IAS Laboratory Client Data Security Statement

All data captured by IAS Laboratory is processed to enable us to provide you with our Orthodontic Dental Laboratory services.

Data Security Measures

IAS has invested in both the physical and virtual security of our servers. All data servers are held either securely in an onsite secure environment or offsite in enterprise-grade highly secure data centres.

Technical controls that are in place include, but are not limited, to the following:

- The access to servers are restricted to IAS Laboratory network using dedicated hardware firewalls

- The access lists on firewalls are based on specific open ports for applications only. All other ports are blocked

- Servers and PCs are protected and regularly scanned with best available updated antivirus / spyware/ malware which are updated in line with our patching policies and processes

16 Jan 2018

Data Protection Statement

IAS Laboratory is committed to data protection and data privacy. With the General Data Protection Regulation (GDPR) becoming enforceable on the 25th May 2018, we have undertaken a GDPR readiness programme to review our entire company, the way we handle data and the way in which we use it to provide our services.
Our GDPR readiness programme is looking at the following areas:
- **Staff training and awareness** – how GDPR, the Data Protection Bill and the ePrivacy Regulation will impact clients, employees and the supply chain
- **Supplier management** – ensuring all appropriate security, organisational controls and governance processes meet the demands of our clients and of IAS Laboratory as it continues to grow
- **Development** – ensuring we maintain our commitment to best practice and developing systems which meet recognised security standards and making sure we meet our commitment to privacy by design
- **Individuals rights** – refining our approach to handling requests for data, or the handling of data, to meet the new demands of GDPR (including the right of subject access, cease processing requests and erasure of personal data)
- **Data mapping** – a full review of all processes and systems to truly understand the customer experience, the data we hold and the way in which it is used
- **Data retention** – confirming data retention periods meet contractual, legal and organisations requirements.