

Privacy Policy

(As at 03 May 2017)

In this Privacy Policy:

- (a) the "Act" means the Singapore Personal Data Protection Act 2012 as amended, revised or re-enacted from time to time;
- (b) "personal data" has the meaning given to it in the Act;
- (b) any reference to "you", "your" and words of similar import means members of FPAS, online users and visitors to our website; and
- (c) any reference to "we", "us" or "our" and words of similar import means FPAS.

By accessing our website and any of its pages, you consent to the collection, use and disclosure of your personal data to us and agree to be bound by the following terms and conditions of our Privacy Policy.

1. Collection and Use of Personal Data

We only collect and use your personal data which is relevant and required for purposes of your FPAS membership or for informing you about courses or events that may be of interest to you as a FPAS member.

2. Withdrawal of Consent

You may at any time withdraw your consent to the collection, use or disclosure of your personal data by giving reasonable notice to us. If you withdraw your consent, we will inform you of the expected consequences of your withdrawal.

3. Handling of Personal Data

Only authorised staff and members of our Executive Committee have access to your personal data. Our authorised staff are required to abide by their contractual obligations to maintain the confidentiality and privacy of your personal data at all times. Executive Committee members undertake to keep all personal data strictly confidential.

4. Disclosure of Personal Data

We do not sell your personal data to anyone or any third party for marketing initiatives.

Your personal data will not be published on our website.

We will only disclose your personal data in limited circumstances such as to outsource or service vendors, our professional advisers, certification bodies (including but not limited to the Financial Planning Standards Board) and regulatory or law enforcement agencies or in accordance with the applicable laws or to enforce and protect our rights, powers and remedies under our security documents and other third parties for such purposes as we deem fit. When we transfer personal data to a recipient outside Singapore, we will ensure that the recipient is bound by law or contract to observe a standard of protection for the personal data that is at least comparable to the protection under the PDPA.

5. Compliance by Third Parties

We may share your personal data with third parties who provide support services or act as our agents. All such third parties must observe and comply with the same privacy policy standards as we do.

6. Security Measures in Place to Protect Personal Data

To protect and safeguard the confidentiality of your personal data and to ensure that it is safe, secure and private, we adopt the following systems security and monitoring measures:-

- Firewalls, data loss prevention system, anti-virus protection and intrusion detection systems to detect and prevent any forms of illegitimate activities and/or illegal intrusions of our network systems;
- Regular security reviews of our systems by our internal and external auditors;
- Vigilant monitoring to detect any suspicious online activities at our website

We are committed to monitoring our security system constantly for potential situations that could compromise the security or the privacy of our members, and visitors to our website and to exploring new technology continually to enhance our security system. Nevertheless, we do not warrant the security of your personal data transmitted to us using our website and online forms. This is because you accept the risks that any of your personal data transmitted to or received by us using our website and internet and online forms may still be accessed and/or disclosed by unauthorised third parties.

Information about use of cookies at our website

Currently, we do not use cookies at our website but may do so in the future. We will update information on the use of cookies at our website if there are changes in the future.

Your responsibility in safeguarding your personal data

- (a) If you wish to access our website, always directly enter our website address in the browser address bar. Do not access our website via any hyperlink within emails.
- (b) Clear your browser's cache and history after each session - default files on a computer, sometimes called "cache" files can retain images of personal data or otherwise sent to or received by us at our website, making them a potential target for a system intruder. Therefore, we strongly advise that you clear your browser's disk cache and history after each visit to our website.
- (c) Refrain from using a shared computer or an internet cafe computer to access our website's online Forms as such computers may be installed with certain software which could capture your personal data or otherwise without your knowledge.
- (d) If you have installed or downloaded any software which claims to speed up your internet connection or other software, games, screensavers etc, you should be aware that they may be spyware which has the ability to track your internet sessions and/or gain access to your personal data and Internet browsing history. We recommend that you uninstall such spywares.
- (e) Do not leave your personal computer unattended during your online session or using the online forms.

- (f) Ensure that your personal computer has the latest anti-virus, anti-spyware and firewall software and updates to guard against new viruses. Make sure that your computer's operating system and browser software are updated with the latest security patches.
- (g) Update us whenever you have changed your contact details in order for us to contact you in a timely manner on any issues or matters relating to your access to our website.
- (h) Contact us should you notice something suspicious or encounter any issues, difficulties or irregularities in accessing our website.
- (i) You should be aware of email frauds via phishing whereby generally you are asked to click a link to a fake website and provide, update or confirm your personal data. To bait you, the fraudsters may falsely inform you of a fake urgent or threatening condition concerning your certification. Please note that we will never send you an email requesting for your personal data or information regarding your certification details with us. You should NOT respond to such fraudulent emails.
- (j) Do not open email attachments from strangers, install software or run programs from unknown sources or origins.
- (k) Delete junk or chain emails.
- (l) Email messages sent to us over the Internet containing your personal data cannot be guaranteed to be completely secure and you assume all risks arising or in connection thereto.

It is important that you do your part to ensure that any personal data provided to us via the online forms or email or any other channels of communication are done in a safe and secure manner. We will not be liable to you for any losses, damages, expenses, costs (including legal costs) and charges (whether direct or indirect, foreseeable or unforeseeable, special or consequential or economic loss) incurred or suffered by you arising out of you sending email messages containing your personal data to us over the Internet or for any error, fraud, forgery, system failure or anything beyond our control or in connection with your failure to adhere to the terms and conditions herein and/or your failure to follow the above recommended security measures.

7. Access to Personal Data

Under the Act, you have the right of access to your personal data in our possession or under our control or information which may have been used or disclosed by us within a year before the date of your request. Your request to us for access must be made in writing and subject to payment of such fees as may be prescribed by us from time to time. In addition, members can access their personal data using their login credentials through the FPAS website.

8. Correction of Personal Data

Keeping your personal data accurate and updated is very important to us. You can help us keep accurate records by informing us of any changes, errors or omissions in your personal data. If you have any reasons to believe that your records with us are inaccurate, incorrect, incomplete or not updated, please write to us. We will promptly update your records accordingly within fourteen (14) working days from the date of receipt of your request.

9. Retention of Personal Data

Your personal data will be retained by us for as long as the original purposes or the legal or business purposes for which your personal data were collected continues. If retention is no longer necessary, your personal data will be deleted, destroyed or de-identified from you unless retention of the same is required to satisfy legal or regulatory requirements or to protect our interests or in accordance with our policies.

10. Third Party Websites

This Policy does not extend or cover any third party websites which may be linked from and/or to our website. When visiting these third party websites, you should read their privacy policies.

11. Enquiries

If you have any queries, concerns or complaints relating to the collection, use or disclosure of your personal data, you may call us at tel: (65) 63721030 during office hours from 9.00 am to 5.00 pm from Mondays to Fridays or email us at admin@fpas.org.sg.

We will attend to your query as expeditiously as possible.

12. Amendments to the Policy

We may amend this Policy from time to time and will make available the updated Policy on our website. By continuing to access our website you agree to be bound by the terms and conditions of the Policy, as amended from time to time.

13. Governing Law and Submission to Jurisdiction

This Policy is governed by Singapore law and you agree to submit to the exclusive jurisdiction of the Singapore courts.

-end-