



En Pointe Theatre Arts Data Protection Policy

Introduction

En Pointe Theatre Arts is committed to ensuring the lawful, fair and transparent management of personal data.

All founders and employees, including freelancers, part-time and temporary staff, along with volunteers, have a responsibility to ensure compliance with this policy, which sets out our commitment to process personal data in accordance with the following legislation:

- UK General Data Protection Regulation
- UK Data Protection Act 2018 (DPA 2018)
- Privacy and Electronic Communications Regulations 2003 (PECR)

Failure to comply with data protection legislation could lead to financial penalties, regulatory action, as well as reputation damage.

En Pointe Theatre Arts is also committed to ensuring compliance with the Children's Code (The Age Appropriate Design Code).

Scope

The policy applies to all personal data that En Pointe Theatre Arts holds in relation to living identifiable individuals regardless of the category of data or the format of the data.

Personal data is any data which could be used to identify a living individual, including e.g. name, address, email, postcode., CCTV image and photograph. Special Category

personal data is any information relating to racial or ethnic origin, political opinions, religious beliefs, health (mental and physical), sexual orientation, Trades Union membership and criminal convictions.

The policy applies to personal data held or accessed on En Pointe Theatre Arts premises or accessed remotely via home or mobile working. Personal data stored on personal and removable devices are also covered by this policy.

This policy, along with the associated appendices, applies to all directors, employees and staff including freelancers, temporary or part-time staff and volunteers.

Responsibilities for compliance

The owner is ultimately responsible for ensuring En Pointe Theatre Arts meets its legal obligations.

All staff have a responsibility for ensuring personal data is collected, stored and handled appropriately and must ensure that it is handled and processed in compliance with data protection regulations this policy and the data protection principles.

The owner (Danielle Emms), with advice and assistance from the Data Protection Officer, is responsible for monitoring compliance with this policy and the data protection legislation, managing personal data breaches and data subject rights, recording and maintaining appropriate records of processing activities and the documented evidence required for compliance.

Compliance

En Pointe Theatre Arts will comply with our legal obligations and the **data protection principles** by ensuring that personal data is:

- **Processed lawfully, fairly and in a transparent manner in relation to individuals.**

Individuals will be advised on the reasons for processing via a Privacy Notice. Where data subjects' consent is required to process personal data, consent will be requested in a manner that is clearly distinguishable from other matters, in an intelligible and easily

accessible form using clear and plain language. Data subjects will be advised of their right to withdraw consent, and the process for Data Subjects to withdraw consent will be simple.

- **Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.** Personal data will only be used for the original purpose, and this will be made clear to the data subject. If En Pointe Theatre Arts wishes to use personal data for a different purpose, we will notify the data subject prior to processing
- **Adequate, relevant and limited to what is necessary in relation to the purpose for which they are processed.** En Pointe Theatre Arts will only collect the minimum personal data required for the purpose. Any personal data deemed to be excessive or no longer required for the purposes collected for will be securely deleted. Any personal information that is optional for individuals to provide will be clearly marked as optional on any forms.
- **Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that inaccurate personal data, having regard to the purposes for which they are processed, are erased or rectified without delay.** En Pointe Theatre Arts will take reasonable steps to keep personal data up to date, where relevant to ensure accuracy. Any personal data that has been shared with third parties will also be updated.
- **Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.** En Pointe Theatre Arts will hold data for the minimum time necessary to fulfil its purpose. Timescales for retention of personal data are outlined in our Retention Schedule. Data will be disposed of in a responsible manner, ensuring confidentiality and security.
- **Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.** En Pointe Theatre Arts will implement appropriate security measures to protect personal data. Personal data will only be accessible to those authorised to access personal data on a need-to-know basis. Employees will keep data secure by taking sensible precautions and following the relevant En Pointe Theatre Arts policies and procedures relating to data protection.

In addition, En Pointe Theatre Arts will comply with the Accountability Principle, which states that organisations are responsible for, and able to demonstrate, compliance with the above principles.

En Pointe Theatre Arts also complies with the new 2026 regulation in relation to complaints in relation to any data we hold which you deem to be misused. If you think this has happened, please utilise the form: <https://docs.google.com/forms/d/1onS42teJ0aVTtmSbtq4AZSGvlerDIUYxXPNe2gZ9h-c/edit>

En Pointe Theatre Arts aims to respond to Data complaints within 48 hours, conduct a full investigation within 4 weeks, and send a response to the individual submitting the complaint. If the investigation has not been completed to its fullest, you will receive a progress report with information on how the investigation is progressing and a date when you can expect the investigation to be completed.

If you are unhappy with the response from En Pointe Theatre Arts, you can make a complaint to the Information Commissioner's Office: <https://www.gov.uk/data-protection/make-a-complaint>

The Children's Code

En Pointe Theatre Arts will conform to the Children's Code (The Age Appropriate Design Code) and demonstrate that our services use children's data fairly and in compliance with data protection law. The code is a set of 15 flexible standards that explain how GDPR applies in the context of children using digital services, ensuring that the best interests of the child are the primary consideration when designing and developing online services. The 15 standards are:

- 1. Best interests of the child:** The best interests of the child should be a primary consideration when you design and develop online services likely to be accessed by a child
- 2. Data protection impact assessments:** Undertake a DPIA to assess and mitigate risks to the rights and freedoms of children who are likely to access your services which arise from your data processing. Take into account offering ages, capacities and development needs and ensure that your DPIA builds in compliance with this code.

- 3. Age-appropriate application:** Take a risk-based approach to recognising the age of individual users and ensure you effectively apply the standards in this code to child users. Either establish age with a level of certainty that is appropriate to the risks to the rights and freedoms of children that arise from your data processing or apply the standards in this code to all your users instead.
- 4. Transparency:** The privacy information you provide to users and other published terms, policies and community standards must be concise, prominent and in clear language suited to the age of the child. Provide additional specific 'bite-sized' explanations about how you use personal data at the point that use is activated.
- 5. Detrimental use of data:** Do not use children's personal data in ways that have been shown to be detrimental to their wellbeing, or that go against industry codes of practice, other regulatory provisions or Government advice.
- 6. Policies and community standards:** Uphold your own published items, policies and community standards (including but not limited to privacy policies, age restrictions, behaviour rules and content policies)
- 7. Default settings:** Settings must be high privacy by default (unless you can demonstrate a compelling reason for a different default setting, taking account of the best interests of the child)
- 8. Data minimisation:** Collect and retain only the minimum amount of personal data you need to provide the elements of your service in which a child is actively and knowingly engaged. Give children separate choices over which elements they wish to activate.
- 9. Data sharing:** Do not disclose children's data unless you can demonstrate a compelling reason to do so, taking account of the best interests of the child
- 10. Geolocation:** Switch geolocation options off by default (unless you can demonstrate a compelling reason for geolocation to be switched on by default, taking account of the best interests of the child). Provide an obvious sign for children when location tracking is active. Options which make a child's location visible to others must default back to off at the end of each session.
- 11. Parental controls:** If you provide parental controls, give the child age-appropriate information about this. If your online service allows a parent or carer to monitor their child's online activity or track their location, provide an obvious sign to the child when they are being monitored.
- 12. Profiling:** Switch options which use profiling 'off' by default (unless you can demonstrate a compelling reason for profiling to be on by default, taking account of the best interests of the child). Only allow profiling if you have appropriate measures in

place to protect the child from any harmful effects (in particular being fed content that is detrimental to their health and wellbeing).

13. Nudge techniques: Do not use nudge techniques to lead or encourage children to provide unnecessary personal data or weaken or turn off their privacy protections

14. Connected toys and devices: if you provide a connected toy or device, ensure you include effective tools to enable conformance with this code

15. Online tools: Provide prominent and accessible tools to help children exercise their data protection rights and report concerns

Data sharing

In certain circumstances, En Pointe Theatre Arts may share personal data with third parties. This may be part of a regular exchange of data, one-off disclosures or in unexpected emergency situations.

In all cases, appropriate security measures will be used when sharing any personal data.

Where data is shared regularly, a contract or data sharing agreement will be put in place to establish what data will be shared and the agreed purpose.

Prior to sharing personal data, En Pointe Theatre Arts will consider any legal implications of doing so.

Data subjects will be advised of data sharing via the relevant privacy notice.

Data processors

Where En Pointe Theatre Arts engages Data processors to process personal data on our behalf, we will ensure that:

- Data processors have appropriate organisational and technical security measures in place
- No sub-processors are used without prior written consent from En Pointe Theatre Arts
- An appropriate contract or agreement is in place explaining the full requirements of the data processor

Security incident & breach management

Occasionally, En Pointe Theatre Arts may experience a data security incident or personal data breach; this could be if personal data is:

- Lost e.g. misplacing documents or equipment that contains personal data through human error via fire, flood or other damage to premises where data is stored.
- Stolen; theft or as a result of a targeted attack on our network (cyber-attack)
- Accidentally disclosed to an unauthorised individual e.g. email or letter sent to the wrong address
- Inappropriately accessed or used

All security incidents or personal data breaches will be reported to and managed by the owner who will be advised and assisted by the Data Protection Officer.

The Information Commissioner's Office and the individuals affected will be notified promptly if required

All security incidents and personal data breaches will be managed in accordance with En Pointe Theatre Arts' information security incident and personal data breach management procedure (see appendices).

Individual rights

En Pointe Theatre Arts will uphold the rights of data subjects to access and retain control over their personal data in accordance with our data subject rights procedure (see appendices). En Pointe Theatre Arts will comply with individuals:

- **Right to be informed:** by ensuring individuals are informed of the reasons for processing their data in a clear, transparent and easily accessible form and informing them of all their rights
- **Right to access:** by ensuring that individuals are aware of their right to obtain confirmation that their data is being processed; access to copies of their personal data and other information such as the privacy notice and how to exercise this right

- **Right to rectification:** by correcting personal data that is found to be inaccurate. We will advise data subjects on how to inform us that their data is inaccurate. Inaccuracies will be rectified without undue delay.
- **Right to erasure:** (sometimes referred to as ‘the right to be forgotten’) we will advise data subjects of their right to request the deletion or removal of personal data when processing is no longer required or justified.
- **Right to restrict processing:** we will restrict processing when a valid request is received by a data subject and inform individuals of how to exercise this right
- **Right to data portability:** by allowing, where possible, data to be transferred to a similar organisation in a machine-readable format
- **Right to object:** by stopping processing personal data, unless we can demonstrate legitimate grounds for the processing which override the interest rights and freedoms of the individual, or the processing is for the establishment t exercise or defence of legal claims.

Data protection by design

We have an obligation to implement technical and organisational measures to demonstrate that we have considered and integrated data protection into our processing activities.

When introducing any new types of processing, particularly using new technologies, we will take account of whether the processing is likely to result in a high risk to the rights and freedoms of individuals and consider the requirements for a data protection impact assessment (DPIA).

All new policies, including the processing of personal data, will be reviewed by the owner to ensure compliance with the law and to determine whether a DPIA is required. As required, advice and assistance will be provided by the DPO, and if it is confirmed that a DPIA is required, it will be carried out in accordance with En Pointe Theatre Arts DPIA Procedure (see appendices).

Training

All staff will be made aware of good data protection practices and where to find guidance and support for data protection issues. Adequate and role-specific data protection training will be provided during induction and regularly thereafter to everyone with access to personal data, to ensure they understand their responsibilities.

Breach of policy

Any breaches of this policy will be dealt with in accordance with En Pointe Theatre Arts disciplinary procedures.

Monitoring and reporting

Regular monitoring and audits will be undertaken by the Director and/or DPO to check compliance with the law, this policy and associated procedures

Policy review

This policy will be reviewed and revised every three years or more frequently if required to meet changes in legislation, address any weaknesses identified and/or to implement new/ good practice or lessons learned.

Appendices”

1. Information security incident and personal data breach management procedure
2. Data subject rights procedure
3. Retention procedure and schedule
4. Data protection impact assessment procedure
5. Model data sharing agreement
6. Template data processor agreement
7. Privacy notice

