

Appendix 12 GDPR Variation – Contract Notice

This Notice amends and varies the terms of the Agreement you and Cambridgeshire County Council ("the Council").

This Notice complies with the Notice provisions of your Agreement.

This Notice is issued by Cambridgeshire County Council to ensure that all Parties to its Agreements comply with the requirements of, the General Data Protection Regulation 2016/679 ("GDPR") in connection with their respective processing activities.

TAKE NOTICE as follows:

- A. From the Effective Date, the definitions and clauses set out in this Notice shall replace any provisions regarding the role of the Parties under the Data Protection Laws and govern any Processing undertaken in relation to the Agreement.
- B. In the event of conflict between the data protection compliance clauses in this Notice and any clauses in the Agreement relating to Data Protection, the terms of this Notice shall prevail.
- C. The "Effective Date" shall be 25th May 2018.
- D. From the Effective Date, the following definitions shall apply to the Agreement:

"Data Loss Event	any event that results, or may result, in unauthorised access to Personal Data held by the Contractor 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 Processor Personnel	means all directors, officers, employees, agents, consultants and contractors of any Data Processor engaged in the performance of its obligations under this Agreement;
Data Protection Impact Assessment	an assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data;
Data Protection Legislation	this includes: <ul style="list-style-type: none"> (a) (the Data Protection Act 1998 for as long as it remains in force), (b) the General Data Protection Regulation (<i>Regulation (EU) 2016/679</i>) (GDPR), (c) the Law Enforcement Directive (<i>Directive (EU) 2016/680</i>) (LED) and any applicable

- national implementing Laws as amended from time to time,
- (d) the Data Protection Act 2018 (subject to Royal Assent) to the extent that it relates to processing of personal data and privacy;
 - (e) Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (where applicable);
 - (f) the Regulation of Investigatory Powers Act 2000 (where applicable);
 - (g) the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (*SI 2000/2699*) (where applicable);
 - (h) Directive 2002/58/EC concerning the processing of Personal Data and the protection of privacy in the electronic communications sector (where applicable);
 - (i) [the Privacy and Electronic Communications (EC Directive) Regulations 2003 (*SI 2003/2426*) (where applicable); and
 - (j) all applicable laws and regulations relating to processing personal data and privacy, including the guidance and codes of practice issued by the Information Commissioner, where applicable;

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;

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 a Data Processor for the purposes of this Agreement;”

E. From the Effective Date, the following clauses shall apply to the Agreement:

- “E1.1 Subject always to the provisions of Clause E1.16 below the Provider shall on request and at the expense of the Council afford the Council or the Council’s representatives such access to those records as may be requested by the Council in connection with the Agreement.
- E1.2 The Provider shall grant the Council during the Term of this Agreement access (free of charge during normal business hours on reasonable notice) to all such documents (including computerised documents and data) for purposes of financial audit of Agreement and Services being delivered by the Provider pursuant to it in order for the Council to carry out examinations into the economy, efficiency and effectiveness with which the Provider has used its resources to deliver the Services. The Council shall provide such explanations as are reasonably required for these purposes.

Data Protection

- E1.3 The Parties shall observe all of their obligations under the Data Protection Legislation that arise in connection with the Service.
- E1.4 For the purposes of this Clause, the terms “Data Controller”, “Data Processor”, “Data Subject”, “Personal Data”, “Personal Data Breach”, “Data Protection Officer” “Process” and “Processing” shall have the meaning prescribed under the Data Protection Legislation. With respect to the Parties' rights and obligations under this Agreement, the Parties agree that in relation to the Personal Data contained within Service User records, the Parties shall act jointly as Data Controllers.
- E1.5 The Parties shall ensure that Personal Data is safeguarded at all times in accordance with the Law, which shall include without limitation obligations to:
- E1.5.1 (where relevant) have a “Caldicott Guardian”, as defined by the Local Authority Circular LAC 2002/2, in this case the Council’s nominated information governance lead, able to communicate with the other Parties, who shall take the lead for information governance and from whom the other Parties shall receive regular reports on information governance matters, including but not limited to details of all incidents of data loss and breach of confidence;
- E1.5.2 (where transferred electronically) only transfer essential data that is (i) necessary for direct Service User care; and (ii) encrypted to the higher of the international data encryption standards for healthcare (this includes, but is not limited to, data transferred over wireless or wired networks, held on laptops, CDs, memory sticks and tapes);
- E1.5.3 have policies which are rigorously applied that describe individual personal responsibilities for handling Personal Data;
- E1.5.4 have agreed protocols for sharing Personal Data with other public authorities and non-public organisations;
- E1.5.5 perform an annual information governance self-assessment.

E1.6 To the extent that any Party (including its staff) is acting as a "Data Processor" on behalf of any other Party, that Party shall, in particular, but without limitation:

E1.6.1 notify the Party acting as "Data Controller" immediately if it considers that any of the Data Controller's instructions infringe the Data Protection Legislation;

E1.6.2 shall provide all reasonable assistance to the Data Controller in the preparation of any Data Protection Impact Assessment prior to commencing any processing. Such assistance may, at the discretion of the Data 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.

E1.6.3 only process such Personal Data, as that term is defined in the Data Protection Legislation, as is necessary to perform its obligations under this Agreement, and only in accordance with any instruction given by the other Party under this Agreement. [If it is so required the Data Processor shall promptly notify the Data Controller before processing the Personal Data unless prohibited by Law];

E1.6.4 ensure that it has in place Protective Measures, which have been reviewed and approved by the Data Controller as appropriate to protect against a Data Loss Event having taken account of the:

- (e) nature of the data to be protected;
- (f) harm that might result from a Data Loss Event;
- (g) state of technological development; and
- (h) cost of implementing any measures;

E1.6.5 ensure that:

- (i) the Data Processor Personnel do not process Personal Data except in accordance with this Agreement;

- (j) it takes all reasonable steps to ensure the reliability and integrity of any Data Processor Personnel who have access to the Personal Data and ensure that they:
- (i) are aware of and comply with the Contractor's duties under this clause;
 - (ii) are subject to appropriate confidentiality undertakings with the Contractor 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 Data Controller or as otherwise permitted by this Agreement;
 - (iv) have undergone adequate training in the use, care, protection and handling of Personal Data; and
 - (v) are aware of and trained in the policies and procedures identified in Clauses 0 and 0 above.

E1.6.6 not transfer Personal Data outside of the EU unless the prior written consent of the Data Controller has been obtained and the following conditions are fulfilled:

- (k) the Data Controller or the Data 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 Data Controller;
- (l) the Data Subject has enforceable rights and effective legal remedies;
- (m) the Data 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 Data Controller in meeting its obligations); and
- (n) the Data Processor complies with any reasonable instructions notified to it in advance by the Data Controller with respect to the processing of the Personal Data;

E1.6.7 at the written direction of the Data Controller, delete or return Personal Data (and any copies of it) to the Data Controller on

termination of the Agreement unless the Data Processor is required by Law to retain the Personal Data.

E1.6.8 shall maintain complete and accurate records and information to demonstrate their compliance with this clause E1.

E1.6.9 allow for audits of its Data Processing activity by the Data Controller or the Data Controller's designated auditor.

E1.6.10 designate a data protection officer if required by the Data Protection Legislation.

E1.7 Before allowing any Sub-processor to process any Personal Data related to this Agreement, the Data Processor must:

E1.7.1 notify the Data Controller in writing of the intended Sub-processor and processing;

E1.7.2 obtain the written consent of the Data Controller;

E1.7.3 enter into a written agreement with the Sub-processor which give effect to the terms set out in this clause E1 such that they apply to the Sub-processor; and

E1.7.4 provide the Data Controller with such information regarding the Sub-processor as the Data Controller may reasonably require.

E1.8 The Data Processor shall remain fully liable for all acts or omissions of any Sub-processor. Subject to clause E1.6, either Party shall notify the other Party immediately if it:

E1.8.1 receives a Data Subject Access Request (or purported Data Subject Access Request);

E1.8.2 receives a request to rectify, block or erase any Personal Data;

E1.8.3 receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;

E1.8.4 receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under this Agreement;

E1.8.5 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

E1.8.6 becomes aware of a Data Loss Event.

E1.9 The Parties' obligations to notify under clause E1.8 shall include the provision of further information to the other Party in phases, as details become available.

E1.10 Taking into account the nature of the processing, each Party shall provide the other with full assistance in relation to either Party's

obligations under Data Protection Legislation and any complaint, communication or request made under clause E1.5 (and insofar as possible within the timescales reasonably required by the Parties) including by promptly providing:

E1.10.1 the other Party with full details and copies of the complaint, communication or request;

E1.10.2 such assistance as is reasonably requested by the other Party to enable the it to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;

E1.10.3 the other Party, at its request, with any Personal Data it holds in relation to a Data Subject;

E1.10.4 assistance as requested by the other Party following any Data Loss Event;

E1.10.5 assistance as requested by the other Party with respect to any request from the Information Commissioner's Office, or any consultation by the other Party with the Information Commissioner's Office.

- E.11 Either Party 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).
- E.12 The Parties agree to take account of any guidance issued by the Information Commissioner's Office. Either Party may on not less than 30 Working Days' notice to the other amend this agreement to ensure that it complies with any guidance issued by the Information Commissioner's Office.
- E.13 Each Party shall indemnify and keep indemnified the other Party against all Losses incurred by it in respect of any breach of this clause by the defaulting Party, except to the extent that such breach was attributable to any act, omission or direction of the non-defaulting Party.

Confidentiality

- E1.14 Except as required by Law and specifically pursuant to this clause E1, each Party agrees at all times during the continuance of this Agreement and after its termination to keep confidential any and all information, data and material of any nature which the Parties may receive or otherwise obtain which has been designated as confidential by the other Parties in writing or that ought to be considered as confidential (however it is conveyed or on whatever media it is stored) in connection with the operation of this Agreement or otherwise relating in any way to the business, operations and activities of the other Party, its employees, agents and/or any other person with whom it has dealings including any client of either Party. For the avoidance of doubt this Clause shall not

affect the rights of any workers under Section 43 A-L of the Employment Rights Act 1996.

E1.15 Subject always to clause E.16 below the Parties agree to provide or make available to each other sufficient information concerning their own operations and actions and concerning Service User information (including material affected by the Data Protection Legislation in force at the relevant time) to enable efficient operation of the Services.

E1.16 The Parties shall ensure that the provision of the Services complies with all relevant Data Protection Legislation regulations and guidance and that the rights of access by Service Users to their data are observed.”

This Notice is supplemental to the Agreement and shall form an addendum to it. Unless specified in this Notice nothing shall have the effect of varying any other term, condition or obligation of the Parties to the Agreement.

This Notice and any dispute or claim arising out of or in connection with it (including non-contractual disputes or claims) shall be governed by and construed in accordance with English law.

Except in so far as they conflict with the terms of this Notice, all relevant terms of the Agreement shall continue to apply.