Data Processing Agreement

BETWEEN

(Please enter Dental practice name and address below)

(Hereinafter known as the Data Controller)

AND

Ashford Orthodontics, Units 14a-14b Southwick Industrial Estate, Riverside Rd, Sunderland SR5 3JG, UK

(Hereinafter known as the Data Processor)

In Support of Digital Orthodontics Support

Revision	
Date	

Contents

THIS AGREEMENT is made on (Date): _____

BETWEEN:

(1) Please enter Dental Practice Name _____ **('Data Controller')**; and

(2) Ashford Orthodontics with its registered office at Southwick Industrial Estate, 14b Riverside Road, Sunderland, SR5 3JG, UK **('Data Processor').**

BACKGROUND

(A) The Data Controller has appointed the Data Processor to perform

(B) In performing the Services, the Data Processor is required to process certain Personal Data (see Annex) for processing only in accordance with the terms of this Agreement from the date on which this Agreement is entered into **(the Commencement Date).**

(C) Access to Personal Data will be supplied on a restricted 'need to know' basis for the purposes specified in the Annex.

IT IS AGREED as follows:

1. Definitions and Interpretation

1.1 The following definitions shall apply in this Agreement:

Controller shall take the meaning given in the Data Protection Legislation;

Data Guidance means any applicable guidance, guidelines, direction or determination, framework, code of practice, standard or requirement regarding information governance, confidentiality, privacy or compliance with the Data Protection Legislation (whether specifically mentioned in this Agreement or not) to the extent published and publicly available or their existence or contents have been notified to the Data Processor by any relevant Regulatory or Supervisory Body. This includes but is not limited to guidance issued by European Data Protection Board and the Information Commissioner;

Data Breach Event means any event that results, or may result, in unauthorised processing of Personal Data held by the Data Processor under this Agreement or Personal Data that the Data Processor has responsibility for under this Agreement including without limitation actual or potential Breach, destruction, corruption or inaccessibility of Personal Data.

Data Processor Personnel means any and all persons employed or engaged from time to time in the provision of the Services and/or the processing of Personal Data whether employees, workers, consultants or agents of the Data Processor or any subcontractor or agent of the Data Processor.

Data Processing Services means the data processing services described in the Annex to this Agreement; **Data Protection Impact Assessment** means an assessment by the Data Controller of the impact of the envisaged processing on the protection of Personal Data;

Data Protection Legislation means (i) the GDPR, the LED and any applicable national Laws implementing them as amended from time to time (ii) the DPA 2018 (iii) all applicable Law

concerning privacy, confidentiality or the processing of personal data including but not limited to the Human Rights Act 1998, the Health and Social Care (Safety and Quality) Act 2015, the common law duty of confidentiality and the Privacy and Electronic Communications (EC Directive) Regulations;

Data Protection Officer shall take the meaning given in the Data Protection Legislation;

Data Subject shall take the meaning given in the Data Protection Legislation;

Data Subject Access Request means 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 means Data Protection Act 2018;

EU means the European Union;

European Data Protection Board has the meaning given to it in the Data Protection Legislation;

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

Information Commissioner means the independent authority established to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals ico.org.uk and any other relevant data protection or supervisory authority recognised pursuant to the Data Protection Legislation;

Law means any law or 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 Data Processor is bound to comply;

LED means the Law Enforcement Directive (Directive (EU) 2016/680);

Personal Data shall take the meaning given in the Data Protection Legislation;

Personal Data Breach shall take the meaning given in the Data Protection Legislation;

Processor shall take the meaning given in the Data Protection Legislation;

Processing and cognate terms shall have the meaning given in the Data Protection Legislation;

Protective Measures means 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;

Regulatory or Supervisory Body means any statutory or other body having authority to issue guidance, standards or recommendations with which the Data Processor and/or Data Processor Personnel must comply or to which it or they must have regard, including:

(i) CQC
(ii) NHS Improvement
(iii) NHS England
(iv) The Department of Health
(v) The National Institute for Health and Care Excellence
(vi) Healthwatch England and Local Healthwatch
(vii) Public Health England
(viii) The General Pharmaceutical Council
(ix) The Healthcare Safety Investigation Branch
(x) Information Commissioner
(xi) European Data Protection Board.

Sub-processor means any third party appointed to process Personal Data on behalf of the Data Processor related to this Agreement;

Working Day means a day other than a Saturday, Sunday or bank holiday in England

1.1.1 Reference to any legislative provision shall be deemed to include any statutory instrument, bye law, regulation, rule, subordinate or delegated legislation or order and any rules and regulations which are made under it, and any subsequent re- enactment, amendment or replacement of the same;

1.1.2 the Annex forms part of this Agreement and shall have effect as if set out in full in the body of this Agreement. Any reference to this Agreement includes the Annex; and

1.1.3 references to clauses and Annexes are to clauses and Annexes to this Agreement.

2. Scope of this Agreement

The terms and conditions of this Agreement shall apply to all Personal Data provided by the Data Controller or obtained by the Data Processor from other sources as part of the provision of the services under the Supply Agreement or derived from any combination thereof.

3. Data Processors Obligations

General

3.1 The Data Processor shall process all Personal Data only in accordance with the instructions set out in the Annex, unless the Data Processor is required to do otherwise by Law. If it is so required, the Data Processor shall promptly notify the Data Controller before processing the Personal Data unless prohibited by Law.

3.2 The Data Processor shall designate a Data Protection Officer and shall communicate to the Data Controller the name and contact details of the Data Protection Officer.

3.3 The Data Processor shall not do or omit to do anything that will put the Data Controller in breach of this Agreement and the Data Protection Legislation.

3.4 The Data Processor shall notify the Data Controller immediately if it considers that any of the Data Controllers' instructions infringe the Data Protection Legislation.

3.5 The Data Processor must assist the Data Controller in ensuring compliance with the obligations set out at Article 32 to 36 of the GDPR and equivalent provisions implemented into Law, taking into account the nature of processing and the information available to the Data Processor.

3.6 The Data Processor must take prompt and proper remedial action regarding any Data Breach Event.

Registration/Certifications

3.7 The Data Processor shall maintain its registration with the Information Commissioner's Office for the duration of this Agreement.

3.8 The Data Processor shall maintain the Cyber Essential (Plus) accreditation or equivalent standard, as approved by the Data Controller, for the duration of this Agreement. Any such approval shall not be unreasonably withheld.

3.9 The Data Processor shall confirm achievement of all relevant HSCIC IG Toolkit standards at satisfactory level (level 2) and provide evidence within 7 days of the request being made by the Data Controller.

3.10 The Data Processor shall confirm that it is working towards full compliance of the new NHS Digital Data Security and Protection (DSP) Toolkit assertions and provide evidence to this effect within 7 days of the request being made by the Data Controller.

DPIAs

3.11 The Data Processor shall provide all reasonable assistance to the Data Controller in the preparation of any Data Protection Impact Assessment (DPIA's) prior to commencing any processing. Such assistance may, at the discretion of the Data Controller, include:

3.11.1 a systematic description of the envisaged processing operations and the purpose of the processing;

3.11.2 an assessment of the necessity and proportionality of the processing operations in relation to the Data Processing Services;

3.11.3 an assessment of the risks to the rights and freedoms of natural persons; and

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

3.12 The Data Processor shall provide all reasonable assistance to the Data Controller if the outcome of the Data Protection Impact Assessment leads the Data Controller to consult the Information Commissioner.

Data Processor Personnel

3.13 The Data Processor shall ensure that its employees, agents or sub-contractors

3.13.1 do not process the Personal Data except in accordance with this Agreement;

3.13.2 are subject to appropriate confidentiality undertakings with the Data Processor or any Sub-processor that are in writing and legally enforceable;

3.13.3 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 advance and in writing to do so by the Data Controller or as otherwise permitted by this Agreement.

3.13.4 have undergone adequate training in the use, care, protection and handling of Personal Data that enables them and the Data Processor to comply with their responsibilities under the Data Protection Legislation and this Agreement. The Data Processor shall provide the Data Controller with evidence of completion and maintenance of that training within three Working Days of request by the Data Controller.

Transfers outside the EEA/EU

3.14 The Data Processor shall not transfer Personal Data outside of the EEA/EU unless the prior written consent of the Data Controller has been obtained and the following conditions are fulfilled:

3.14.1 the Data Controller or the Data Processor have provided appropriate safeguards in relation to the transfer as determined by the Data Controller;

3.14.2 the Data Subject has enforceable rights and effective legal remedies;

3.14.3 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

3.14.4 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.

Data security (Protective Measures)

3.15 The Data Processor shall ensure that it has in place Protective Measures as appropriate to protect against a Data Breach Event taking account of the nature of the data to be protected, the harm that might result from a Data Breach Event, state of technological development and cost of implementing any measures, including, but not limited to the minimum data security requirements as set out in the Annex.

3.16 The Data Processor shall at the written direction of the Data Controller, delete or return all Personal Data (and any copies of it) to the Data Controller on termination of the Contract unless the Data Processor is required by Law to retain the Personal Data.

3.17 If the Data Processor is asked to delete Personal Data held in paper format, a cross cut shredder shall be used. Alternatively, a sub-processor might be appointed subject to clause 3.18 and provided that any process is compliant with EU standard EN15713. The Processor shall ensure that electronic storage media used to hold or process Personal Data is destroyed or overwritten to current CESG standards as defined at www.cesg.gov.uk. The Data Processor shall provide the Data Controller with evidence that all Personal Data has been securely deleted in accordance with the Data Protection Legislation within 10 Working Days.

Sub-processing

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

3.18.1 notify the Data Controller in writing of the intended Sub-processor and processing;

3.18.2 obtain the written consent of the Data Controller;

3.18.3 enter into a written agreement with the Sub-processor which gives effect to the terms set out in this Agreement such that they apply to the Sub-processor and in respect of which the Data Controller is given the benefits of third party rights to enforce the same; and

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

3.19 The Data Processor shall ensure that the third party's access to the Personal Data terminates automatically on termination of this Agreement for any reason save that the Sub-processor may access the Personal Data in order to securely destroy it.

3.20 The Data Processor shall remain fully liable for all acts or omissions of any Sub-processor.

Data Subject Rights

3.21 The Data Processor shall notify Data Controller immediately if it:

3.21.1 receives a Data Subject Access Request (or purported Data Subject Access Request) connected with Personal Data processed under this Agreement;

3.21.2 receives a request to rectify, block or erase any Personal Data connected with Personal Data processed under this Agreement;

3.21.3 receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation connected with Personal Data processed under this Agreement;

3.21.4 receives any communication from the Information Commissioner or any other Supervisory or Regulatory Body connected with Personal Data processed under this Agreement;

3.21.5 receives a request from any third party for disclosure of Personal Data connected with this Agreement; or

3.21.6 becomes aware an actual or suspected Data Breach Event.

3.22 This notification shall be given by sending the original request and any subsequent

communications to the Data Controller Data Protection Officer's e-mail address stated in the Annex.

3.23 The Data Processor shall not respond substantively to the communications listed at clause 10 save that it may respond to a Regulatory or Supervisory Body following prior consultation with the Data Controller

3.24 The Data Processor must assist the Data Controller by taking appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Data Controller obligation to respond to requests for exercising rights granted to individuals by the Data Protection Legislation.

Data Breach

3.25 The Processor will immediately and without undue delay notify the Controller, using the email address contained in the Annex, if it becomes aware of any Data Breach Event and the Controller with the following information:

3.25.1 description of the nature of the Data Breach Event

3.25.2 categories and approximate number of both Data Subjects and Personal Data records concerned

3.25.3 the likely consequences

3.25.4 a description of the measures taken, or proposed to be taken to address the Data Breach Event, including measures to mitigate its possible adverse effects.

3.26 Immediately following any Data Breach Event, the parties will co-ordinate with each other to investigate the matter. The Processor will reasonably co-operate with the Controller in the Controller's handling of the matter, including:

3.26.1 assisting with any investigation

3.26.2 providing the Controller with physical access to any facilities and operations affected

3.26.3 facilitating interviews with the Processor's employees, former employees and others involved in the matter

3.26.4 making available all relevant records, logs, files, data reporting and other materials required to comply with all Data Protection Legislation or as otherwise reasonably required by the Controller; and

3.26.5 taking reasonable and prompt steps to mitigate the effects and to minimise any damage resulting from the Data Breach Event or unlawful Personal Data processing.

3.27 The Data Processor will not inform any third party of any Data Breach Event without first obtaining the Data Controller's prior written consent, except when required to do so by law.

3.28 The Data Processor agrees that the Data Controller has the sole right to determine:

3.28.1 whether to provide notice of the Data Breach Event to any Data Subjects, supervisory authorities, regulators, law enforcement agencies or others, as required by law or regulation or in the Controller's discretion, including the

contents and delivery method of the notice; and

3.28.2 whether to offer any type of remedy to affected Data Subjects, including the nature and extent of such remedy.

3.29 The Data Processor will cover all reasonable expenses associated with the performance of the obligations under 3.25 and 3.26 unless the matter arose from the Data Controller's specific instructions, negligence, wilful default or breach of this Agreement, in which case the Data Controller will cover all reasonable expenses.

3.30 The Data Processor will also reimburse the Data Controller for actual reasonable expenses which the Data Controller incurs when responding to a Data Breach Event to the extent that the Data Processor negligently caused such a Data Breach, including all costs of notice and any remedy as set out in this Agreement.

3.31 The Data Processor's obligation to notify under clause 3.25 shall include the prompt provision of further information to the Data Controller in phases, as details become available.

4. Complaints

4.1 Taking into account the nature of the processing, the Data Processor shall provide the Data Controller with full assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under clause 3.21 (and insofar as possible within the timescales reasonably required by the Data Controller) including by promptly providing:

4.1.1 the Data Controller with full details and copies of the complaint, communication or request;

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

4.1.3 such assistance as is reasonably requested by the Data Controller to enable the Data Controller to comply with other rights granted to individuals by the Data Protection Legislation including the right of rectification, the right to erasure, the right to object to processing, the right to restrict processing, the right to data portability and the right not to be subject to an automated individual decision (including profiling);

4.1.4 the Data Controller, at its request, with any Personal Data it holds in relation to a Data Subject;

4.1.5 assistance as requested by the Data Controller following any Data Breach Event;

4.1.6 assistance as requested by the Data Controller in relation to informing a Data Subject about any Data Breach Event, including communication with the Data Subject;

4.1.7 assistance as requested by the Data Controller with respect to any request from the Information Commissioner's Office, or any consultation by the Data Controller with the Information Commissioner's Office;

4.1.8 the Data Controller to exercise their rights under the Data Protection Legislation. Such requests must be sent to the Data Controller Data Protection Officer's e-mail

address stated in the Annex.

4.1.9 Immediately, and in no longer than one Working Day of receipt by the Data Processor.

5. Audits/Record Keeping

5.1 The Data Processor shall provide the Data Controller with evidence to demonstrate compliance with all of its obligations under this Agreement, including but not limited to the minimum data security requirements as set out in the Annex.

5.2 The Data Processor shall allow for audits of its delivery of the Data Processing Services by the Data Controller or the Data Controller designated auditor.

5.3 The Data Processor shall maintain complete and accurate records and information to demonstrate its compliance with this Agreement. The Data Processor must create and maintain a record of all categories of data processing activities carried out under this Agreement, containing:

5.3.1 the categories of processing carried out under this Agreement;

5.3.2 where applicable, transfers of Personal Data to a third country or an international organisation, including the identification of that third country or international organisation and, where relevant, the documentation of suitable safeguards;

5.3.3 a general description of the Protective Measures taken to ensure the security and integrity of the Personal Data processed under this Agreement; and

5.3.4 a log recording the processing of Personal Data in connection with this Agreement comprising, as minimum, details of the Personal Data concerned, how the Personal Data was processed, where the Personal Data was processed and the identity of any individual carrying out the processing.

5.4 The Data Processor shall ensure that the record of processing maintained in accordance with Clause 3.35 is provided to the Data Controller within two Working Days of a written request from the Data Controller.

5.5 This Agreement does not relieve the Data Processor from any obligations conferred upon it by the Data Protection Legislation.

5.6 The Parties agree to take account of any guidance issued by the Information Commissioner. The Data Controller may on not less than 30 Working Days' notice to the Data Processor amend this Data Processing Agreement to ensure that it complies with any guidance issued by the Information Commissioner.

6. Warranties

The Data Processor warrants and undertakes that it will deliver the Data Processing Services in accordance with the Data Protection Legislation, any mandatory Data Guidance and this Agreement and that it has in place Protective Measures which are sufficient to ensure that the delivery of the Data Processing Services complies with the Data Protection Legislation.

7. Remedies and No Waiver

7.1 The Data Processor shall indemnify, defend and hold harmless the Data Controller from and against all and any claims, liabilities, costs, charges, expenses, awards and damages of any kind including any fines, legal and other professional fees and expenses which it/they may suffer or incur as a result of, or arising out of or in connection with, any breach by the Data Processor of any of its obligations in this Agreement.

7.2 For the avoidance of any doubt, any limitation of liability which applies under the Supply Agreement shall not apply to the Data Processor's liability under the indemnity in this clause 5 which shall be limited to £10,000,000.

7.3 The rights and remedies provided under this Agreement are in addition to, and not exclusive of, any rights or remedies provided by Law or in equity.

7.4 A waiver of any right or remedy under this Agreement or by Law or in equity is only effective if given in writing and signed on behalf of the party giving it and any such waiver so given shall not be deemed a waiver of any similar or subsequent breach or default.

7.5 A failure or delay by a party in exercising any right or remedy provided under this Agreement or by Law or in equity shall not constitute a waiver of that or any other right or remedy, nor shall it prevent or restrict any further exercise of that or any other right or remedy. No single or partial exercise of any right or remedy provided under this Agreement or by Law or in equity shall prevent or restrict the further exercise of that or any other right or remedy.

8. General

8.1 This Agreement represents the entire understanding of the parties relating to necessary legal protections arising out of their Data Controller/Processor relationship under Data Protection Legislation.

8.2 If there is an inconsistency between any of the provisions of this Agreement and the provisions of the Supply Agreement, the provisions of this Agreement shall prevail.

8.3 The Data Processor shall not assign, transfer, mortgage, charge, subcontract, declare a Data Controller over or deal in any other manner with any or all of its rights and obligations under this Agreement without the prior written consent of the Data Controller.

8.4 No variation of this Agreement shall be effective unless it is in writing and signed by the parties to this Agreement.

8.5 This Agreement may be executed in any number of counterparts, each of which when executed and delivered shall constitute a duplicate original, but all the counterparts shall together constitute the one agreement. No counterpart shall be effective until each party has executed at least one counterpart.

9. Governing Law and Jurisdiction

9.1 This Agreement and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) shall be governed by and construed in accordance with the Law of England and Wales.

9.2 Each party irrevocably agrees that the courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim arising out of or in connection with this Agreement or its subject matter or formation (including non-contractual disputes or claims), provided that nothing in this clause shall prevent a party from enforcing any judgement obtained in the court of England and Wales in any other court with jurisdiction over the other party.

THIS AGREEMENT has been entered into on the date stated at the beginning of it.

10. Signatures

DATA CONTROLLER

On behalf of

Name (Print) _____

Job Title _____

DATA PROCESSOR

On behalf of Ashford Orthodontics

Name (Print) _____

Job Title _____

9.2 Each party irrevocably agrees that the courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim arising out of or in connection with this Agreement or its subject matter or formation (including non-contractual disputes or claims), provided that nothing in

11. Annex – Data Processing Services

1. The Data Processor shall comply with any further written instructions with respect to processing by the Data Controller.
2. Any such further instructions shall be incorporated into this Annex.

Description	**Details**
Subject matter of the processing	The purpose of the processing is to assist the Dental Practice in manufacturing dental appliances and store digital images. E.g. Orthodontics retainers.
Duration of the processing	Throughout the engagement of service via Ashford Orthodontics Terms and Conditions.
Legal basis for processing	Processing for the management of health or social care systems and services: Art 6 1 (a) Art 6 1 (e) and 9(2)(h) GDPR in conjunction with Schedule 1 DPA 2018.
Permitted Purpose	For Production of Orthodontic Devices
Type of Personal Data (dataset)	Special Category information - Ethnicity - Sexual Orientation - Health information - Biometric Information
Minimum data security requirements	All data will be transferred and stored using encryption.
Data Controller's contact details (Data Protection Officer)	
Receiving Party's contact details (Data Protection Officer)	