

**GENERAL DATA PROTECTION REGULATION SCHEDULE
("THE GDPR SCHEDULE")**

**IN RELATION TO THE SANGATE LIBRARY CONTRACT
("THE CONTRACT")**

Reviewed and agreed: Full Council Committee meeting 22nd April 2021- Agenda item 7

PARTIES

The Kent County Council Data Controller

Sandgate Parish Council Data Processor

The Parties agree that the Contract is varied to include the GDPR Schedule and its Annex 1.

STANDARD DEFINITIONS

Party: a Party to this Contract;

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;

Processor Personnel: means all directors, officers, employees, agents, consultants and contractors of the Processor and/or of any Sub-Contractor engaged in the performance of its obligations under this Contract.

GDPR CLAUSE DEFINITIONS:

Data Protection Legislation: (i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time (ii) the DPA 2018 to the extent that it relates to processing of personal data and privacy; (iii) all applicable Law about the processing of personal data and privacy;

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 GDPR;

Data Loss Event: 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;

Data Subject Access Request: a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data;

DPA 2018: Data Protection Act 2018;

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

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;

Sub-processor: any third Party appointed to process Personal Data on behalf of the Processor related to this Contract

1. DATA PROTECTION

- 1.1 This GDPR Schedule includes Annex 1 (Schedule of Processing, Personal Data and Data. Annex 1 must be completed for this Schedule to be valid.
- 1.2 In the event of a conflict between this Schedule and other Clauses of the Contract pertaining to data protection, the Clauses within this Schedule shall apply.
- 1.3 The Parties acknowledge that for the purposes of the Data Protection Legislation, the Controller and the Processor are as described at the start of this Schedule. The only processing that the Processor is authorised to do is listed in Annex 1 to this Schedule by the Controller and may not be determined by the Processor.
- 1.4 The Processor shall notify the Controller immediately if it considers that any of the Controller's instructions infringe the Data Protection Legislation.
- 1.5 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:
 - 1.5.1 a systematic description of the envisaged processing operations and the purpose of the processing;
 - 1.5.2 an assessment of the necessity and proportionality of the processing operations in relation to the Services;

- 1.5.3 an assessment of the risks to the rights and freedoms of Data Subjects;
and
 - 1.5.4 the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.
- 1.6 The Processor shall, in relation to any Personal Data processed in connection with its obligations under this Contract:
- 1.6.1 process that Personal Data only in accordance with Annex 1 to this Schedule, 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;
 - 1.6.2 ensure that it has in place Protective Measures, which have been reviewed and approved by the Controller as appropriate to protect against a Data Loss Event having taken account of the:
 - a. nature of the data to be protected;
 - b. harm that might result from a Data Loss Event;
 - c. state of technological development; and
 - d. cost of implementing any measures;
 - 1.6.3 ensure that:
 - a. the Processor Personnel do not process Personal Data except in accordance with this Contract (and in particular Annex 1 to this Schedule);
 - b. it takes all reasonable steps to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:
 - i. are aware of and comply with the Processors duties under this Clause;
 - ii. are subject to appropriate confidentiality undertakings with the Processor or any Sub-processor;
 - iii. 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 Contract; and
 - iv. have undergone adequate training.

- 1.6.4 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:
- a. 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;
 - b. the Data Subject has enforceable rights and effective legal remedies;
 - c. the Processor complies with its obligations under the Data Protection Legislation 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
 - d. the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the processing of the Personal Data;
- 1.6.5 at the written direction of the Controller, delete or return Personal Data (and any copies of it) to the Controller on termination of the Contract unless the Processor is required by Law to retain the Personal Data.
- 1.7 Subject to Clause 1.8, the Processor shall notify the Controller immediately if it:
- 1.7.1 receives a Data Subject Access Request (or purported Data Subject Access Request);
 - 1.7.2 receives a request to rectify, block or erase any Personal Data;
 - 1.7.3 receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;
 - 1.7.4 receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under this Contract;
 - 1.7.5 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
- 1.7.6 becomes aware of a Data Loss Event.
- 1.8 The Processor's obligation to notify under Clause 1.7 shall include the provision of further information to the Controller in phases, as details become available.

- 1.9 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 Data Protection Legislation and any complaint, communication or request made under Clause 1.7 (and insofar as possible within the timescales reasonably required by the Controller) including by promptly providing:
 - 1.9.1 the Controller with full details and copies of the complaint, communication or request;
 - 1.9.2 such assistance as is reasonably requested by the Controller to enable the Controller to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;
 - 1.9.3 the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;
 - 1.9.4 assistance as requested by the Controller following any Data Loss Event;
 - 1.9.5 assistance as requested by the Controller with respect to any request from the Information Commissioners Office or any consultation by the Controller with the Information Commissioner's Office.
- 1.10 The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this Clause 1.
- 1.11 The Processor shall allow for audits of its Data Processing activity by the Controller or the Controllers designated auditor.
- 1.12 The Processor shall designate a data protection officer if required by the Data Protection Legislation.
- 1.13 Before allowing any Sub-processor to process any Personal Data related to this Contract, the Processor must:
 - 1.13.1 notify the Controller in writing of the intended Sub-processor and processing;
 - 1.13.2 obtain the written consent of the Controller;
 - 1.13.3 enter into a written agreement with the Sub-processor which give effect to the terms set out in this GDPR Schedule such that they apply to the Sub-processor; and
 - 1.13.4 provide the Controller with such information regarding the Sub-processor as the Controller may reasonably require.
- 1.14 The Processor shall remain fully liable for all acts or omissions of any Sub-processor.

1.15 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 Contract to ensure that it complies with any Guidance issued by the Information Commissioner's Office.