disputes.

**IN WITNESS WHEREOF** the parties have signed this Agreement on the day and year first above written.

|  |  |
| --- | --- |
| Signed for and on behalf of  DERBYSHIRE COUNTY COUNCIL: | Signed for and on behalf of  [tenderer name] |
|  |  |
| Name: [name] | Name: [name] |
| Position: [designation] | Position: [designation] |
| Date: [date] | Date: [date] |

**Annex A - Schedule of Processing, Personal Data and Data Subjects**

**Processing, Personal Data and Data Subjects**

This Annex A shall be completed by the Controller, who may take account of the view of the Processors, however the final decision as to the content of this Schedule shall be with the Controller at its absolute discretion.

* + 1. The contact details of the Controller’s Data Protection Officer are: [Janet.Gardom@Derbyshire.gov.uk](mailto:Janet.Gardom@Derbyshire.gov.uk)
    2. The contact details of the Processor’s Data Protection Officer are: **[Insert** Contact details]
    3. The Processor shall comply with any further written instructions with respect to processing by the Controller.
    4. Any such further instructions shall be incorporated into this Schedule.

|  |  |
| --- | --- |
| **Description** | **Details** |
| Identity of the Controller and Processor | The Parties acknowledge that for the purposes of the Data Protection Legislation, the Customer is the Controller and the Contractor is the Processor in accordance with Clause 1.1. |
| Subject matter of the processing | The processing is needed in order to ensure the Processor can effectively provide an accurate price and service for the tender. |
| Duration of the processing | *From 29th June 2021 to 27th July 2021* |
| Nature and purposes of the processing | *The nature of the processing is employment information with the end purpose to provide accurate pricing as TUPE is applicable to this contract.* |
| Type of Personal Data being Processed | *Employee pay, age, location, pension details* |
| Categories of Data Subject | *Staff* |
| Plan for return and destruction of the data once the processing is complete  UNLESS requirement under union or member state law to preserve that type of data | *Data should be destroyed after 27th July 2021 once processing has been completed.* |