



FERTILE
GROUND

Fertile Ground Privacy Policy

Fertile Ground is the North East of England's premiere touring dance company.

Dedicated to talent development and retention in the North East and North of England Fertile Ground aims to nurture, challenge and inspire a new generation of dance artists and develop and present inspirational and accessible dance for the people of the North. During 2019 Fertile Ground will extend its reach and present work both regionally and nationally.

The Company's vision is to help make the North East of England *the* place to dance. We collect statistics and feedback from our audiences and workshop participants and data from staff, contractors and suppliers.

Consent

When we collect data that may be personal e.g: for purposes of training, health and safety, monitoring equal opportunities, we ensure that we have the data subject's consent and that the data subject has been made aware that they have the right to withdraw that consent.

Consent must be:

- Specific to the purpose for which we are using the data
- Unambiguous
- Active not implied: Silence is not consent; pre-ticked boxes, inactivity, failure to opt-out or passive acquiescence will not constitute valid consent.
- Freely given: Consent will not be valid if the data subject does not have a genuine and free choice or cannot refuse or withdraw consent without detriment.

Ways in which we may ask for consent include:

- Written consent;
- Ticking a box on a web page;
- Choosing technical settings in an app;
- Verbal consent (which is then recorded in writing);
- Any other statement/conduct that clearly indicates (in this context) the data subject's acceptance of the proposed processing of personal data e.g: cookie acceptance.

We only publish data that we have permission to publish.

We do not contact individuals for direct marketing purposes by email, the internet, phone, fax or any other electronic systems that may be introduced, without prior consent.

We provide opt-out opportunities in all our mailings to ensure compliance with the principle that data held should be accurate and up to date. All our mailings make it clear who the sender is, so the recipient's ability to opt out is viable.

We do not share data with any third parties. Our audiences, participants, staff, contractors and suppliers are given the choice to opt in to:

- FG processing any personal data they may provide.
- FG using their data for marketing purposes, i.e to send news and training and events information.

Training

FG workshop booking forms include tick boxes to indicate:

- Consent to FG processing any personal data provided, in relation to the workshop booked
- Consent to FG retaining any personal data provided for future notification of information about FG events.

It also includes a statement that we do not sell, trade or rent personal data to others, information about the right to be forgotten and information on how to make a data subject request.

Staff recruitment

The FG application form includes a declaration that states that the applicant understands that their personal data is being processed solely for the purpose of this specific job application and that sensitive data in the Equal Opportunities Monitoring form is processed anonymously. It also states that we do not sell, trade or rent personal data to others, that application material will be destroyed after 12 months and information on how to make a data subject request. Rejection letters offer the option to have personal data kept on FG records for more than a year if they want to be considered for other vacancies.

Staff recruitment-diversity monitoring

These forms are anonymous, separated from job application forms immediately and destroyed as soon as the data they contain has been processed.

Deletion of data

Data subjects have the right to request to be “forgotten”, FG will delete records in line with GDPR as follows:

- When processing can cause substantial damage or distress;
- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed;
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing;
- If the personal data was unlawfully processed.

If personal data being erased has been disclosed to third parties we will inform them about the erasure, unless it is impossible or involves disproportionate effort.

If personal information has been processed online, for example on social networks, forums or websites we will inform any other organisations who are involved to erase links to, copies or replication of “forgotten” personal data.

FG will not always delete records, a request to be forgotten can be refused where data has been processed:

- To exercise the right of freedom of expression and information;
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority;
- For public health purposes in the public interest;
- For archiving purposes in the public interest, scientific research historical research or statistical purposes; or
- For the exercise or defence of legal claims.

The principles of good data protection practice

FG processes data in line with the Act, which says that:

- Personal data shall be processed fairly and lawfully.
- Personal data shall be obtained only for specified, lawful purposes and shall not be further processed in any manner incompatible with such purpose(s).
- Personal data shall be adequate, relevant and not excessive in relation to the purpose(s) for which they are processed.
- Personal data shall be accurate and, where necessary, kept up to date.
- Personal data processed for any purpose(s) shall not be kept for longer than is necessary.
- Personal data shall be processed in accordance with the rights of data subjects under the Act.
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss, destruction of or damage to, personal data.
- Personal data shall not be transferred to a country or territory outside the EEA unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.