Data Protection / Confidentiality Procedures

This guide is for everyone who accesses data through Fall into Place Theatre, including directors, volunteers and all staff.

What is data?

Data is anything that can identify a person. It includes email addresses, photos, phone numbers etc.

What data does Fall into Place hold?

Fall into Place holds the following data:

Group attending members and interested members (those who have asked about joining our groups, have attended in the past or are members already): photos, emails and phone numbers (received consent for).

Training Workshop database – emails and phone numbers of workplaces in Leeds (publically available from websites or gained consent for).

Photos of workshops, performances and young people (gained parental and child consent for).

Partners Database (emails and phone numbers of local charities who can signpost people to our groups and performances) – publically available on websites.

Names, medical information and other relevant information about children attending our holiday clubs / after school clubs (gained consent for).

Contact, recruitment and other relevant information of our freelancers and volunteers.

Where does Fall into Place store data?

Online:

On google drive - you need a password to log in.

Confidential information will be kept in a locked cabinet, along with finances and any other personal data on paper.

How is it kept secure?

We have log in security on google drive and a lock for the cabinet.

All our computers and devices are password protected.

We will permanently delete all data or destroy any old computers or phones, to avoid their data being used again.

We will check that our 'lending laptop' is wiped of all data before a new person uses it.

How can I ensure I keep all data secure?

Follow these instructions:

Do not download personal data or write it down. If you need to do one of these things, make sure you destroy it/permanently delete it as soon as you are finished with it.

Use and keep personal data in the secure folder they are saved in. Put paper files away in the locked drawer immediately after use.

Ensure all marketing contact, such as by phone, email or home address, contains our opt out line: "If you no longer wish to hear from us, you can opt out by…"

Do not share any passwords or data with anyone else. Do not email personal data to your own personal email address.

Only use memory sticks or external hard drives that Fall into Place have provided, so that we can ensure they are encrypted.

Do not pass an individual's personal email or phone number onto someone else without that person's consent.

We cannot use data for reasons that we have not gained consent for. If in doubt ask one of the Responsible Persons.

Gain written (or email) consent from people before storing or sharing their data, including photos on social media.

If using social media, please read our social media policy (if you have not received this please request it from your line manager.)

Use our photo consent forms and gain consent from the pupil's legal guardians before taking or sharing photographs of children. Delete off your phone / camera as soon as they are saved securely in the online drive.

In addition to the point above, with close up photographs or videos of children where the child is the focal point and easily identified, please ask for consent from the child before sharing on social media.

Avoid sending mass 'bcc' emails where possible, and if needed double check it says 'bcc' before sending.

Don't leave your laptop screen open or personal files out when leaving your desk, e.g. to go to the bathroom.

If you are given access to a secure folder, virtual or physical, do not share with other people without first gaining permission from your line manager and/or the person who gave you access.

Always log out of everything and put everything away before leaving the office/finishing for the day.

What is a breach?

A breach means personal data has been taken by someone who should not have access to it. For example, a computer is stolen, or you accidentally email the wrong person some personal data.

What should I do if I suspect a breach?

Tell a responsible person immediately. They will then have to inform the ICO if it is deemed worthy of reporting.

What should I do if someone asks to see his or her data?

We must show people how we store and use their data. Immediately tell a responsible person who will show the individual their data.

What should I do if I'm unsure or need more advice?

Speak to a Responsible Person:

Sarah Shaw

Last updated: 12 April 2021 by Sarah Shaw and Vanessa Brown