



DATA PRIVACY SECURITY POLICY

1. Objective

1.1 This policy ("Policy") sets out how each department within Regal Hotels International (the "Group") collects, uses, stores and handles Personal Data.

2. Commitment to Personal Data Protection

2.1 We are committed to protecting the privacy of the personal data ("Personal Data") we hold. To ensure that users can make informed decisions and feel confident about providing users' Personal Data to us, we outline in this Policy our practices and the choices users have concerning the collection and use of users' Personal Data.

3. The Personal Data We Collect

3.1 The types of Personal Data we collect from users will depend on the specific type of services and products as requested by, or provided to, users. The types of Personal Data may include (without limitation) the following:

- (a) users' personal information (e.g. users' name, gender and date of birth);
- (b) users' contact information (e.g. telephone numbers, mailing addresses, email addresses and fax numbers);
- (c) users' business information (e.g. company name, business title and associated contact information);
- (d) users' interests, personal preferences or comments;
- (e) information when users use our websites or other services or products (e.g. behavioural information, location information, browser details, IP addresses);
- (f) users' bank and credit card information.

3.2 Certain Personal Data (e.g. relating to users' personal information and contact information) are required for specific services or products and if users fail to supply such Personal Data as requested, we may not be able to deliver users the services or products. By providing users' Personal Data to us, users acknowledge that such provision is fair and reasonable in the circumstances.

4. Purposes for which Users' Personal Data is Collected and Used

4.1 The purposes for which users' Personal Data are collected and used may include (without limitation) one or more of the following purposes:

- (a) for the supply of any services, products, facilities and/or other subjects (together, the "Services") which the Group may offer to users, or users may require from us, from time to time;
- (b) for use of the online services available at any of the websites of the Group and/or through other telecommunication channels;
- (c) with users' consent, for marketing or promoting any of the Services of the Group (e.g. sending users updates on our latest offers and promotions in relation to any of our Services from time to time);
- (d) with users' consent, for promoting and soliciting donations or contributions for charitable or non-profit making causes;
- (e) for sale or purchase of any of the Services of the Group and/or for management or other related services;
- (f) for identification and verification purposes in connection with any of the Services that may be supplied to users;
- (g) for communicating with users by email, mail, fax, phone or other means, including contacting users regarding users' enquiries;
- (h) for making disclosures when required by law, regulation, or court order of any jurisdiction and/or as requested by any government, regulatory or law enforcement authority or administrative organisation, which may be within or outside The Hong Kong Special Administrative Region of the People's Republic of China ("Hong Kong");
- (i) for establishing legal claims or defences, obtaining legal advice, and/or exercising, defending and/or protecting the rights or properties of any member of the Group, including identifying, contacting or bringing legal action against any person who may be causing interference with such rights or properties (whether intentionally or otherwise) or where any other person could be harmed or property of any other person could be damaged by such interfering activities;
- (j) for the use by any member of the Group in connection with any of the above purposes and/or any of the Services that any member of the Group may offer or

supply to users from time to time; and/or

- (k) for any other incidental or associated purposes relating to the above, or any other purposes as specified in a personal information collection statement when users' Personal Data is being collected, or any other purposes which users may from time to time agree.

4.2 We will not knowingly or intentionally use, share or sell users' Personal Data in ways which are unrelated to the above purposes (or purposes as specified in a personal information collection statement when we collect users' Personal Data) without users' prior consent.

5. Disclosure and Transfer of Personal Data

5.1 To facilitate the purposes mentioned under "Purposes for which users' Personal Data are Collected and Used", we may transfer, disclose, grant access to or share users' Personal Data with third parties located within or outside Hong Kong, and users' Personal Data may be transferred within or outside Hong Kong. These third parties may include the following:

- (a) any member of the Group;
- (b) any agent, contractor or third-party service provider who provides administrative, distribution, data processing, telemarketing, telecommunications, computer, or other services to or support the operation of the Group's business (including its/their direct marketing activities);
- (c) medical professionals, clinics, hospitals, insurers and/or loss adjusters;
- (d) any person, government or law enforcement authority or administrative organisation; any person under a duty of confidentiality to any member of the Group (including accountants, legal advisers or other advisers);
- (e) any actual or proposed assignee or purchaser of all or any part of the business and/or asset of the Group; and/or charitable or non-profit making organisations.
- (f) The Personal Data users provide to us may also be sourced from or transferred to other jurisdictions outside Hong Kong for the purposes mentioned above.

6. Direct Marketing

6.1 If we intend to use users' Personal Data (including users' name and contact details)



collected from users for direct marketing purposes (e.g. to send users marketing communications about news, offers or promotions in relation to the Services or Activities of the Group), we will first obtain users' consent (or an indication of no objection) before doing so.

- 6.2 If we intend to provide users' Personal Data (including users' names and contact details) collected from users to third parties for their use in direct marketing, we will first obtain users' consent (or an indication of no objection) before doing so.
- 6.3 Users may opt out from receiving marketing communications from us at any time, free of charge by following the opt-out instructions contained in the communications.

7. Our Commitment to Children's Privacy

- 7.1 Protecting the privacy of children is our primary concern. Hence, we will not knowingly collect or maintain Personal Data in our database from persons who are under 16 years of age without prior consent from a parent or guardian.

8. Use of Cookies and Log Files

- 8.1 If users visit any of our websites, we may use cookie files to store and track information about users and users' preferences. A cookie is a small text file that our website transfers to users' computer's or device's hard disks. We use cookies to better serve users and/or maintain users' information across multiple pages within or across one or more sessions. Most web browsers automatically accept cookies, but if users prefer, users can edit users' browser options to block them in future. However, if users disable cookies or refuse to accept a request to place a cookie, certain functionalities on our websites may not be available.
- 8.2 Cookies contain information about users and users' preferences.
- 8.3 Only the information that users provide, or the choices users make while visiting a website, can be stored in a cookie. For example, the site cannot determine users' email name unless users choose to type it. Allowing a website to create a cookie does not give that or any other site access to the rest of users' computer, and only the site that created the cookie can read it.
- 8.4 We may also collect information regarding users' IP address, browser type, domain name and access time. This information is used for our own research purposes. As it is not linked to any personal information, it is separate from users' Personal Data. In rare instances, IP addresses may be used to assist in deterring and/or preventing abusive or criminal activity on the website.
- 8.5 If users use the WiFi available at our properties, we may collect users' location data

- 8.6 (if users have consented to this on users' device). We may use users' location data to keep track of users' activity patterns and preferences in order to improve the level of service users receive. Users' location data may be combined with other information we receive from third parties to provide users with better service and, where users have consented to receive direct marketing, we may provide users with targeted advertisements, content, features, deals and offers in relation to the classes of marketing subject as set out in the relevant personal information collection statement when users' Personal Data is being collected.
- 8.7 If users interact with us on social media platforms (for example if users "Like" our Facebook Page or post on our timeline), we can interact with users and send users messages via these platforms. We will interact with users in accordance with the social media platform's rules but we are not responsible for how the platform operators collect and handle users' Personal Data. We are not responsible for what third parties post on our social media accounts.

9. Data Retention

- 9.1 Subject to any legal, statutory, regulatory or accounting requirements, the Personal Data users provide to us will be kept by us in the appropriate form only for as long as is necessary to fulfil the purposes mentioned above after which it will be destroyed.

10. Data Security

- 10.1 To ensure the correct use and to maintain the accuracy of the Personal Data collected from users, as well as preventing unauthorised or accidental access, processing, erasure or other use of the Personal Data, we have implemented various internal policies (including physical, electronic and management measures) to safeguard and secure the Personal Data we collect.

- (a) For example, where we collect Personal Data online, we use an industry standard for encryption over the Internet known as Secure Socket Layer (SSL) protocol, to protect the Personal Data.
- (b) Our websites have firewalls in place, which should protect the Personal Data collected from users against unauthorised or accidental access. However, complete confidentiality and security are not yet possible over the Internet, and privacy cannot be assured in users' communications with us. Users are encouraged to protect against unauthorised access to users' passwords. Make sure users sign out from users' accounts when finished particularly when using a shared computer.

- 10.2 Effective security is a team effort involving the participation and support of every employee of the Group, who deals with or uses information and/or information

10.3 systems. It is the responsibility of every computer user to strictly follow these guidelines, and conduct his/her activities accordingly. Various internal guidelines have been implemented to protect the employees, the stakeholders and the Group from potential risks including that of virus attacks, compromise of network systems and services, and legal issues.

- (a) For example, whether the information contained on computer hard drives is confidential or not, employees should take all necessary steps to prevent unauthorized access to such information, especially any information contained on portable computers.
- (b)
- (c) Employees must pay extreme caution when opening e-mail attachments received from unknown senders, which may cause disastrous consequences. Unexpected or uncharacteristic emails from known contacts should be treated with extreme caution as well. Employees should not open and should delete those emails sent from unreliable sources, and should report the case to the MIS Department immediately.
- (d) The Group reserves the right to audit networks, systems and group-owned devices on a periodic basis to ensure compliance with the Group's Data Security Policies. The Group only carries out these monitoring activities to the extent reasonably necessary, using what it considers to be the least intrusive means, and with the least impact on the privacy of the employees concerned.

11. Other Websites

11.1 To anticipate users' needs, our websites may contain links to third-party sites that are operated under different privacy practices.

11.2 All such websites are independent from our websites. We have no control over the contents of such other websites or their privacy policies or compliance with the law. Users should therefore be fully aware the provision of such links does not constitute an endorsement, approval, or any form of association by or with the Group. We have no control over Personal Data that is submitted to these other websites. Users should remain alert when users leave our websites and read the privacy statements of other websites.

The Group and each department will review this policy from time to time as appropriate, and in any event, once every three years.

August 2025