Schedule 11

GENERAL DATA PROTECTION REGULATION (GDPR)

1. New data protection legislation is due to come into force during 2018, which aims to protect the privacy of all EU citizens and prevent data breaches. It will apply to any public or private organisation processing personal data. Established key principles of data privacy remain relevant in the new Data Protection Legislation but there are also a number of changes that will affect commercial arrangements, both new and existing, with suppliers.

2. The Data Protection Legislation comprises: i) the General Data Protection Regulation (GDPR) which comes into force on 25 May 2018; and ii) the Data Protection Act (DPA) 2018 which is anticipated to come into force (subject to Parliamentary approval) on 6 May 2018 for law enforcement processing, and 25 May for GDPR.

3. **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 Provider is bound to comply;

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

4. **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; (iiii) 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 Provider 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 Provider related to this Contract.

5. DATA PROTECTION

5.1. The Parties acknowledge that for the purposes of the Data Protection Legislation, the Council is the Controller and the Provider is the Processor. The only processing that the Provider is authorised to do is listed in Schedule 11 Annex 1 by the Council and may not be determined by the Provider.

5.2. The Provider shall notify the Council immediately if it considers that any of the Council's instructions infringe the Data Protection Legislation.

5.3. The Provider shall provide all reasonable assistance to the Council in the preparation of any Data Protection Impact Assessment prior to commencing any processing. Such assistance may, at the discretion of the Council, include:

5.3.1. a systematic description of the envisaged processing operations and the purpose of the processing;

5.3.2. an assessment of the necessity and proportionality of the processing operations in relation to the Services;

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

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

5.4. The Provider shall, in relation to any Personal Data processed in connection with its obligations under this Contract:

5.4.1. process that Personal Data only in accordance with Schedule 11 Annex 1, unless the Provider is required to do otherwise by Law. If it is so required the Provider shall promptly notify the Council before processing the Personal Data unless prohibited by Law;

5.4.2. ensure that it has in place Protective Measures, which have been reviewed and approved by the Council 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;

5.4.3. ensure that:

(a) the Provider Personnel do not process Personal Data except in accordance with this Contract (and in particular Schedule 11 Annex 1);

(b) it takes all reasonable steps to ensure the reliability and integrity of any Provider Personnel who have access to the Personal Data and ensure that they:

(i) are aware of and comply with the Providers duties under this Clause;

(ii) are subject to appropriate confidentiality undertakings with the Provider 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 Council or as otherwise permitted by this Contract; and

(iv) have undergone adequate training use, care, protection and handling of Personal Data; and

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

(a) the Council or the Provider has provided appropriate safeguards in relation to the transfer (whether in accordance with GDPR Article 46 or LED Article 37) as determined by the Council;

(b) the Data Subject has enforceable rights and effective legal remedies;

(c) the Provider 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 Council in meeting its obligations);

(d) the Provider complies with any reasonable instructions notified to it in advance by the Council with respect to the processing of the Personal Data;

5.4.5. at the written direction of the Council, delete or return Personal Data (and any copies of it) to the Council on termination of the Contract unless the Provider is required by Law to retain the Personal Data.

5.5. Subject to Clause 5.6, the Provider shall notify the Council immediately if it:

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

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

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

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

5.5.5. 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

5.5.6. becomes aware of a Data Loss Event.

5.6. The Providers obligation to notify under Clause 5.5 shall include the provision of further information to the Council in phases, as details become available.

5.7. Taking into account the nature of the processing, the Provider shall provide the Council with full assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under Clause 1.5 (and insofar as possible within the timescales reasonably required by the Council) including by promptly providing:

5.7.1. the Council with full details and copies of the complaint, communication or request;

5.7.2. such assistance as is reasonably requested by the Council to enable the Council to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;

5.7.3. the Council, at its request, with any Personal Data it holds in relation to a Data Subject;

5.7.4. assistance as requested by the Council following any Data Loss Event;

5.7.5. assistance as requested by the Council with respect to any request from the Information Commissioners Office or any consultation by the Council with the Information Commissioner's Office.

5.8. The Provider shall maintain complete and accurate records and information to demonstrate its compliance with this Clause. This requirement does not apply where the Provider employs fewer than 250 staff, unless:

5.8.1. the Council determines that the processing is not occasional;

5.8.2. the Council 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; and

5.8.3. the Council determines that the processing is likely to result in a risk to the rights and freedoms of Data Subjects.

5.9. The Provider shall allow for audits of its Data Processing activity by the Council or the Councils designated auditor.

5.10. The Provider shall designate a data protection officer if required by the Data Protection Legislation.

5.11. Before allowing any Sub-processor to process any Personal Data related to this Contract, the Provider must:

5.11.1. notify the Council in writing of the intended Sub-processor and processing;

5.11.2. obtain the written consent of the Council;

5.11.3. enter into a written agreement with the Sub-processor which give effect to the terms set out in this Schedule 11 such that they apply to the Sub-processor; and

5.11.4. provide the Council with such information regarding the Sub-processor as the Council may reasonably require.

5.12. The Provider shall remain fully liable for all acts or omissions of any Sub-processor.

5.13. The Provider 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 Contract).

5.14. The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Council may on not less than 30 Working Days' Notice to the Provider amend this agreement to ensure that it complies with any Guidance issued by the Information Commissioner's Office.

GENERAL DATA PROTECTION REGULATION (GDPR)
ANNEX 1
Schedule of Processing, Personal Data and Data Subjects

Provider: **[ENTER PROVIDER NAME]**
Contract: **SS14 142 Older Persons Residential and Nursing Care Home Contract**

1. The Processor shall comply with any further written instructions with respect to processing by the Controller.

2. Any such further instructions shall be incorporated into this Schedule.

3. Part A and/or Part B, as appropriate, describe the Data relationship(s) between the Parties. Only completed Part(s) apply and an uncompleted Part indicates that the Data relationship pertaining to that Part does not exist within the Contract. At least one Part must be completed and apply and both Parties may be completed and apply but the latter can only apply to different Data within the Contract.

PART A

The Kent County Council Data Controller
The Provider Data Processor

Description	Details
Subject matter of the Processing	Processing of personal or sensitive data in relation to the provision of Adult Social Care service provision All Providers delivering a service on behalf of Kent County Council are contractually obliged to manage personal or sensitive data to enable the delivery of the service commissioned. This may be through a framework contract, individual or spot contract or other arrangement whereby payment is made. Personal or sensitive data includes that of the person receiving the service, as commissioned or purchased on behalf of Kent County Council.
Duration of the Processing	The Terms and Conditions of the Contract state the duration of Processing throughout the duration of the contract and held for the agreed period of time after contract expires. The information is required to be held in accordance with the subject matters use, in line with the organisations' record retention policy or governing body / legislation whichever is the greatest. On early termination of contract, refer to the Contract particulars as detailed in the Terms and Conditions of the Contract.
Nature and purposes of the Processing	In the delivery of this Contract Kent County Council are the Data Controllers for information provided on service users referred to the service. The Provider is the Data Processer for the personal and sensitive information relating to this contract. . [Where the Provider collects data in excess of the requirements of this Contract, the Provider will be the Data Controller of that data. The Provider is the Data Controller of its employee information; where reviewed through Contract Monitoring, the Council will be the Processer of that data.] Due to the nature of the service provided, the high-risk area of information will be that which is collected manually. The information

	will either be transferred to a computerised system with paper records filed in locked cabinets. This could be for client records, staff files or other requirements. The expectation is that where records are filed in locked cabinets, the keys are kept in a locked storage box in a locked office and the office is locked each time it is not in use. Computerised records would need to be backed up with up to date security software. Email accounts are specific to the service and are not utilising Gmail, Yahoo or other generic or personal accounts and need to be enabled to use secure email to and from KCC and other necessary organisations. Information that is portable and used in the community, for instance service delivery that requires a visit to hospital, GP or for an outing must be kept to a minimum with key relevant information being transported. This information has to be kept secure in a folder in a closed bag, preferably with a lock. If information is left unattended in a car for a short period, this must be locked in the boot out of sight. Fire grab packs containing personal or sensitive information held within services must be secured in a break-glass (or similar) unit with key access for regular reviewing and updating. It must be accessible in the case of emergency. Further information and advice around the suitability of storage, transfer and handling of information can be found at https://ICO.org.uk The nature of the Processing under this Contract will cover the following: receiving, 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 (whether or not by automated means) etc. Information must be Processed and reported according to: Data Protection Act Information Governance – general responsibilities section of this Contract (Contract Terms and Conditions) and Schedule - General Data Protection Regulation (GDPR) The purpose of the Processing are as follows: • To measure, accept suitability of care packages, • To liaise with Kent County Council Case/Care Managers • To inform staff of service to be delivered and escalation routes. • To deliver services to Specification according to need. • To manage unforeseen situations, and emergencies • To invoice KCC according to the individual's details. • To analyse current and future service provision via KPI data • To ensure safe working practice via monitoring of training, DBS collection, registration and insurances. Information will be shared with the Commissioner, the Regulator, the NHS/CCG and Ambulance Trust where and when necessary in a timely and legitimate manner, obtaining consent where required. Due to the nature of the data collected GDPR compliance will also be appended to any contract management schedules for monitoring progress
Type of Personal Data	Personal and sensitive data required includes: Information on Service recipients: name, address, date of birth, NHS details, social care identification number, NI number, telephone

	number, medical conditions and assistance needs, key safe information as needed, next of kin information, risk assessment information.
Categories of Data Subject	Service users/Individuals/Residents/Clients – the person using the service Next of Kin to the person using the service. Witness and Investigation information in relation to complaint, safeguarding and criminal investigations (may include photographic evidence)
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	Retention of data as per 'Contract particulars' in the Terms and Conditions Or Retention as required by legislation or governing bodies such as CQC. whatever period is the greatest. Storage, Transfer and Destruction of data as per Data Protection Act Information Governance – general responsibilities section of the Contract Terms and Conditions On early termination of contract all data to be returned to Kent County Council as per section 'recovery upon termination' within the Contract Terms and Conditions.

PART B

The Kent County Council Data Processor
The Provider Data Controller

Description	**Details**
Subject matter of the Processing	Additional information received relating to the individual using the service and shared with the Council Employee information collated by the Provider to deliver the Service and shared with the Council through Contract Monitoring, Safeguarding or other legitimate requirement
Duration of the Processing	For the duration of the Service and Contract – refer to the Terms and Conditions of the Contract or Safeguarding and other Legislation
Nature and purposes of the Processing	The nature of the Processing means any operation such as 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 (whether or not by automated means) etc. The purpose to include employment processing, statutory obligation, recruitment assessment etc.
Type of Personal Data	Staff/Volunteers. professional registrations, insurances, proof of ID, NI details, Bank details, training details, DBS information Additional Personal or Sensitive information collated in relation to a Service recipient in order to deliver the Service
Categories of Data Subject	Service users/Individuals/Residents/Clients – the person using the service Next of Kin to the person using the service. Staff (including volunteers, agents, and temporary workers)

	Suppliers/third parties in the delivery of the service, including trainers Witness and Investigation information in relation to complaint, safeguarding and criminal investigations (may include photographic evidence)
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	Retention of data as per ‘Contract particulars’ in the Terms and Conditions Or Retention as required by legislation or governing bodies such as CQC. whatever period is the greatest. Storage, Transfer and Destruction of data as per data protection act information governance – general responsibilities section of the Contract Terms and Conditions On early termination of contract all data to be returned to Kent County Council as per section 'recovery upon termination' within the Contract Terms and Conditions.