CFS Events Use of Personal Data Policy & Staff Briefing Note

May 2017

Protecting Other Peoples' Data

Data Protection and Freedom of Information Acts

As CFS Events Ltd holds and processes information about our clients, employees and suppliers, we are legally obliged to protect that information.

Under the Data Protection Act, CFS Events must:

- only collect information that we need for a specific purpose;
- keep it secure;
- ensure it is relevant and up to date;
- only hold as much as we need, and only for as long as we need it; and
- allow the subject of the information to see it on request.

Good information handling makes good business sense, and provides a range of benefits. It can enhance the business' reputation, increase customer and employee confidence, and by ensuring that the information is accurate, save both time and money. But largely we NEED to do it to comply with the law.

Staff Training on Data Protection:

- All staff members to have read and understood the ICO's paper, 'Taking a positive approach to information rights'
- All staff members to have read and understood the ICO's paper, 'Training checklist for small and medium sized organisations'
- All staff members to have read and understood the CFS Events Ltd Data Protection Policy (below)

Collecting Personal Data

Under the Data Protection and Freedom of Information Acts, we must bear the following in mind when collecting personal data from delegates, speakers and suppliers:

- We are only to collect the personal information we need for a particular business purpose
- We must explain new or changed business purposes to customers, and obtain consent or provide an opt-out where appropriate
- We need to update records promptly – for example, changes of address, marketing preferences
- We need to delete personal information the business no longer requires, in an appropriate fashion

Which data is classed as 'personal'?

Any information relating to a living individual that is held on one of our computers or in an organised filing system that could identify that person (names, addresses, email addresses etc.)

Card Payment Security:

When requesting card payment details from Customers NEVER ask for the 3 digit security code in writing, only collect this verbally. When taking card payment details over the phone from a Customer they should be written down on a separate sheet of paper and the transaction completed whilst the Customer is on hold.

This ensures that the card details are correct and the Customer knows that the transaction has been completed successfully. Any problems can be resolved whilst the Customer is on the line. As soon as the transaction has been completed the sheet of paper with the card details MUST be shredded immediately.

Computer Security:

Cybercrime is a growing and increasingly sophisticated industry and it is important that we all follow basic security measures to minimise this threat.

Each PC should have an updated version of Internet Security software (Norton or Kaspersky) and have settings enabled to ensure regular software updates are installed automatically. It is also essential that the automatic settings allow a full scan of each PC on a minimum of a weekly basis. Any problems found during the scan should be reported to the Data Security Manager.

Emails – Antivirus software will usually intercept malicious emails but it is not perfect so it is important to always be vigilant and suspicious of unusual emails, particularly those with attachments or those with links requesting you to click on them to confirm your details. If in any doubt DO NOT OPEN the email or attachment and seek advice from the Data Security Manager.

CFS Events Policy Checklist for collection of personal data:

1. Is it necessary to collect the individual's personal information?

- Circumstances where it is acceptable to ask for individual's personal data:
- During the event registration process
- When booking flights and/or accommodation for those individuals
- Where CFS Events requires that information for billing purposes

2. Do I know what I will use this information for?

- If you are unsure as to the purpose for collecting information this could equate to a breach of Data Protection Laws – always check with a manager if you are unsure

3. Have I let those people whose information I am collecting know what it will be used for?

CFS Events Fair processing notice (FPN):

Data Protection Note: Please be aware that CFS Events Ltd will store this data securely for use in conjunction with this specific meeting, for example in the booking of travel or accommodation. CFS Events Ltd will **not** sell your personal data to third parties for commercial purposes. CFS Events Ltd will securely dispose of any financial information relating to you as soon as it has been used for the purposes for which it was obtained.

From time to time, CFS Events Ltd may contact you, using the personal information provided to notify you of other educational meetings which may be of interest. If you would like to opt out of these listings, please email admin@cfsevents.co.uk, and insert 'REMOVAL FROM DATABASES' into the subject line.

- Include this FPN at the bottom of:
- All regonline pages
- All requests for speaker and exhibitor personal information
- Any correspondence which requests responses which will include personal information

4. If data is to be stored for marketing purposes (all regonline databases) were individuals made aware that their details could be used in this way?

- CFS Events will include the fair processing notice on all regonline forms
- CFS Events will include an option to opt-out on all mass-emails
- After events, individuals who have opted out of this MUST be removed from databases and their data stored so that they are not re-entered onto a database

5. If the purposes for which I intend to use the information change, have I made the individual aware of that?

Opt-out of CFS Events Databases

1. **Receive a request for opt-out of our databases**
2. **Act immediately**
3. **Go to Regonline**
4. **Go to Email Invites Tab**
5. **Search for the name/email address in recent email invitation list**
6. **Select Name**
7. **Select Opt-out**

Opt-out following an event

1. **Following an event, act immediately**
2. **Go to Regonline**
3. **Go to Email Invites Tab**
4. **Create new email invitation list**
5. **Create a list with just the attendees of the event you have just run in it**
6. **Pull a report showing those people who have OPTED OUT of our databases**
7. **Select each name on the list and select 'opt-out'**

Disposing of Personal Data Policy Checklist:

In disposing of any hardcopy personal data CFS Events will:

- Shred all personal data

In disposing of any electronically held personal data, CFS Events will:

- Permanently destroy any personal information, including financial information which is no longer needed
- In the event of an individual opting out of their data being stored- permanently delete their personal data from databases and ensure they cannot be re-added

Protecting CFS Events' Data

Credit/Debit card Security:

One of the many conditions set by Lloyds is that the card pin number should never be written down nor shared with anyone. (NEED to check this as it doesn't make sense!!)

Hotels and venues frequently request card payment details to guarantee a reservation. Under NO circumstances must the 3 digit security code, on the reverse of the card, be sent with the card details by fax, post or email. Neither must the card be photocopied /scanned and emailed , faxed or posted. The security code, if requested, may ONLY be given verbally after confirming the identity of the person requesting the information.