Data Protection Policy

Reviewed on: March 2019

Strike A Light (the data controller) need to collect, store and use (data processing) information (personal data) about individuals (data subjects) in order to effectively deliver our organisational aims, commitments and legal obligations. Some of this data might be sensitive data for example about an individual's ethnicity or religion (special category data). We may also need to pass on data to other organisations for specific purposes (data processors).

This may include information on our audiences, participants, staff or other organisations with whom we work.

This policy sets out how we will do this in a way which ensures we comply with current data protection legislation and protects the rights and privacy of the individual.

Organisational Responsibilities

Under the General Data Protection Regulation (GDPR) 2018 we have a legal responsibility to ensure that data is processed lawfully, fairly and in a transparent manner in relation to individuals.

We must ensure that personal data we hold is:

- Collected for specific, clear and legitimate purposes and only used in the ways which were specified when the data was originally collected.

- Relevant and limited only to the data that we need

- Accurate as far as is reasonable and kept up to date where required

- Only kept for as long as is necessary and securely destroyed afterwards

- Processed securely

And that as an organisation we can demonstrate compliance with these principles.

Staff Responsibilities and Training

The lead member of staff for Data Protection is Christina Poulton, Executive Director, but all staff have a responsibility to ensure that the processes laid out in this policy are observed.

All staff should read this policy carefully and raise any questions with the Data Protection lead to ensure they are clear on their responsibilities.

To ensure an effective whole-organisation approach to data protection we will:

- Provide a data protection briefing on induction and detailed training on any aspects relevant to a particular role for staff and trustees, for example within box office or marketing
- Provide briefings to volunteers collecting or handling data, for example mailing list sign ups or evaluation forms
- Provide whole staff training every two years
- Keep up to date on legislation through the Data Protection lead and provide briefings when there are significant updates or changes to legislation
- Include data protection on board agendas

Recording and Reviewing Data Processing and Compliance

We have carried out a data audit which will be reviewed annually. This details:

- what personal data we process
- why we process it
- how we have communicated this information to the data subject
- whether this is special category data
- a confirmation that this is the minimum data required to complete the task
- how the data is kept securely
- how long the data is held for
- how the data is checked for accuracy and kept up to date
- any actions required

Regarding reasons for processing, GDPR sets out 6 reasons why data may be processed. These are:
- Consent (when a data subject gives consent)
- Contract (in order to be able to deliver or enter in to a contract)
- Legal obligation (where the law requires it)
- Vital interests (to protect someone's life)

- Public task (to perform a task in the public interest or for official functions)
- Legitimate interests (necessary for your legitimate interests unless there is a good reason to protect the individual's personal data which overrides those legitimate interests)

Where consent is given the data audit will also record for that particular type of data:
- how consent is given and where this is recorded
- how people can as easily withdraw their consent, for example by unsubscribing

After each review, individual staff members will then be briefed as to their responsibilities and the actions needed relating to different data.

In addition to the above, where we are collecting sensitive data, we must also meet one or more additional criteria to have a reason to process the data. Those that are relevant to our work include:

- The individual whom the sensitive personal data is about has given explicit consent to the processing.
- The processing is necessary so that you can comply with employment law.
- The processing is necessary for monitoring equality of opportunity, and is carried out with appropriate safeguards for the rights of individuals.

We will also carry out an audit of third party processors which details:
- the type of data shared
- the reason for sharing it
- how data is transferred securely
- how we know the processor complies with data protection law
- That the processor does not transfer data outside of the European Economic Area (EEA) and if so that their data protection is at least equal to that of companies inside the EEA (e.g. IOS Certificate or US Security Shield) and how data subjects are informed of this
- any actions needed

GDPR compliance should be demonstrated through contracts with third party processors, for example specifying how data will be kept securely included in terms and conditions for mailing list software used or specific data protection clauses included in contracts with external payroll companies.

Actions and Compliance

The data audit details actions specific to individual types of data processing. The following actions for compliance underpin this but should not be seen as exhaustive. Staff should take responsibility for ensuring a data audit is carried out, with the support of the Data Protection lead, when new forms of data are collected and new technologies are implemented.

Marketing
- ensure privacy and cookie policies are up to date and compliant
- ensure mailing list sign up statements follow requirements for unambiguous, specific and, where possible, granular options e.g. choosing what they receive information on and by what methods- phone, email etc.
- ensuring an audit is carried out for any third party processors used e.g. mailing software
- ensuring the legal basis for direct marketing, either by legitimate interest or consent, is clearly established, recorded and appropriate actions taken
- ensuring consent can be clearly given by an affirmative action and as easily withdrawn

Participation
- ensure young people's data is only processed with their guardian's consent
- ensure young people's data is only shared on a need to know basis e.g. medical information with workshop tutors
- ensure all freelancers, tutors and volunteers are briefed regarding their data protection responsibilities regardless of how short their contract is
- ensure young people's data is kept securely during practical sessions e.g. permission forms during a workshop

Box Office
- ensure terms and conditions for box office use reflect current data protection legislation and are available to the customer
- ensure mailing list sign up options include clear, compliant information being given to the customer regardless of ticketing method e.g. online, by 'phone or in person.
- ensure third party ticketing systems are audited and compliant
- ensure data sharing agreements with third parties e.g. touring companies, are effectively implemented with information being shared with customers at point of collection and an audit carried out

Operations
- ensure website privacy policy and cookie policy is clear and compliant and online providers have been audited
- ensure audits, staff training and briefings are carried out
- ensure IT policies are in place and compliant and staff are briefed
- ensure IT software and hardware is audited and offers sufficiently robust security
- ensure procedures are in place for responding to data breaches, subject access requests, data portability and requests for the right to be forgotten and to support staff in responding to such requests

All staff
- ensure data is updated as soon as inaccuracies are discovered e.g. if you receive an email bounceback
- ensure unnecessary duplicates of data are not created e.g. multiple versions of a mailing list

- ensure copies of personal data are not made on to personal computers
- use strong passwords and password protect files and lock screens for computers that contain personal data.

Storing Data Securely

The data audit will include an audit of how each type of data is secured.
General practice should include:
- use of locked filing cabinets or similar where data is stored on paper, memory sticks or other physical items
- shredding of paper data that is no longer required
- Computer log in passwords that are strong, not shared and changed regularly
- restrictions on access levels and use of passwords where data is stored on a cloud based system or network
- only using third party processors, which includes cloud based systems, where this has been audited and agreed
- Not saving data to personal computers, mobile ‘phones or similar devices.

Where data held is special category data, this should be noted in the data audit and security measures interrogated to ensure they are sufficient.

Breaches

In the event of a security breach, the Data Protection lead must be informed immediately.
Depending on the circumstances of the breach action will include:
- completing an incident report
- taking action to address the cause of the breach
- taking action to minimise the damage that may be caused by this data not being kept securely
- possible disciplinary action

If the breach is likely to result in a risk to people’s rights and freedoms, for example discrimination, damage to reputation or financial loss, it is mandatory to report a personal data breach to the ICO within 72 hours. The Data Protection lead will make this report and also report to the Chair of trustees. This may then also need to be reported to the Charities Commission as a serious incident that has been reported to a third party regulator.

If a member of staff realises that they have been processing data in a way not compatible with the data audit or with the way in which it was originally collected they must also inform the Data Protection lead as soon as possible so a plan of action can be agreed.

Individual Rights

Individuals can withdraw their consent to their data being processed at any time. They can also request to restrict processing e.g. that we can use their data to send them information about one type of activity but not another. They should also be able to quickly and easily request that the data we hold about them is updated and any corrections made.

In instances where consent was actively given and used as the legal basis for processing, it must be as easy to withdraw consent and this must be acted on immediately.

Individuals also have the right to be forgotten e.g. all data held about them removed, and the right to data portability e.g. for us as an organisation to provide their data in a format which is then suitable to be transferred to another organisation or that we undertake that transfer for them.

If the data is being processed by any other purposes, for example, legal obligation, then we as an organisation may reject this request but this should be referred to the Data Protection lead.

Individuals can also submit a subject access request, whereby we as an organisation would provide all of the data we hold on that individual. This must be done free of charge and within one month of the request.

As an organisation we can extend the period of compliance by a further two months where requests are complex or numerous and we will inform the individual within one months of this and explain the reasons why.

If a request is excessive or clearly without relevant purpose, in particular where it involves repetitive tasks we can choose to charge a reasonable fee, proportionate to the administration incurred or refuse the request. In the event that a request is refused we will respond within one month to explain the reasons for this decision and inform the individual of their right to complain to a supervisory authority or take legal action.