Data Protection Policy

The Ivors Academy Trust ("us" "we" "our")

1. Policy Statement

The privacy and data security of the people we work with is important. We enable people to be informed about and involved with The Ivors Academy Trust (hereinafter “the Trust”) through our public education and grant programmes and our communications and fundraising activities. This statement explains how we use personal data for these purposes.

Everyone has rights about the way in which their personal data is handled. During the course of our activities we will collect, store and process personal data about our beneficiaries, donors, supporters, suppliers and other third parties, and we recognise that the correct and lawful treatment of this data will maintain confidence in the organisation, thereby enabling us to carry out our charitable purpose.

2. About our policy

2.1 The types of personal data that the Trust may handle include information about current, past and prospective suppliers, grants beneficiaries, supporters, donors, and others that we communicate with (“data subjects”). The personal data, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the General Data Protection Regulation (“GDPR”).

2.2 This policy and any other documents referred to in it sets out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources.

2.3 This policy does not form part of any employee’s contract of employment and may be amended at any time.

2.4 This policy sets out rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store personal data.

2.5 The Trust Administrator is responsible for ensuring compliance with GDPR and with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Trust Administrator. See 15.1.

3. Definition Of Data Protection Terms

3.1 Data is information that is stored electronically, on a computer, or in certain paper-based filing systems.

3.2 Data subjects for the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.

3.3 Personal data is information relating to an identifiable living individual. Whenever personal data is processed, collected, recorded, stored or disposed of it must be done within the terms of the GDPR. Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

3.4 Data controllers are the people who, or organisations that, determine the purposes for which, and the manner in which, any personal data, is processed. They are responsible for establishing practices and policies in line with the GDPR. The Ivors Academy Trust is the data controller of all personal data used in our charity’s operation.

3.5 Data processors include any person or organisation that processes personal data on our behalf and on our instructions. Employees of data controllers are excluded from this definition but it could include suppliers that handle personal data on The Ivors Academy Trust’s behalf.

3.6 Processing is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

3.7 Sensitive personal data includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned.

4. Data protection principles

Anyone processing personal data must comply with the eight enforceable principles of good practice. These provide that personal data must be:

(a) Processed fairly and lawfully.

(b) Processed for limited purposes and in an appropriate way.

(c) Adequate, relevant and not excessive for the purpose.

(d) Accurate.

(e) Not kept longer than necessary for the purpose.

(f) Processed in line with data subjects' rights.

(g) Secure.

(h) Not transferred to people or organisations situated in countries without adequate protection.

5. Fair and Lawful Processing

5.1 The GDPR is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

5.2 For personal data to be processed lawfully, they must be processed on the basis of one of the legal grounds set out in the GDPR. These include, among other things, the data subject's consent to the processing, or that the processing is necessary for the performance of a contract with the data subject, for the compliance with a legal obligation to which the data controller is subject, or for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, additional conditions must be met. When processing personal data as data controllers in the course of our business, we will ensure that those requirements are met.

6. Processing for limited purposes

6.1 In the course of our work, we may collect and process the personal data set out in Schedule 1 of this policy. This may include data we receive directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and data we receive from other sources (including, for example, companies we use to deliver our charitable services such as ticket providers to our events).

6.2 We will only process personal data for the specific purposes set out in the Schedule or for any other purposes specifically permitted by the GDPR. We will notify those purposes to the data subject when we first collect the data or as soon as possible thereafter.

7. Notifying data subjects

7.1 If we collect personal data directly from data subjects, we will inform them about:

(a) The purpose or purposes for which we intend to process that personal data.

(b) The types of third parties, if any, with which we will share or to which we will disclose that personal data.

(c) The means, if any, with which data subjects can limit our use and disclosure of their personal data.

7.2 If we receive personal data about a data subject from other sources, we will provide the data subject with this information as soon as possible thereafter.

7.3 We will also inform data subjects whose personal data we process that we are the data controller with regard to that data.

8. Adequate, relevant and non-excessive processing

8.1 We will only collect personal data to the extent that it is required for the specific purpose notified to the data subject.

9. Accurate data

9.1 We will ensure that personal data we hold is accurate and kept up to date. We will check the accuracy of any personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data. Where the data subject is providing the data, for example filling out an event ticket order form, we will assume the data subject is providing accurate personal data.

10. Timely processing

10.1 We will not keep personal data longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required. Third parties who gather data on our behalf, for example event ticket providers or research companies, are also subject to the same GDPR requirements for timely processing.

11. Processing in line with data subject's rights

11.1 We will process all personal data in line with data subjects' rights, in particular their right to:

(a) Request access to any data held about them by a data controller (see also Clause 15).

(b) Prevent the processing of their data for direct-marketing purposes.

(c) Ask to have inaccurate data amended (see also Clause 9).

(d) Prevent processing that is likely to cause damage or distress to themselves or anyone else.

12. Data security

12.1 We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

12.2 We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. The Trust website is on a UK-based encrypted https server. Personal data entered using contact forms or sign-up lists on the website are stored on that encrypted server and deleted as soon as no longer needed. Personal data held by the Trust is stored on a password-protected server at the Trust's office. The data is backed-up daily and a copy made weekly to a separate hard drive kept in a fireproof safe. The only people with access to the server are the Trust Administrator, the IT manager, and The Ivors Academy Trust's CEO.

12.3 We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

(a) Confidentiality means that only people who are authorised to use the data can access it.

(b) Integrity means that personal data should be accurate and suitable for the purpose for which it is processed.

(c) Availability means that authorised users should be able to access the data if they need it for authorised purposes. Personal data is stored on one central computer drive at our address. The computer drive is held under double-lock and key and is backed up nightly. Once a week, an additional back up to hard drive is made and this drive is kept in fire proof safe.

12.4 Security procedures include:

(a) Entry controls. Any stranger seen in entry-controlled areas should be reported.

(b) Secure lockable desks and cupboards. Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)

(c) Methods of disposal. Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required.

(d) Equipment. Data users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

13. Transferring personal data to a country outside the EEA

13.1 We may transfer any personal data we hold to a country outside the European Economic Area ("EEA"), provided that one of the following conditions applies:

(a) The country to which the personal data are transferred ensures an adequate level of protection for the data subjects' rights and freedoms.

(b) The data subject has given his consent.

(c) The transfer is necessary for one of the reasons set out in the Act, including the performance of a contract between us and the data subject, or to protect the vital interests of the data subject.

(d) The transfer is legally required on important public interest grounds or for the establishment, exercise or defence of legal claims.

(e) The transfer is authorised by the relevant data protection authority where we have adduced adequate safeguards with respect to the protection of the data subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights.

13.2 Subject to the requirements in Clause 12.1 above, personal data we hold may also be processed by staff operating outside the EEA who work for us or for one of our suppliers. That staff maybe engaged in, among other things, the fulfilment of contracts with the data subject, the processing of payment details and the provision of support services.

14. Disclosure and sharing of personal information

14.1 If we are under a duty to disclose or share a data subject's personal data in order to comply with any legal obligation, or in order to enforce or apply any contract with the data subject or other agreements; or to protect our rights, property, or safety of our employees, customers, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

14.2 We may also share personal data we hold with selected third parties for the purposes set out in the Schedule.

15. Dealing with subject access requests

15.1 Data subjects must make a formal request for information we hold about them. This must be made in writing. Trustees who receive a written request should forward it to the Trust Administrator immediately.

info@ivorsacademytrust.org

020 7636 2929

15.2 When receiving telephone enquiries, we will only disclose personal data we hold on our systems if the following conditions are met:

(a) We will check the caller's identity to make sure information is only given to a person who is entitled to it.

(b) We will suggest that the caller put their request in writing if we are not sure about the caller's identity and where their identity cannot be checked.

15.3 Our employees or contractors will refer a request to the Ivors Academy Trust board of trustees for assistance in difficult situations. Employees or contractors should not be bullied into disclosing personal information.

16. Changes to this policy

16.1 We reserve the right to change this policy at any time. Where appropriate, we will notify data subjects of those changes by mail or email.

Schedule 1 – Personal Data We Collect

1. Instances where we collect personal data
There are many instances in which we may collect information about you. For example, we may collect information if you:

- Sign up to one of our grants or bursaries
- Sign up to be a Trustee of our organisation
- Attend an event we host or are involved with
- Donate to the Ivors Academy Trust via our website or other portals
- Sign up for a programme we are involved with through a partner organisation
- Subscribe to our newsletters, request information from us or join a campaign
- When you visit one of our websites or social media pages via technologies such as cookies and other online identifiers
- Make comments on our social media, or mention one of our accounts
- Apply for a job with us
- Contact us or become involved with us in any other way than as stated above.

2. Types of personal information we collect

The information we may collect from the above interactions may include, but is not limited to any of the following:

- Your name, address, telephone number, mobile number and email address, along with your preferences as to how we should contact you in the future
- Financial and credit card information which you give to us making a donation, including your gift aid status (note that we do not store credit or debit card information)
- Records of your donation history and correspondence with us
- Details of your visit to our websites, including technical information such as the IP address you use to access the website, your device, browser type and version
- We might obtain personal data about individuals who may be interested in giving major gifts to organisations like ours. In these limited cases only, in addition to information you give us directly, we may also collect information from publicly available sources about your work or interests
- Any other details in which you give us including your reasons for supporting us.

In limited and specific circumstances, we may collect special categories (sensitive personal data) of information from you.

These special categories of sensitive personal data may include:

- information about your ethnicity, sexuality, education status, socio-economic status or disability status.
- financial records for the purposes of verifying financial status,
- If we are required to do so for legal or governance reasons, a scan of your identity documents to verify your identity.

Circumstances where we would collect this information include:

- If you apply for a grant or bursary.
- If you apply for a job or Trustee position with us
- If you participate in research or feedback interviews, surveys, or focus groups.

This information will only be used for monitoring the diversity of our applicants and to ensure that our selection processes are being fairly applied or fulfilling our legal and governance duties. The

data will only be used for the stated purpose and kept no longer than is necessary for that purpose. Where possible we will collect the information on an anonymous basis so that you cannot be identified.