TAKE ONE ACTION FILM FESTIVALS: PRIVACY & DATA SECURITY POLICY

Take One Action are the UK's leading global change film festival. We believe small actions lead to big ones and that we all make a difference. We connect individuals and groups through film, creativity and action for a better world – starting from Scotland.

Privacy and security are of key importance to Take One Action. We are acutely aware of the importance of data security – that of our audiences, staff and our organisation – and we are committed to ensuring that our activities and work methods are created in such a way that our high standards are upheld and that our work abides by current best practice and regulations including GDPR legislation.

OUR BUSINESS:

Take One Action was established in 2008 to celebrate the people and movies that are changing the world and inspire positive social change. We do this through annual festivals held in the Autumn in Edinburgh, Glasgow, Aberdeen and Inverness, one-off events across the year and by supporting a network of Local groups who organise their own screenings across the country. Our small team is helped by a group of passionate and dedicated volunteers throughout the year.

OUR IMPACT:

We are committed to ensuring that all data is secure in relation to our

- audiences
- filmmakers and event contributors
- staff and volunteers
- office practice

OUR COMITTMENTS:

We are committed to ensuring that all of our activities prioritise the privacy and security of personal data. Our main areas of focus are:

- Separating all audience demographic data from identifiable data (names and email addresses) and ensuring that only the necessary information is collected and stored;
- Creating password protected folders for any files containing personal data and ensuring these are not stored on any cloud platforms;
- Shredding and securely disposing of any documents with personal data;
- Upholding a strict timeline for the storing and deletion of personal data;
- Regularly updating business passwords on any accounts holding personal data;

- Ensuring that all admin and account holders on our website and social media accounts are valid and known.

Signed: 

Tamara Van Strijthem
Executive Director

Date: 14 Feb 2018

TAKE ONE ACTION FILM FESTIVALS: PRIVACY & DATA SECURITY PLAN

Take One Action aim to be a responsible, trustworthy and engaged organisation in areas of data privacy and security and we are committed to improving our policies and tools in this area. The aim of this Action Plan is to outline the steps we will take to fulfil our commitments and eliminate any areas of weakness in our practice. The following areas have been identified as being of key importance:

- our audiences
- our filmmakers and event contributors
- our staff and volunteers
- office practice

1. OUR AUDIENCES:

Objective:	Action:	Time Line:	By Whom:
1.1 Obtain all audience data with consent and clarity	• All audience information shall be gathered with full consent – either through opt in sign up forms at screenings or via opt in mailing list sign ups on the TOA website • The TOA Privacy & Data Policy		
1.2 Store all audience data securely	• Only collect the information that is needed • Separate identifiable data (name and email address) from any demographic data collect on receipt and store separately. • Use secure organsiation laptops to load names and email addresses on to MailChimp and then delete from all devices and cloud platforms. • Anonymise all demographic data • If identifiable data needs to be stored this will be password protected and stored on a hard drive, not on a Cloud-based platform, and deleted after 3 years • All physical copies of personal data will be stored securely in a locked office	Ongoing – after each event or festival	Festivals & Networks Development Officer

1.3 Delete all audience data securely	• All identifiable personal data from audiences will be stored no longer than 3 years after which it will be deleted and securely disposed of (e.g. shredded) • Any audience data shared through online platforms (e.g. enquiry forms on website, ticket bookings) will be deleted automatically after 3 years if not done so manually • Audience information created by the user themselves via a profile on the TOA website will be stored securely and can be deleted completely upon request, or by the user themselves.	Ongoing	Festivals & Networks Development Officer

2. OUR FILMMAKERS & EVENT CONTRIBUTORS:

Objective:	Action:	Time Line:	By Whom:
2.1 Store all filmmaker and event contributors data securely	• All contact details will be stored securely on password protected computers and cloud platforms • All passport details will be stored securely on password protected computers and cloud platforms • Individuals contact information will be retained after the festival/event for contact purposes only – no additional personal information will be stored	Ongoing	Festivals & Networks Development Officer

3. OUR STAFF:

Objective:	Action:	Time Line:	By Whom:
3.1 All staff details (personal, financial etc.) are stored securely	• All identifiable personal information will be stored in a password protected folder with the password regularly updated	Ongoing	Executive Director

4. OFFICE PRACTICE:

Objective:	Action:	Time Line:	By Whom:
4.1 All office equipment will be secure	• Staff will use secure passwords for every computer and online account • Each password will be different • Passwords will be changed every 12 months • Computers will never be left unattended in public spaces • Back up hard drives will be checked regularly to ensure that all necessary personal information has been deleted • Hard drives containing personal data will be stored in a locked drawer	Ongoing	All staff
4.2 Website security will be maintained by web designer	• Website designer will ensure that the website server and all cloud platforms and apps used on the website are based in Europe and that no data passes through non-secure countries	Ongoing	Festivals & Networks Development Officer & Website Designer
4.3 Emails and online platforms will be secure and maintained	• Staff will ensure that automatic log in is not enabled on laptops • Staff will only use secure wifi connections when out of the office • Staff will clear out old emails every 12 months to ensure that no secure data is kept unnecessarily • Staff will delete any emails containing identifiable personal information after use	Ongoing	All staff
4.4 The office space will be securely locked at all times	• Staff will ensure that the door and windows are locked when the office is empty • The securely locked doors between the office and the main entrance to the building will be closed and locked at all times.		
4.5 Materials containing personal information will be stored securely if taken out of the office	• Staff will be responsible for all materials taken out of the office and will not leave these unattended in public places (e.g. email sign up sheets, volunteer contact forms etc.)		