**Schedule 5**

**Information Governance**

The definitions given in the Particulars apply.

1. **Protection of Personal Data**
   1. The only Processing that the Service Provider is authorised to do is listed by the Council in the Table below and may not be determined by the Service Provider.

* 1. The Service Provider shall, in relation to any Personal Data Processed in connection with its obligations under this Contract Process that Personal Data only in accordance with this Schedule, unless the Service Provider is required to do otherwise by an Enactment, in which case, it will notify the Council before carrying out such Processing.
  2. The Service Provider shall notify the Council immediately if it considers that any of the Council’s instructions infringe Data Protection Legislation.
  3. The Service 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:

1. a systematic description of the envisaged Processing operations and the
2. purpose of the Processing;
3. an assessment of the necessity and proportionality of the Processing
4. operations in relation to the Services;
5. an assessment of the risks to the rights and freedoms of Data Subjects; and
6. the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

1.5 Without prejudice to any other provisions of the Contract, the Service Provider shall not authorise any third party or Sub-contractor to Process the Personal Data without the prior written consent of the Council and should such consent be given, it shall not relieve the Service Provider from any liability or obligation under the Contract and the Service Provider shall be responsible for the acts, omissions, defaults or neglect of any Sub-Contractor and its agents or employees in all respects as if they were the acts, omissions, defaults or neglect of the Service Provider. The Service Provider shall ensure that in relation to Personal data, such Sub-contractor or third-party processor is under contractual obligations which are no less protective than the data protection requirements set out in the Contract. The Service Provider shall provide the Council with such information regarding the Sub-contractor as the Council may reasonably require.

* 1. The Service Provider shall in Processing pursuant to this Contract, ensure that it takes all appropriate technical and organisational security measures to protect against a Data Loss Event having taken into account 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 security measures.

and the Service Provider shall provide to the Council such information as the Council may reasonably require to satisfy itself that the Service Provider is complying with the obligations referred to in this Clause 1.6. The Council shall be entitled to reject on reasonable grounds any technical, organisational and security measures employed by the Service Provider, provided that failure to reject such measures shall not amount to approval by the Council of such measures.

* 1. The Service Provider must exercise its best endeavours to ensure the accuracy of any Personal Data Processed in carrying out its obligations under the Contract and that where necessary such Personal Data is kept up to date.
  2. The Service Provider shall not Process or otherwise transfer any Personal Data in or to any country outside the European Economic Area unless the prior written consent of the Council has been obtained and:

1. the Service Provider has provided appropriate safeguards in relation to the transfer in accordance with Chapter V of the GDPR;
2. the Data subject has enforceable rights and effective legal remedies;
3. the Service Provider complies with the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred; and
4. the Service Provider complies with any reasonable instructions notified to it in advance by the Council with respect to the Personal Data.

It shall be the responsibility of the Service Provider to produce satisfactory evidence of compliance with this clause 1.8 during the Contract Period.

1.9 The Service Provider shall take reasonable steps to ensure the reliability and integrity of any Staff who have access to the Personal Data and ensure that:

1. all Staff required to access the Personal Data are informed of the confidential nature of the Personal Data and comply with all the Service Provider’s obligations with respect to Personal Data, including the confidentiality undertakings under the terms of this Contract;
2. staff do not Process Personal Data except in accordance with this Contract;
3. staff are subject to appropriate confidentiality undertakings with the Service Provider or any subcontractor used by the Service Provider in delivering the Service;
4. none of their Staff publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Council or unless otherwise permitted under this Contract; and
5. staff have undergone adequate training in the use, care, protection and handling of Personal Data.

1.10 The Service Provider shall ensure that Data Subjects are provided at first point of contact with a Privacy Notice.

1.11 The Service Provider shall notify the Council immediately if it becomes aware of a Data Loss Event or if it receives:

1. a Data Subject Request concerning any aspect of the processing or handling of that person's Personal Data;
2. a request to rectify, block or erase any Personal Data;
3. a complaint, request or communication relating to the Council's obligations under the Data Protection Legislation;
4. any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data Processed under this Agreement; or
5. a request from any third party for disclosure of Personal Data where compliance with such request is required or is purported to be required by any Enactment.

1.12 The Service Provider’s duty to notify the Council under clause 1.11 shall include the provision of further information to the Council in phases, as details become available.

1.13 The Service Provider shall provide the Council with full cooperation and assistance in relation to any complaint or request made in relation to either party’s obligations under Data Protection Legislation including by providing:

1. the Council with full details of the complaint, communication or request;
2. such assistance and information as is reasonably requested by the Council to enable the Council to comply with a Data Subject Request within the timescales required by the Council;
3. the Council with any Personal Data it holds in relation to a Data Subject (within the timescales required by the Council);
4. assistance as requested by the Council following any Data Loss Event.
5. such assistance as requested by the Council with respect to any request from the Information Commissioner’s Office, or any consultation by the Council with the Information Commissioner’s Office.

1.14 The Service Provider shall maintain complete and accurate records and information to demonstrate its compliance with this Schedule.

1.15 The Service Provider shall permit the Council or the Council’s representative (subject to reasonable and appropriate confidentiality undertakings), to inspect and audit the Service Provider's data processing activities (and/or those of its agents, subsidiaries and sub-contractors) and comply with all reasonable requests or directions by the Council to enable the Council to verify and/or procure that the Service Provider is in full compliance with its obligations under this Contract.

1.16 The Service Provider shall comply with any further written instructions given by the Council with respect to processing and any such further instructions shall be incorporated into this Schedule.

1. **Data Processing Table**

|  |  |
| --- | --- |
| **Description** | **Details** |
| Type of Personal Data | First name, surname, address including postcode, date of birth, age, gender, sexual orientation, ethnicity, exemption status from prescription charges, pregnancy status, occupation, telephone number(s), notes detailing Service delivery data including pharmacotherapy (where applicable) and any other data for the purposes of reporting the data needed for the Stop Smoking Services Quarterly Return used for the delivery of Local Stop Smoking Services[[1]](#footnote-1). |
| Duration of the processing | The Service Provider will collect, record and update on Service Users data from the Service Commencement Date and shall continue for the Contract Period. |
| Categories of Data  Subject | Service Users, Patients, Clients, Residents |
| Nature of the processing | The Service Provider will collect and input data on a suitable web-based Information and Communication Technologies (ICT) system for the purposes of the following operations: collection, recording, organisation, storage, adaptation or alteration, retrieval, use, dissemination or otherwise making available, restriction. |
| Plan for return and  destruction of the data  once the processing is  complete | Stored by Service Provider in accordance with retention periods set out below unless termination or expiry of Contract occurs earlier.  Provisions governing return/destruction of data on expiry or termination of Contract are in the Special Condition 17 and Condition 30.2 of the Contract.  Prior to the expiry or termination of the Contract: (i) Personal Data will be retained for seven years from the last time a patient accesses clinical services; and (ii) for other data which are non-clinical retention should be in accordance with the Contract and retained for six years.  The Service Provider shall securely destroy and permanently delete all data it is holding at the end of the relevant retention period. |

1. **Policies and Procedures**
   1. The Service Provider must have in place at the Commencement Date and throughout the Contract Period:
      1. internal records of its data processing activities;
      2. policies and procedures for data protection compliance;
      3. specific Staff training relating to data protection; and
      4. a documented system for the handling of security incidents and close calls (‘near misses’)
   2. The Service Provider will co-operate with the monitoring of such obligations on an annual basis and will notify the Council immediately of any data protection issues and security incidents within its organisation.
   3. When delivering the Services, the Service Provider will uphold the highest standards in safeguarding Personal Data, and specifically will:
2. ensure that information governance/data security is a key component of both the induction and on-going training programmes;
3. not allow Staff to use their own personal equipment to store Council Data;
4. provide Staff with appropriate means and guidelines for keeping any personal information they are required to store outside of the office securely;
5. ensure that equipment holding Personal Data is kept secure;
6. have procedures in place to ensure immediate reporting to the Council of any security related incidents and to ensure that full and prompt cooperation can be given to the Council in the investigation of such incidents.

3.4. Appoint a qualified Data Protection Officer (if required by the GDPR), or where not required by the GDPR, allocate responsibility for data protection to a named senior member of Staff who has responsibility for information governance in their organisation. This person will:

1. develop information governance within the Service Provider’s organisation;
2. complete and submit an annual position statement to the Council by end of April each year, to include an information governance improvement plan for the coming 12 months; and
3. draft and implement policies, procedures and guidance to ensure that the above information governance best practice is adopted.

1. <https://digital.nhs.uk/data-and-information/data-collections-and-data-sets/data-collections/stop-smoking-services-collection> [↑](#footnote-ref-1)