Data Protection

Purpose

The purpose of this policy is to ensure that staff, volunteers and trustees of NoFit State Circus are clear about the purpose and principles of Data Protection and to ensure that the organisation has all necessary guidelines and procedures in place which are consistently followed. Failure to adhere to the Data Protection Act 1998 is unlawful and could result in legal action taken against individuals of NoFit State Circus its staff, volunteers or trustees.

Contents

Responsibility

NoFit State are registered with the Information Commissioner's Office (ICO) as a Data Protection Controller (under registered number ZA058887).

NoFit State's Data Protection Officer: Alison Woods, Executive Director
NoFit State's Data Controller: Luc Morris, Communications and Marketing Officer

At the beginning of any new project or type of activity the member of staff managing it will consult the Data Controller about any data protection implications.

There may be situations where NoFit State Circus works in partnership with other organisations on projects that require data sharing. NoFit State will clarify which organisation is to be the Data Controller and will ensure that the Data Controller deals correctly with any data that NoFit State Circus has collected.

Policy Statement

NoFit State Circus collects and uses personal information about and from a wide range of beneficiaries, staff, donors, contractors and subcontractors, volunteers, applicants, and partners. This personal information will be dealt with properly and securely in line with the Data Protection Act 1998 regardless of how it is collected, recorded and used.

NoFit State Circus regards the lawful and correct treatment of all personal information as essential to the successful and efficient performance of charitable aims and to maintain the confidence of everyone with whom it comes into contact

To this end NoFit State Circus fully endorses and adheres to the principles of Data Protection as set out in the Data Protection Act 1998.

The organisations and people about which NoFit State holds information are referred to in this policy as data subjects.

NoFit State Circus holds 5 types of information which are covered by this policy:

organisational information - both publicly available and some confidential information

internal data records - staff, volunteers and trustees

external data records - members, customers, clients

personal information - information about individuals such as names, addresses, job titles

sensitive personal information - next of kin, health and medical details, financial information, criminal records, etc.

Information about organisations is not covered by the Data Protection Act. However, there is sometimes ambiguity about whether certain information is personal or organisational. For instance, the contact details for a developing company may be someone's home address Also NoFit State strives for best practice regarding organisational information. For these reasons organisational information is covered by this policy.

Principles

The Data Protection Act 1998 regulates the processing of information relating to living and identifiable individuals (data subjects). This includes the obtaining, holding, using or disclosing of such information, and covers computerised records as well as manual filing systems and card indexes.

Data users must comply with the data protection principles of good practice which underpin the Act. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

To do this NoFit State Circus follows the eight Data Protection Principles outlined in the Data Protection Act 1998:

1. Personal data will be processed fairly and lawfully
2. Data will only be collected and used for specified purposes
3. Data will be adequate, relevant and not excessive
4. Data will be accurate

5. Data will not be held any longer than necessary
6. Personal data must be processed only for specified and compatible purposes
7. Personal data must be processed in accordance with the rights of the subject
8. Personal data must be kept secure adequately protected if it is to be transferred outside the European economic area

Consent

NoFit State Circus will not hold information about individuals without their knowledge and consent.

NoFit State Circus will only hold information for specific purposes. It will inform data subjects what those purposes are. It will also inform them if those purposes change.

Data subjects will be given the option not to be contacted by NoFit State about anything other than essential information (eg. class/event cancellations, emergency contact).

Information about data subjects will not be disclosed to other organisations or to individuals who are not members of NoFit State staff or Board except in circumstances where this is a legal requirement, where there is explicit or implied consent or where the information is publicly available elsewhere.

Where practicable, NoFit State will seek consent from individuals before displaying photographs in which they appear. If this is not possible (for example, a large group photo), the company will remove any photograph if a complaint is received. This policy also applies to photographs published on the company's website or in the Newsletter.

Data subjects will be entitled to have access to information held about them by NoFit State Circus. A written request must be submitted and a £10 administration charge may apply plus the data subject must prove they are the data subject. Request to be dealt with within 21 days.

Data will be kept safe from unauthorised access, accidental loss or damage
Information is kept in a secure filing, paper and electronic system and is only accessed by those individuals involved in the delivery of the service, who have had the data protection training and have signed the organisations's data protection agreement. Information will not be passed on to anyone outside the organisation without their explicit consent, excluding statutory bodies e.g. the Inland Revenue.

Information will not be retained once it is no longer required for its stated purpose.

Personal data is kept in paper-based systems and on a password-protected computer system. Every effort is made to ensure that paper-based data is stored in an organised and secure manner.

Accuracy
NoFit State Circus will seek to maintain accurate information by creating ways in which data subjects can update the information held.

Implementation
All staff will be given training on the data protection policy and procedures.

All staff, trustees and volunteers dealing with data will sign a document to confirm they will uphold the organisation's data protection procedures and a confidentially agreement

Review
NoFit State Circus will carry out an annual review of its data protection policy and procedures.

Access
Only the organisation's staff, volunteers and trustees will normally have access to personal data.

All staff, volunteers and trustees will be made aware of the Data Protection Policy and their obligation not to disclose personal data to anyone who is not supposed to have it or the misuse of personal data.

Department Guidelines and Procedures

Marketing
Responsibility for overseeing this department: Luc Morris

We only use contact data from people who have willing opted in either by signing up to our newsletter or when booking tickets for classes and shows. This is stored on Patronbase or Mailchimp, both of which are password protected.

We include 'unsubscribe' buttons when sending out newsletter campaigns.
If contacted by an individual and asked to be removed from our mailing lists and data base we will do so within 21 days of them contacting us.

For corporate marketing purposes we collect contact data which is freely and publicly available and will not use the home or personal details of a particular person.

Where possible, we attempt to only use photographs of people who have given consent to have their image used, and will remove any image if a complaint is made by someone who does not wish their image to be used.

We will ensure that we only secure personal data from a partner organisation when the data subject has given explicit consent for their data to be shared. Once we receive the data it is protected under our policy.

Our website uses Google Analytics and other associated tools to collect and log visitor information in an anonymous form via the use of cookies on your computer. No personally identifiable information is collected about the user. This information is compiled to produce statistical reports on website activity and metrics to optimise content and marketing.

Reception and administration data
Responsibility for overseeing this department: Beth Coffey

Data held by reception contains personal details plus sensitive medical information. This information is kept locked in a room that is only accessible by NoFit State staff and company members.

The only people with access to these records are designated members of staff who have signed our data protection agreement and received relevant training in our guidelines and procedures.

Bookings are made using the Patronbase box office system which is password protected and only once training is complete are passwords issued. Passwords are regularly changed and each staff member has a personal log in.

No personal details will be passed on to another individual without prior consent from the data subject.

For card payments taken over the phone, or otherwise when the card-holder is not present, the card receipt will be shredded and a receipt be printed from Patronbase.

Data subjects have an opportunity to opt out of mailings list with an unsubscribe button on the bottom of mail outs. Any written request from a data subject to remove their details from our database will be completed with within 21 days.

All computers are password protected and only authorised staff are allowed on these computers or to view personal data.

All paper data records are shredded before being disposed of.

Teachers
Responsibility for overseeing this department: Tan Watson and Beth Coffey

NoFit State teachers will have access to participants' and learners' sensitive data including medical information and injuries history. All teachers are under contract to only share this information with other relevant teachers.

As outlined in the teacher's contract this information must not be shared with others in the class without expressed consent from the data subject and never with an external source/ person other than medical professionals such as ambulance staff.

Tour Box Office
Responsibility for overseeing this department: Tim Adam

Data collected in the ticket booking process is defined by the Head of Box Office, Tim Adam.

All Box Office staff and volunteers receive training on the organisation's Data Protection guidelines and procedures and will have signed the data protection policy to uphold these. The Patronbase box office system is password protected and only once training is complete are passwords issued. Passwords are regularly changed and each staff member has a personal log in.

The only payment details held will be card receipts. All card details take over the phone will be entered will be entered directly on to a card machine wherever possible. If card details are

ever written down the information will be electronically processed and all paper records destroyed before the end of a shift.

For telephone bookings the data subject is asked if they would like us to keep their receipt. If the answer is 'no' then the receipt is shredded straight away. If the answer is 'yes' the receipt is attached to the ticket and their name and the card presented or last four digits of the card is confirmed before the ticket and receipt is given to data subject.

All merchant copy card receipts will be kept securely in the tour safe and transferred secure storage in Four Elms as soon as possible.

The reason the information is requested will be explained at the time of booking; for example, a phone number in case of problem with booking or a show cancellation.

Data subjects will be asked within the ticket booking process if they would like to be on the NoFit State mailing list. Only consenting data subjects will be contacted by the company.

Funding and Development
Responsibility for overseeing this department: Bethan Touhig-Gamble

All personal details of individual donors are kept on a password secure computer. These details are never shared without expressed permission of the data subject.

Contact details for events are kept separate from the CRM systems.

Board meeting minutes, funding forms and business plans are kept in a secure lockable office and cupboard and password secure computers.

Any group e-mails are sent out as BCC or via secure invite service like Mailchimp.

All online donations are processed through a recognised and secure donation service – (PayPal and Just Giving) and therefore the organisation never sees or has access to any donor bank details.

We have secure storage for all necessary paper copies of all agreements, financial information with access confined to staff processing that information who have had the correct training and have signed the organisation's data protect agreement.

Finance
Responsibility for overseeing this department: Wendy Hii

Employee details
- Only specifically necessary information will be collected
- Payroll software is only accessed by authorised staff and is password protected.
- Individuals can request for details of information held by them once they have proved they are the data subject.

Account Details
- Online banking system can only be accessed by authorised and fully trained staff.
- User name and password kept in a secure place and require card authentication device.
- Account details only kept as long as needed

Computer security

- All computers have firewall and virus checking systems
- Regular backups of information are made and secured off site

General

- All credit card slips are kept in a locked secure cupboard and are not kept longer than necessary
- Information is collected for specific purposes and stored in locked cupboards and password secure computers
- Information is reviewed regularly to ensure it is relevant and up to date

Visa Information and sponsorship licences
Responsibility for overseeing this department: Lizzy Ferguson

Relevant data subjects will be made aware of the details and documentation that will be kept in regards to sponsorship licences and work visas. These files are kept in a locked cupboard and password secure computer system only accessible by Lizzy Ferguson and Alison Woods.

Barring and Disclosure Procedures
Responsibility for overseeing this department: Lizzy Ferguson

Relevant data subjects will be asked to go through the Barring and Disclosure Procedures by the company verifiers; Lizzy Ferguson, Sarah Smith or Lynn Carroll. Data and results are confidential and will be kept securely within the guidelines of the Barring and Disclosure Code of Practice.

Company Procedures in case of lost or stolen data

How we respond to lost or stolen data?
There are four important elements to any breach-management plan. We will:-

1. Containment and recovery

- Define who takes the lead in the investigation
- Define what needs to be done to stop it happening again
- Define who needs to be made aware of the breach (Line managers, Data Controller/Officer, individuals whose data is lost or stolen, the ICO and/or the Police)
- If it is a staff or volunteer who has breach data protection immediate suspension may be necessary whilst an investigation takes place
- Ensure a robust recovery plan

2. Assessing the risks

- Define the nature of the data lost
- Clarify data's sensitivity
- Define how many individuals are at risk
- Assess any risk associated with the breach, and define how this affects what we do once the breach has been contained
- Assess the potential adverse consequences for individuals and the company; how serious or substantial these are and how likely they are to happen?

Potential Consequences

Company	Individuals
Loss of trust	Disciplinary proceedings
Fines	Civil proceedings
Civil proceedings	Criminal proceedings
Seizure of data	Loss of employment
Loss of future funding	

3. Notification of breaches

Notification will always be given to:

- The individual responsible for the security breach
- Their line manager
- The Data Controller
- The Data Officer
- The Board of Trustees

Notification may be given to:

- The individuals involved
- The ICO
- Regulatory Bodies
- The police
- Financial institutions

4. Evaluation and response

The causes of any data breach will be investigated and the company's response to the breach will be evaluated. If necessary, policies and procedures will be updated accordingly.

Document History		Due for review	March 2017
Last updated	06/05/2016 Lizzy Ferguson	Approved by NFS Board	
	12/03/2015 Sarah Smith		
	12/06/2015 Alison Woods and Sarah Smith		
	11/07/2014 Alison Woods		