Security and Data Breach Policy

BookitZone takes handling of personal data very seriously and will continue to maintain the highest standards with respect to security of this data.

Data security
We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality.

As is our duty, we will report certain types of personal data breach to the relevant supervisory authority and will do this within 72 hours of becoming aware of the breach, where feasible .

Please note that there are always risks associated with providing personal data, whether in person, by phone or over the internet, and no system of technology is completely safe, "tamper" or "hacker-proof". BookitZone does have site security measures in place to protect your personal data, utilising RSA 2048-bit key/256-bit SSL encryption and implementing appropriate site security measures such as storing your personal data on secure servers with encrypted disks and controlling your account by password and username unique to you. We endeavour to continually review these measures to prevent and minimize risks of unauthorised access to, improper use of, and also the accuracy of, your personal data.

BookitZone does not collect or handle any credit/debit card information on site. Payments are handled securely off-site by an external transaction processing company.

BookitZone cannot guarantee the security or integrity of any personal data which is transferred from you or to you via the internet.

BookitZone may monitor or record communications with you (such as telephone conversations and emails) for the purpose of quality assurance, training, fraud prevention and compliance.