Heart of Appalachia Website Privacy & Use Policy

Effective Date of Current Policy: January 1, 2021

1. INTRODUCTION

This Privacy Policy ("Policy") applies to heartofappalachia.com (the "Website") any subdomain of heartofappalachia.com (the "Subsite") and the Heart of Appalachia mobile application ("App") and the services Heart of Appalachia Tourism Authority ("Company" or "We") makes available through its Website and App ("Services") on behalf of one or more clients. This Privacy Policy describes how we collect, use, and disclose certain information. If you disagree with our policies and practices, do not use our Website or download our App. Your continued use of the Website or the App constitutes your acceptance to this Policy. We may change this Policy from time to time. Your continued use of the Website or App after we make changes is deemed to be acceptance of those changes.

Residents of California are provided certain rights regarding their Personal Information under California Law. Residents of California should review the California Privacy Notice that supplements and forms a part of this Privacy Policy. The California Privacy Notice is available at: https://heartofappalachia.com/california-privacy-notice/

Our Service is not intended for children under 13 years of age. You must be 13 years or older before using our Service. If you are under 13 please stop using our Service immediately and do not submit any information to us.

2. INFORMATION WE COLLECT

User-Provided Information: We may collect your name, email address, and other information you share when you sign up for the Service directly or log in through your Facebook account. We may also collect interests you have selected, as well as places, events, or tours you have added to your plan.

Location Information: We may use data transmitted from your mobile device to determine your location and use it for the purpose of marketing and analyzing customer information. This Information allows us to periodically determine your location.

Device Information: We may collect certain information from your mobile device, which may include information about your device; information about your use of features, functions, or notifications on the device; and signal strength relating to WiFi or Bluetooth, and other technical data. We may collect this information even if you are not logged in to the Service.

User ID: An automatically generated unique identifier for authenticated users on the Services.

Plan ID: An automatically generated unique identifier for any user (authenticated or anonymous) that adds any item to their plan in the Services.

OneSignal Player ID: An automatically generated unique identifier for any user that accepts push notifications on the Apps.

Firebase Instance ID: An automatically generated unique identifier for any user that accesses the Services through the Apps.

Plot Projects User ID: An automatically generated unique identifier for any user that accepts location and notification services on the Apps.

IDFA: An automatically generated unique identifier for any user that accesses the Services through the Apps.

Cookie Information: We may place small files, known as "cookies" on the hard drive of your computer to save your preferences. You may disable browser cookies, but then you may be unable to access certain features of the Service.

Non-Identifying Information: We may collect other non-identifying information.

3. USE OF THE INFORMATION

We use information that we collect or that you provide, including any personal information to:

Register Your Account: Your name, email, and other information you share are used to register your account and allow you to use our Service on the same device in the future as well as on other devices from which you access the Services.

Maintain Your Plan & Preferences: Your interest selections and any places, events, and tours added to your plan are used to maintain your plan on the same device in the future as well as on other devices from which you access the Services.

Enhance or Improve the Service: Your account information and preference selections are stored and used to enhance your use of the Services and to understand how you use our Service.

Device Information:

User ID: Your User ID is used to enable cross device use of the Services.

Plan ID: Your Plan ID is used to enable saving of unique plans for use on the same device or other devices from which you access the Services.

OneSignal Player ID: The OneSignal Player ID is a UUID (Unique Universal Identifier) that OneSignal creates per device per OneSignal App Id. The Player Id is generated based on the Google Advertising ID for Android and identifierForVendor for iOS. It is used for the delivery of notifications to App users of the Services who have accepted notifications on their device.

Firebase Instance ID: Google's Firebase Instance IDs are used to identify individual installations of the apps for the purpose of improving the Services through monitoring analytics, crashes, and Android Cloud Messaging.

Plot Projects User ID: The Plot Projects User IDs are dynamically generated unique identifies per installation of the app to connect the data generated by each device for the purpose of delivering location based notifications to improve the Services and provide notifications about nearby attractions of interest.

IDFA: The Identifier for Advertisers (IDFA) is a random device identifier assigned by Apple to a user's device. The IDFA is used to deliver customized advertising. The IDFA is used for tracking and identifying a user without revealing personal information.

Send you emails and respond to inquiries.

Provide user support.

Carry out other purposes that are disclosed to you and to which you consent.

4. DISCLOSURE OF THE INFORMATION

We may disclose your personal information to our vendors and other third parties we use to support the Service and who have agreed to keep personal information confidential and to use the personal information only for the purposes for which we disclose it to them.

We may disclose your personal information to authorities if compelled to by a court order. We may disclose your personal information if we believe that you have violated a U.S. law or our Terms of Service or Privacy Policy or if we believe that a third party is at risk of bodily harm. We may also report you and release your information to third parties if we believe that it is proper to do so for legal reasons. You release us from any damages that may arise from or relate to the release of your information under the conditions listed in this paragraph.

We may also disclose personal information to a buyer or other successor in the event of a merger, divestiture, reorganization, dissolution or other sale or transfer of some or all of our assets, whether as a going concern or as part of bankruptcy, liquidation or similar proceeding.

User data may be shared with partner organizations or organizations represented by Heart of Appalachia in the delivery of its core mission to market the Southwest Virginia region to the general public.

We will not sell or share your personal information or email address to other businesses or third party websites other than as noted in the previous paragraphs.

5. MODIFYING OR DELETING YOUR INFORMATION

After creating an account, you may be able to edit information submitted through the Service by accessing your account. If you want your personal information to be removed from our database please contact us. We delete user information at regular intervals, but we cannot guarantee that your information has been or will be deleted immediately. Some information may still be stored in a web browser's cache or in other devices.

6. THIRD PARTY SITES

We may post links to third party websites through the Service. If you access a third party site through our Service, you acknowledge that these third party websites are not screened for privacy or security issues by us, and you release us from any liability for the conduct of these third party websites.

7. SECURITY

We use commercially reasonable efforts to keep your personal information secure. We make no guarantees, however, as to the security or privacy of your personal information. To protect your personal information, we recommend you use firewalls, anti-virus, spyware and other encryption methods when submitting personal information or content to us

8. CROSS-BORDER TRANSFER

Your information may be transferred to – and stored on – computers located outside of your state or province. We may transfer personal information to the United States and process it there. Your use of the Service constitutes your agreement to that transfer.