Friends of the University of Bristol Botanic Garden

DATA PROTECTION ACT 2018

Privacy policy

Introduction

This privacy policy sets out how the Friends of the University of Bristol Botanic Garden ('the Friends') uses and protects any personal information that you give us when you become a member of the Association or make a donation. The privacy and security of your personal information is important to us and we wish you to be confident about giving it to us.

What we collect

When you join the Friends or make a donation we may collect the following personal data which is required in connection with your membership.

- Name, address, telephone number and email address.
- Financial information such as credit or debit card or bank details and whether we can claim Gift Aid.

How we use your personal data

- Details are required for registration of membership.
- Financial information is used in connection with the payment of the annual subscription or donations or to claim Gift Aid.
- Your email or telephone number may be used if there are any queries regarding your membership.
- Your personal address will be used for issuing the Friends' newsletter and the Botanic Garden Index Seminum.
- If you have provided an email address this will be used to send out the enews with additional information and updates on activities related to the Botanic Garden and its supporters.

Security

We are committed to ensuring that your information is secure. In order to prevent unauthorised access or disclosure, we have put in place suitable physical and electronic procedures to safeguard and secure the information we collect. You should be aware that your information is available only to the appropriate Friends' committee members.

Controlling your personal information

We will not disclose your personal information to third parties. You may request details of personal information which we hold about you under the Data Protection Act 1998. If you would like a copy of the information held on you please write to membership@fubbg.co.uk

If you believe that any information we are holding on you is incorrect or incomplete, or if you believe you have submitted any personal information that you did not wish to divulge then please contact membership@fubbg.co.uk to get the information corrected or removed.

The Seven Principles of the Data Protection Act

Lawfulness, fairness and transparency

Data must be processed lawfully, transparently and fairly, as well as communicating details, regarding data collection and processing, to individuals in plain and clear language, and easily understandable by data subjects giving consent.

Purpose limitation

Not only must data be collected in a transparent manner, but the purposes stated at the point of collection must not be extended in practice. A data subject should be privy to the purpose of their data being processed, though it should be noted that processing for public interest, scientific or historical research or for statistical purposes is not necessarily considered ‘incompatible’ with this right.

Data minimisation

This principle obliges organisations to limit their collection of data to the minimum needed for the intended purpose. Rather than just hoarding enormous loads of information, a company is required to hold only what is adequate, relevant and necessary.

Accuracy

Personal data being held must be kept up to date, as well as reasonable measures being taken to ensure data is accurate. Should it be known that personal data is not accurate and cannot reasonably be corrected or rectified, then data must be erased and deleted.

Storage limitation

This principle of storage limitation obliges organisations to keep personal data no longer that necessary for the intended and previously stated reason. Though, again there are provisions allowing prolonged retention for some purposes (scientific, statistical etc.), information must not be simply kept indefinitely.

Integrity and confidentiality

Organisations must take appropriate measures to ensure the security of personal data and protect against the possibility of a data breach. Not only taking the form of technical measures (encryption, anonymisation etc.), suitable organisational measures must also be taken.

Accountability

Finally, without an equivalent within the DPA 1998, the accountability principle lays the responsibility of data protection squarely at the feet of organisations handling personal data. Not only are organisations responsible for compliance, but also for the documentation of said compliance.