Data Protection Statement
Last updated: 30 October 2026

Our Commitment
Grand Aesthetics Ltd ("we", "us", "our") is committed to protecting personal data. We comply with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. We implement appropriate technical and organisational measures to prevent unauthorised or unlawful processing and to protect against accidental loss, destruction or damage to personal data (UK GDPR, Article 5(1)(f)).

Scope
This statement covers personal data relating to patients, clients, website visitors, staff and suppliers, in all formats (digital systems, cloud services, and paper records). It applies to our employees and trusted third-party processors working on our behalf.

How We Protect Your Data
- Collect only the data we need for care delivery, bookings, enquiries, operations and legal requirements.
- Use data lawfully, fairly and transparently; keep it accurate and up to date.
- Limit access to authorised personnel, use secure systems and access controls.
- Apply data minimisation, retention limits and secure disposal/anonymisation.
- Never sell personal data. Share only with trusted providers or authorities where lawful and necessary.
- Do not store patients' bank account details in our patient systems or paper notes.

Security Measures (Examples)
- Secure servers, role-based access and multi-factor authentication where appropriate.
- Encryption in transit and at rest where appropriate; regular backups and recovery testing.
- Device management and patching; logging and monitoring for suspicious activity.
- Staff confidentiality agreements and regular data protection training.
- Vendor due diligence and data processing agreements with third-party providers.

What Counts as a Personal Data Breach?
A personal data breach is a security incident that leads to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. Examples include lost devices, human error, hacking, inappropriate access controls or equipment failure.

How We Handle a Breach
1. Contain and recover - isolate affected systems, secure accounts, restore from backups, and prevent further loss.
2. Assess risk - identify the data affected, sensitivity, protections (e.g. encryption), number and type of individuals involved, and potential harms.

3. Notify where required - we will notify the Information Commissioner's Office (ICO) without undue delay and within 72 hours where the breach is likely to result in a risk to individuals' rights and freedoms and inform affected individuals when there is a high risk.
4. Learn and improve - investigate root cause, update policies, enhance controls, and train staff as needed.

Governance & Accountability

- Policies: Privacy Policy - Access to Information, Information Security, and Business Continuity.
- Roles and training - staff are responsible for safeguarding data and reporting incidents promptly.
- Regular reviews -we test our controls, review risks and vendors, and improve continuously.

Your Rights

Under UK GDPR you have rights including access, rectification, erasure, restriction, portability (where applicable), and the right to object to processing, including direct marketing. You may withdraw consent at any time where processing is based on consent.

Contact & Complaints

To exercise your rights or raise a concern, contact: info@grandaesthetics.co.uk . You can also raise a complaint with the Information Commissioner's Office at www.ico.org.uk.

Related Policies

For more detail, please see our Privacy Policy and Cookies Policy on this website.