The Laurel Trust

Data protection policy

Date of last review: **January 2021**

Date of next review: **January 2023**

Review Period: **2 years**

Owner: **The Laurel Trust**

Data protection

1. INTRODUCTION

1.1. The Laurel Trust (Registered Charity Number: 1117330, Company Limited by Guarantee and Registered in England Number: 05774260, with registered office at c/o Stone King LLP, Boundary House, 91 Charterhouse Street, London, EC1M 6 HR.), "the Trust" is the Controller for the purposes of the UK General Data Protection Regulation.

1.2. The Trust collects and uses certain types of personal data (as explained in paragraph 2.1 below) of the following categories of individuals:

1.2.1. trustees and other volunteers involved in governance and delegated committees;

1.2.2. consultants commissioned by the Trust to enact the management of its affairs on behalf of the trustees;

1.2.3. professional advisers and service providers including third party solicitors and auditors and providers of book-keeping, banking and investment advice and management services;

1.2.4. teachers including headteachers and other professional or volunteer educational providers, advisers, evaluators, trainers and supporters working with the Trust on research projects and the dissemination of research outcomes through conferences, seminars and multi- media publications; and

1.2.5. other individuals such as educational academics and the trustees and senior managers of other charitable trusts who come into contact with the Trust and its research and dissemination activities.

1.3. The Trust processes this personal data to fulfil the charitable, public benefit functions of the Trust as a grant making organisation, dedicated to the advancement of education. The processing is carried out in the following ways:

1.3.1. we process the full names, email and workplace addresses and other necessary contact details such as telephone numbers of all categories of individuals listed in clause 1.2 above, to ensure effective communications; and

1.3.2. we undertake processing of personal data required to comply with any legal obligations imposed on us.

1.4. This policy is intended to ensure that personal data is processed lawfully, fairly, transparently and securely and in accordance with the UK General Data Protection Regulation (the "UK GDPR"), the Data Protection Act 2018, the Privacy and Electronic Communications (EC Directive) Regulations 2003 and other related legislation (the "UK Data Protection and Privacy Laws"). It applies to personal data regardless of the way it is used or recorded and for as long as the data remains in the Trust's control.

1.5. The UK GDPR applies to all personal data held in electronic systems and structured manual files.

1.6. This policy will be updated as necessary to reflect any possible changes to the Trust's organisation, new processing activities, new regulatory guidance, best practice and any amendments to the UK Data Protection and Privacy Laws, and shall be reviewed every 2 years.

2. PERSONAL DATA

2.1. ‘Personal data’ means any information that identifies or is capable of identifying an individual. A sub-set of personal data, known as ‘special category personal data’ relates to:

2.1.1. race or ethnic origin;

2.1.2. political opinions;

2.1.3. religious or philosophical beliefs;

2.1.4. trade union membership;

2.1.5. physical or mental health;

2.1.6. an individual’s sex life or sexual orientation;

2.1.7. genetic or biometric data for the purpose of uniquely identifying a natural person.

2.2. The Trust does not collect or process any special category personal data or any personal data of individual children involved in research projects. The confidentiality and processing of children’s personal data is the responsibility of the schools and other educational providers involved in research projects receiving grants from the Trust.

3. THE DATA PROTECTION PRINCIPLES

3.1. The Trust is committed to complying with the seven data protection principles laid down in the UK GDPR at all times. This means that the Trust will:

3.1.1. process personal data lawfully, fairly and transparently (i.e. it will inform individuals (especially by way of privacy notice) about how and why it processes their personal data

3.1.2. process personal data only for the purposes for which it has been collected;

3.1.3. collect and process only personal data that is adequate, relevant and necessary in relation to the purposes for which it has been collected;

3.1.4. ensure accuracy of personal data and will keep it up to date;

3.1.5. ensure that personal data is not held longer than is necessary for the purposes for which it has been collected and is disposed of in a secure manner.

3.1.6. ensure that appropriate security measures, as required under the UK GDPR, are in place to safeguard integrity and confidentiality of personal data processed by the Trust.)

3.2. The Trust has procedures for responding to individuals’ requests, complaints and queries relating to personal data and is committed to ensuring that any person dealing with personal data on its behalf will facilitate the exercise of data subjects’ rights (as explained in more detail in paragraphs 7 and 8 below).

3.3. The Trust will share personal data with third parties only when it is necessary and lawful to do so (as explained in more detail in paragraph 5 below).

3.4. The Trust will address and manage any personal data breaches and any breaches of the UK Data Protection and Privacy Laws in accordance with the procedure in paragraph 9 below.

4. LAWFUL BASIS FOR PROCESSING

4.1. The Trust will process personal data only where it has lawful basis for it. We will usually rely on the following lawful basis:

4.1.1. the individual has given us their informed, unambiguous and free consent to the particular type of processing of their personal data; or

4.1.2. the processing is necessary for the performance of a contract, to which the individual is a party, or is necessary for the purpose of taking steps to enter into a contract with the individual, at their request; or

4.1.3. the processing is necessary for the performance of a legal obligation to which the Trust is subject; or

4.1.4. the processing is necessary to protect the vital interests of the individual or another; or

4.1.5. the processing is necessary for the performance of a task carried out in the public interest; or

4.1.6. the processing is necessary for a legitimate interest of the Trust or of a third party, except where such interest is overridden by the interests or fundamental rights and freedoms of the individual concerned. More details of this are given in the Privacy Notice.

5. DISCLOSURE OF PERSONAL DATA

5.1. The following list includes the main reasons why the Trust might authorise disclosure of personal data to a third party:

5.1.1. to give a confidential reference relating to a current or former consultant or volunteer;

5.1.2. where it is necessary for the prevention or detection of crime;

5.1.3. where it is necessary for the assessment of any tax or duty;

5.1.4. where it is necessary to exercise a right or obligation conferred or imposed by law upon the Trust;

5.1.5. for the purpose of, or in connection with, legal proceedings (including prospective legal proceedings) or any investigation by a statutory authority or regulator; or

5.1.6. for the purpose of obtaining legal advice.

5.2. To fulfil its functions in compliance with the law, the Trust may need to share personal data with third party recipients, such as the Trust's consultants, professional advisers (for example, its solicitors) and service providers (for example, its accountants or IT consultants). All such third parties will be subject to contractual obligations as required by law, and will need to provide confidentiality undertakings.

5.3. Where the Trust receives requests from third parties (i.e. those other than the data subject and the Trust), to disclose personal data it holds, such data will not be disclosed unless necessary to comply with legal obligation or otherwise lawful.

5.4. All requests for the disclosure of personal data must be sent to the Chair of Trustees, who will review and verify the identity of the requesting third party before deciding whether to make any disclosure.

6. SECURITY OF PERSONAL DATA

6.1. The Trust will take reasonable steps to ensure that trustees, consultants and third-party advisers and service providers will only have access to personal data where it is necessary for them to carry out their

duties. All such persons will be made aware of this Policy and their duties under the UK Data Protection and Privacy Laws. The Trust will take all reasonable steps to ensure that all personal data is held securely and is not accessible to unauthorised persons.

6.2. Due to the size of the Trust and the fact that it does not have employees, the Trust does not have its own ICT equipment. Those handling personal data within the Trust (trustees, consultants and volunteers) use their own ICT equipment. Those handling personal data related to the Trust's activities must at all times use their best efforts to physically secure their devices used to process the Trust's data against loss, theft or use by unauthorised persons. They must secure the relevant devices whether or not in use. This includes strong passwords, encryption, physical control of the device and ensuring that the device auto-locks if inactive.

6.3. Those handling personal data within the Trust must ensure that they are using the latest software and that all devices are appropriately password protected. Passwords must not be shared with third parties. Any removable storage devices (e.g. USB sticks) must be password protected.

6.4. Those handling personal data within the Trust should install reputable anti-virus/anti-malware software and should maintain the device's original operating system and keep it current with patches and updates. They should not use a device which has been "rooted" i.e. where the manufacturer's operating system has been replaced with an alternative, as this can compromise any security measures.

6.5. Those handling personal data related to the Trust must prohibit the use of their personal ICT devises storing the Trust related personal data by anyone not authorised by the Trust, unless the other user can be prevented from gaining access to any Trust related personal data, e.g. by use of separate logins.

6.6. The Trust related personal data should not be processed from an unsecured physical environment, such as a mobile hot-spot, including free Wi-Fi.

6.7. Those handling personal data within the Trust must ensure that all Trust related personal data is securely removed from their device or protected before they dispose of it, transfer it to someone else including when selling, lending, sharing or submitting it for repair and maintenance.

6.8. In the event that any device storing Trust related personal data is lost or stolen, or where any trustee, consultant or volunteer believes that such a device may have been accessed by an unauthorised person and any Trust related personal data compromised as a result, such incident must be reported to the Chair of Trustees immediately, so that appropriate steps can be taken in a timely manner.

6.9. The Trust shall ensure that all those handling personal data within the Trust are aware of their obligations to keep personal data secure, are subject to confidentiality undertakings and undergo relevant training where required.

7. DATA SUBJECT ACCESS REQUESTS

7.1. Any request (oral or written) for confirmation if the Trust processes the requestor's personal data and for access to such data needs to be treated as a potential data subject access request. All information relating to the individual held in electronic and structured manual files should be considered for disclosure.

7.2. Any person who receives a request from an individual relating to their personal data should forward such request to the Chair of Trustees without any delay and not later than within 2 working days of receipt. The Trust is required to deal with a data subject access requests in full without delay and at the latest within one month of receipt, unless there are grounds to extend that period by further two months (see Article 15 of the UK GDPR).

7.3. The Chair of Trustees must verify the identity of an individual making the request. Where an individual appoints another person to request access to their personal data, the Chair of Trustees must be confident of the identity of the individual making the request and of the authorisation of the individual to whom the request relates.

7.4. Access to personal data may be restricted or refused in instances where an exemption under the UK GDPR or the DPA applies, for example, the relevant information is covered by legal advice privilege, sharing may place the individual at risk of significant harm or jeopardise police investigations into any alleged offence(s). The Trust must decide whether to apply any potential exemption based on the circumstances of a particular request.

7.5. A data subject access request does not need to be made in writing – oral requests may be valid but to enable the Trust to deal with them appropriately, any oral requests should be documented and the requestor should be encouraged to confirm their request in writing. The Trust may ask for any further information reasonably required to locate the requested personal data.

7.6. An individual only has the right to access their personal data, and therefore care needs to be taken not to disclose the personal data of third parties where consent has not been given and where it would not be reasonable to disclose third party's personal data (for example by applying redaction or compiling extracts of the requestor's personal data). Similarly, particular care must be taken in the case of any complaint or dispute to ensure confidentiality and/or legal privilege are protected.

7.7. All files must be reviewed and applicable exemptions under the UK GDPR and the DPA must be applied (with legal advice where appropriate) before any disclosure takes place. Access to personal data must not be granted before this review has taken place and the response is approved by the Chair of Trustees. Any response sent to the requestor must comply with the requirements of the UK GDPR and must include the information about the rights to complain to the Information Commissioner's Office (the ICO) and to bring a civil claim and all additional information required under the UK GDPR. It must be sent within a month of receipt of the request (unless this deadline is extended in accordance with the UK GDPR).

7.8. Where some data in a document needs to be redacted prior to disclosure, a copy of the full (original) document and the altered document should be retained, with the reasons for the redactions.

8. OTHER RIGHTS OF INDIVIDUALS

8.1. Other rights of individuals that the Trust needs to comply with include the right to:

8.1.1. object to processing;

8.1.2. rectification;

8.1.3. erasure; and

8.1.4. data portability.

8.2. These rights apply in certain circumstances and are not absolute. Please ensure that you follow the approach set out in this policy to ensure that the Trust's response to data subject requests is compliant with the UK GDPR and the DPA.

Right to object to processing

8.3. In certain circumstances set out in the UK GDPR (Article 21 of the UK GDPR), individuals have the right to object to the processing of their personal data, for example where they dispute the existence of lawful basis for the processing of their personal data.

8.4. Any objections received form data subjects must be sent to the Chair of Trustees without any delay and in any case within 2 working days of receipt, and the Chair of Trustees will assess whether the processing should cease or whether there are compelling legitimate grounds to continue processing which override the interests, rights and freedoms of the individual concerned, or whether the information is required for the establishment, exercise or defence of legal proceedings.

8.5. The Chair of Trustees shall be responsible for notifying the individual of the outcome of their assessment within a month of receipt of the objection (unless this deadline is extended in accordance with the UK GDPR), including informing them about their rights to complain to the ICO and to bring a civil claim.

Right to rectification

8.6. An individual has the right to request the rectification of inaccurate personal data without undue delay (Article 16 of the UK GDPR). Any request for rectification received from a data subject must be sent to the Chair of Trustees without any delay and in any case within 2 working days of receipt. Any processing of the relevant personal data should be restricted until the Trust considers the request.

8.7. Where proof of inaccuracy is given or where individuals update their personal data, the data shall be amended as soon as reasonably practicable, and the individual notified within a month of receipt of the request (unless this deadline is extended in accordance with the UK GDPR).

8.8. Where there is a dispute as to the accuracy of the data, the request and reasons for refusal should be documented and notice of refusal should be provided to the individual within a month of receipt of the request (unless there are grounds to rely on the extension of time).

8.9. Any response sent to the requestor must comply with the requirements of the UK GDPR and must include the information about rights to complain to the ICO and to bring a civil claim.

Right to erasure

8.10. Individuals have a right, in certain circumstances (set out in Article 17 of the UK GDPR), to have their personal data permanently erased without undue delay. This right arises in the following circumstances:

8.10.1. where the personal data is no longer necessary for the purpose or purposes for which it was collected and processed;

8.10.2. where consent is withdrawn and there is no other legal basis for the processing;

8.10.3. where an objection has been raised under the right to object, and found to be legitimate;

8.10.4. where personal data is being unlawfully processed; or

8.10.5. where there is a legal obligation on the Trust to delete the data.

8.11. The Chair of Trustees will make a decision regarding any request for erasure of personal data, and will balance the request against the exemptions provided for in the UK Data Protection and Privacy Laws. Where a decision is made to erase the data, and this data has been passed to other controllers, and/or has been made public, the Trust should make reasonable attempts to inform those controllers of the request.

8.12. A response must be sent to the requestor within a month of receipt of the request (unless this deadline is extended in accordance with the UK GDPR). It must comply with the requirements of the UK GDPR and must include the information about individual's rights to complain to the ICO and to bring a civil claim.

Right to restrict processing

8.13. In the following circumstances, individuals can request that processing of their personal data is restricted (Article 18 of the GDPR):

8.13.1. where the accuracy of personal data has been contested, during the period when the Trust is attempting to verify the accuracy of the data;

8.13.2. where processing has been found to be unlawful, and the individual has asked that there be a restriction on processing rather than erasure;

8.13.3. where personal data would normally be deleted, but the individual has requested that their data be kept for the purpose of the establishment, exercise or defence of a legal claim;

8.13.4. where there has been an objection to the processing, pending the outcome of any decision.

8.14. The Chair of Trustees will make a decision regarding any request. A response must be sent to the requestor within a month of receipt of the request (unless this deadline is extended in accordance with the UK GDPR). It must comply with the requirements of the UK GDPR and must include the information about individuals' rights to complain to the ICO and to bring a civil claim.

Right to portability

8.15. In certain circumstances (set out in Article 20 of the UK GDPR), if an individual wants to receive their personal data that they have provided to the Trust or to have it sent to another organisation, they have a right to request that their personal data is provided in a structured, commonly used and machine readable format. If such a request is received from a data subject, it should be forwarded to the Chair of Trustees without undue delay and in any case within 2 working days of receipt.

8.16. The Chair of Trustees will make a decision regarding any request. A response must be sent to the requestor within a month of receipt of the request (unless this deadline is extended in accordance with the UK GDPR). It must comply with the requirements of the UK GDPR and must include the information about individuals' rights to complain to the ICO and to bring a civil claim.

9. PERSONAL DATA BREACHES AND BREACHES OF THE UK DATA PROTECTION AND PRIVACY LAWS

9.1. Any identified or suspected personal data breaches (as defined in the UK GDPR) and breaches of Data Protection and Privacy Laws, shall be reported as soon as they are discovered, to the Chair of Trustees.

9.2. The Chair of Trustees shall consider any alleged breach of Data Protection and Privacy Laws and take appropriate steps.

9.3. Once notified of a personal data breach, the Chair of Trustees shall consider any alleged personal data breach and promptly assess:

9.3.1. the extent of the breach;

9.3.2. the risks to the data subjects arising out of the breach;

9.3.3. any security measures in place that will protect personal data;

9.3.4. any measures that can be taken to contain the breach and to mitigate the risk to the individuals.

9.4. If following the assessment of a breach (the ICO's breach assessment tool may be used as part of the assessment process: https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/), the Chair of Trustees concludes that the breach is likely to result in a risk to the rights and freedoms of individuals, the breach must be notified to the ICO within 72 hours from the Trust becoming aware of the breach. Any delay would need to be justified to the ICO.

9.5. A form for personal data breach reporting, published on the ICO's website (https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/) should be used to report personal data breach and the information provided to the ICO should include:

9.5.1. details of the breach, including the volume of personal data at risk, and the number and categories of data subjects;

9.5.2. the contact point for any enquiries (which should be the Chair of Trustees);

9.5.3. the likely consequences of the breach; and

9.5.4. measures proposed or already taken to address the breach.

9.6. If the breach is likely to result in a high risk to the rights and freedoms of the affected individuals the Chair of Trustees shall also notify data subjects of the breach without undue delay.

9.7. Notification to data subjects should describe in clear language the nature of the personal data breach and contain at least the following information:

9.7.1. the likely consequences of the personal data breach;

9.7.2. who to contact with any questions; and

9.7.3. measures taken or proposed to be taken to mitigate any risks and possible adverse effects of the personal data breach.

9.8. The Chair of Trustees shall be responsible for instigating an investigation into the breach, including how it happened, and whether it could have been prevented. Any recommendations for further training or a change in procedure shall be reviewed by the trustees and a decision made about implementation of those recommendations.

10. CONTACT

10.1. If anyone has any concerns or questions in relation to this policy they should contact:

The Chair of Trustees, Bill Goddard. Registered Office: c/o Stone King LLP, Boundary House, 91 Charterhouse Street, London, EC1M 6HR. Registered Charity Number: 1117330.