WIMBORNE
HISTORY FESTIVAL

General Data Protection Regulation

The General Data Protection Regulation (GDPR) came into force on 25th May 2018.

This paper sets out the information required for the general public, suppliers and others that have a relationship with Wimborne History Festival Limited (WHFL).

1 Data Protection Officer

1:1 The WHFL does not require a Data Protection Officer, but Tracy Whitham, WHFL Chair, is the main point of contact for any Data Protection issues.

2. Processing of Data

2:1 WHFL deals with the public, suppliers and volunteers. All information about people, irrespective of the context, will be treated with the same level of care.

2:2 WHFL is both Controller and Processor of the data that it holds. It uses data to:

- Raise invoices
- Pay invoices
- Communicate

2:3 No unnecessary data is held. No sensitive data is held.

2:4 Data is held in five ways:

- Web Server
- Dropbox
- Accounting Software
- E-mail
- Mailing Service (Mail Chimp)

2:5 Other parties that we share data with

Contractors and suppliers, who have access to our mailing lists and social media accounts during specific project-driven time periods.

2:6 Contractors

WHFL requires contractors to submit a GDPR statement about how they manage and control data. Our Terms and Conditions require them to remove access/delete any data that they have used as a part of their contract.

Data is accessed by desktop/laptop and other mobile devices. All such devices have password or other device-specific security. All passwords are complex.

3. Web Server

3:1 Some data is held on a web server, which is hosted by GODADDY.

3:2 The computer is password secured.

4. Dropbox

4:1 Data is held in Dropbox.

4:2 All access to Dropbox is via user-name and complex password.

5. Accounting Software

5:1 Spreadsheets are used for accounting.

5:2 Accounting data is held on a Synology server housed in an office secured by alarms connected to a monitoring service.

6. E-mail

6:1 WHFL uses a webmail service for e-mail, with local copies of e-mail on laptops. All laptops are password secured.

7. Mailing Service

7:1 WHFL uses MailChimp for sending mailshots and newsletters. Every e-mail sent allows-opt out. Individuals who have asked to be added to the mailing list have been signed-up through MailChimp, and the date and time that they added themselves is recorded

7:2 The MailChimp Website (https://kb.mailchimp.com/accounts/management/about-the-general-data-protection-regulation) contains the following information"

"We've been researching the GDPR and modifying many of our internal practices and policies over the last year, because we are committed to achieving compliance with the GDPR in 2018. For example, we're in the process of updating our Data Processing Agreement and third-party vendor contracts to meet the GDPR's requirements.

We're also assessing the impact of the GDPR on MailChimp's tools to see if we can make them more practical for users who are subject to the GDPR.

As further guidance is released and our research progresses, we'll continue to look for ways we can help our users around the world get ready for the GDPR."

8: Access to Data

8:1 Should you want to see the data that we hold about you, please contact T Whitham at directors@wimbornehistoryfestival.co.uk

9. Deletion of Data

9:1 Should you want us to delete the data that we hold about you, please contact, T Whitham at directors@wimbornehistoryfestival.co.uk .

9:2 Please note WHFL cannot delete financial or contractual information for seven years.

9:3 Should you receive a mailing from us and want to opt-out please follow online instructions to do so.

10. Data Breach

10:1 It will be mandatory to report a personal data breach under the GDPR if it's likely to result in a risk to people's rights and freedoms.

10:2 If we are notified of or detect a data breach we will first investigate to ensure that the source of the breach is identified and, if necessary, closed. If our investigation shows that there has been a breach, we will:

- Notify the Information Commissioner's Office and other bodies as appropriate
- Assess the level of risk of the accessed data
- Notify those impacted by the breach and inform them of any actions that they should take
- Take appropriate steps to stop the breach being repeated.