Privacy Notice

This policy details how we respect privacy when we handle personal data.

It details what personal information we collect and how we use it.

This Privacy Policy applies to information we collect from:

- visitors to our website and ticketing platform
- those who visit or engage with our social media accounts
- those who subscribe to our newsletter
- visitors to Edinburgh Cocktail Week

If you have any comments or questions about this Privacy Policy, please contact our designated Data Protection Officer, Gary Anderson, on hello@edinburghcocktailweek.co.uk

You have the right to make a complaint to the ICO if you think there is a problem with the way we handle data.

1. Collecting and storing information

We may collect, store and use personal information that you provide to us when:

- enquiring about our event via email or our website
- subscribing to our email newsletter
- purchasing a ticket for our event via our website, or ticketing platforms including Citizen Ticket

Information collected is stored electronically on our website, ticketing platforms, email, and email marketing provider's external servers until we delete it. You can request for your information to be deleted at any time.

1.2 Cookies

A 'cookie' consists of information downloaded to your computer when you visit a website. Cookies are widely used within digital marketing and can do a number of things, i.e. remember your preferences, record what you have put in your shopping basket, and count the number of people who visit a website.

We use Google Analytics, Google Adwords and Facebook Business Manager to analyse the use of our digital platforms and build lists of people who have visited our website and Citizen Ticket and engaged with our social media channels. Google Analytics, Google Adwords and Facebook Business Manager generate statistical and other information about users by means of cookies, which are stored on users' computers. The information collected about usage of our website is not personally identifiable. The data is collected anonymously, stored by Google and Facebook and used by us to create reports and digital marketing campaigns.

Here are links to privacy policies for Google, Facebook and Citizen Ticket.

2. Using your personal information

Personal information submitted to us via email, our website, Citizen Ticket and social media channels will be used for the purposes specified in this privacy.

We may use your personal information to:

- enable your use of the services available on our website and ticketing platforms
- reply to enquiries and registrations you send to us
- send you marketing communications by email relating to our business which we think may be of interest to you (you can inform us at any time if you no longer require marketing communications)
- deliver digital marketing campaigns specific to our event and business which we think may be of interest to you (you can inform us at any time if you do not want us to use your data for these purposes)

We will not, without your express prior consent, provide your personal information to any third party.

3. Updating and deleting your information

You can submit a request to update or delete your information at any time. If you would like us to update or delete your data, please submit your request by email to hello@edinburghcocktailweek.co.uk

When submitting your request, please tell us which information you would like us to update or delete from the list below:

- information submitted by email, website or social media
- information submitted when subscribing to email marketing (Mailchimp)
- information submitted when purchasing a ticket via our website or other ticketing platform

We will acknowledge receipt of your request by email and update and/or delete your information within one week of acknowledgement. There is no charge for updating or deleting your information unless we deem your request to

be excessive. For such requests, an external Data Management Consultancy will be contracted to perform your request and their service fee will be charged back to you, with your prior consent.

The updating or deletion of information is actioned by our Data Protection Officer by logging into each individual system and updating and/or deleting your data, including searching our central server for your information and permanently deleting your information from all our devices (including their recycling/deleted bins).

Here are links to more information on how information is deleted on our website, Citizen Ticket and Mailchimp.

4. Data Breaches

The cyber threat landscape is constantly evolving, so it's important that we evolve with it. This means making sure our employees and technology are up to date with new attack methods and the ways criminals exploit organisations.

To help us avoid data breaches we:

- train our team on how to avoid data breaches
- only store information electronically on password protected devices
- only store information electronically on systems that have strict data protection policies and software in place to deter breaches
- regularly change passwords

In the event of a data breach, which may result in a risk to the rights and freedoms of individuals – if, for example, it could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage, we will notify the ICO within 72 hours of the breach.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, we will notify those affected by email or social media announcement within 72 hours of the breach.

We are able to detect possible data breaches by:

- training our team how to detect data breaches and how to report this
- receiving a notification of a password change which was not actioned by our team
- receiving a notification of a login from an unverified device which was not approved by our team
- being unable to log into a system
- identifying irregular activity on any of our systems or social media channels
- being notified of unusual email activity
- being notified by one of our tech providers of a data breach
- monitoring the news for reports of data breaches

Following the reporting and investigation of a data breach, policies and procedures will be developed and implemented to help avoid and manage future breaches. This is the responsibility of our Data Protection Officer.