EMERGING VOICES GDPR POLICY

1.0 PURPOSE OF THIS DOCUMENT

This document provides high level GDPR background information. The information is required to ensure that Emerging Voices (EV) complies with GDPR requirements and forms part of the essential reading for staff and volunteers when starting with the organisation. This information should be reviewed regularly to help ensure that EV is following the correct procedures when handling personal information.

This document also contains a series of necessary GDPR policies that enables EV to function and comply with the appropriate GDPR regulations.

Finally, the document can be used as a training source for new and existing members and volunteers for the charity.

2.0 BACKGROUND AND CONTEXT

2.1 THE GDPR ACT 2018

This replaces the previous EV policy document to reflect that GDPR policy has recently been updated to reflect the minor changes that were brought in following the UK's withdrawal from the EU. UK GDPR is now covered by the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. The GDPR took effect on the 25 May 2018, across the EU and the UK. It regulates how any organisation, including charities, should handle data and is at the core of the UK's digital privacy legislation.

The legislation protects EU and UK citizens' personal data, including the data held by Emerging Voices.

GDPR applies to any personal data that EV collects and stores on EV's users, donors, employees, and volunteers.

2.2 GDPR NON-COMPLIANCE

Organisations found to be non-compliant with the GDPR risk fines of up to 4% of their income or 4 million euros, whichever is larger.

If EV had a data breach that negatively impacted on a data subject then, if the appropriate tests required it, the Information Commissioner's Office would need to be informed within 72 hours of the breach being known.

3.0 THE RIGHTS THAT PEOPLE HAVE UNDER GDPR

Under the UK GDPR, people have the right to inquire about how their personal data is being used, processed, and stored by Emerging Voices. These rights enable people to:

- Receive information on how their information is being used;
- Access their personal data;
- Update any incorrect or inaccurate personal information;
- Request erasure of any information that EV may hold on the person;
- Stop or restrict the processing of any information held on them;
- Allow them to receive or transmit their data;
- Object to how the data is processed.

4.0 THE SEVEN PRINCIPLES OF GDPR

- **Lawfulness, Fairness and Transparency** – EV must be open and honest about how it collects and processes personal data.
- **Purpose Limitation** – EV must demonstrate that personal data will only be used in the manner that is defined in its GDPR policy.
- **Integrity and Confidentiality –** EV is accountable for the protection of the personal data that it holds. The risks associated with illegal processing, loss or the damage of data, need to be assessed and documented accordingly.
- **Data Minimisation –** EV should capture the minimum of necessary data, keeping just the minimum data that allows it to operate effectively. All data should be sufficient, relevant and confined for a single purpose (it should not collect information for 'just in case' scenarios).
- **Storage Limitation –** EV should not keep personal data longer that is strictly necessary (12 months after the last action taken, after a person leaves EV).
- **Data Accuracy –** EV should take all reasonable steps to ensure that personal data is accurate and amend if necessary.
- **Accountability –** GDPR compliance is the responsibility of the organisation and EV must be able to evidence its compliance with the regulations.

5.0 GDPR - DATA CONTROLLER AND DATA PROCESSORS

As EV processes all its data internally, both the Data Controller and the Data Processor have responsibilities.

EV's data controller is responsible for GDPR compliance and must be satisfied that sufficient data protection measures are in place. GDPR applies to any personal data that EV collects and stores on EV's users, donors, employees, and volunteers.

6.0 EMERGING VOICES SPECIFIC GDPR POLICIES

6.1 The types of personal data that Emerging Voices might be required to handle include:

- information about current, past and prospective musicians (beneficiaries of Emerging Voices) and employees and others that we communicate with.

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 UK GDPR Regulation and the Data Protection Act 2018.

This policy and any other documents referred to in it sets out the basis on which we will ensure the privacy of our members and employees and how we will process any personal data we collect from individuals, or that is provided to us by individuals or other sources.

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

6.3 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.

6.4 The Data Protection Compliance Officer is responsible for ensuring compliance with the Act and with this policy. The post is held by Mike Hughes who you can contact by email via projectmanager@emergingvoicescharity.co.uk

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 Data Protection Compliance Officer Mike Hughes.

7.0 Definition of data protection terms

7.1 **Data** is information which is stored electronically, on a computer, or in certain paper-based filing systems.

7.2 **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.

7.3 **Personal data** means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). 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.

7.4 **Data controllers** are the people who or organisations which 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 regulations. Emerging Voices is the data controller for all data controlled by Emerging Voices.

7.5 **Data users** are those of our employees whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.

7.6 **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.

7.7 **Sensitive personal data** includes information about a person's:

(a) racial or ethnic origin,
(b) political opinions,
(c) religious or similar beliefs,
(d) trade union membership,
(e) physical or mental health or condition,
(f) sexual life, or
(g) about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person.

Sensitive personal data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned.

8.0 Privacy

8.1 We will endeavour to ensure the privacy of all of our musicians and employees (including volunteers and contractors). Any information which is provided to us which could reasonably be expected to be confidential will be kept confidential.

8.2 Due to the nature of the work which Emerging Voices does by participating as a musician, there is an inference that the Data Subject has experienced or is experiencing a mental health condition. Emerging Voices will be sensitive to this at all times and will only disclose information about musicians outside of the organisation with their consent (see paragraph 14 below).

9.0 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.

10.0 Fair and lawful processing

10.1 The GDPR regulations are 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.

10.2 For personal data to be processed lawfully, it must be processed on the basis of one of the legal grounds set out in the Act. 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.

10.3 When sensitive personal data is being processed, additional conditions must be met. When processing personal data, we must ensure that those requirements are met.

11.0 The purposes for which we're allowed to process data

11.1 In the course of our operations, we may collect and process the personal data. This may include data we receive directly from a Data Subject (for example, by completing an application form or by corresponding with us by post, phone, email or otherwise) and data we receive from other sources (including, for example, statutory services and partner organisations (e.g. Converge).

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

12.0 What we need to tell data subjects

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

12.1 The purpose or purposes for which we intend to process that personal data. The types of third parties, if any, with which we will share or to which we will disclose that personal data. The means, if any, by which data subjects can limit our use and disclosure of their personal data.

12.2 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.
We will also inform data subjects whose personal data we process that we are the data controller with regard to that data and who the Data Protection Compliance Officer is.

13.0 Don’t collect more data than we need

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

14.0 Make sure data is accurate

We will ensure that personal data we hold is accurate and kept up to date. We will ask Data Subjects to confirm the accuracy of any personal data that they provide us with. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

15.0 How long do we keep data?

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.

We will retain musicians’ records for twelve months after the musician stops attending Emerging Voices courses, choirs or one to one tuition and after twelve months the musician’s record will be reduced to a skeleton record.

16.0 Processing in line with data subject's rights

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

16.1 Request access to any data held about them.

16.2 Prevent the processing of their data for marketing purposes.

16.3 Ask to have inaccurate data amended.

16.4 Prevent processing that is likely to cause damage or distress to themselves or anyone else.

17.0 Data security

17.1 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.

17.2 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. Personal data will only be transferred to people outside of Emerging Voices if they agree to comply with our procedures and policies or if he/she puts in place adequate measures him/ herself.

17.3 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. However, we are aware that we are reliant on Data Subjects to update us if their personal data changes.

(c) Availability means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on the cloud.

Security procedures include:

(a) 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.)

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

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

(d) Digitally stored data. Data must be password protected and encrypted. Only appropriate Emerging Voices employees will have access to the folders in which the data is stored.

18.0 Disclosure and sharing of personal information

18.1 With the permission of the Data Subject we may disclose personal data about a Data Subject to that Data Subject's mental health support contact. In exceptional circumstances where we feel there is an imminent risk to the Data Subject or another person we may disclose personal data about a Data Subject to that Data Subject's mental health support contact without their permission.

18.2 We may also disclose personal information 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 to protect the safety of our students, employees or others.

19.0 Dealing with requests for information made by people outside of Emerging Voices

19.1 If we receive a request for information or enquiry about a Data Subject from a person outside of Emerging Voices then we must deal with it as follows:

(a) If the request or enquiry is from a mental health support worker or other health or social care worker then we can confirm that the Data Subject is an Emerging Voices musician but we must not give any other information without the Data Subject's consent. We must not meet with the support worker without the consent and participation of the Data Subject;

(b) If the request or enquiry is from a relative of the Data Subject then we should not give any information about the Data Subject without the consent of the Data Subject. This means we cannot confirm that the Data Subject is an Emerging Voices musician or give any information about their attendance or progress.

20.0 Dealing with subject access requests

20.1 Data subjects must make a formal request for information we hold about them. We do not require them to pay a fee to do this.

20.2 Any subject access request should be made in writing if possible. Once the request is received, it should be forwarded to the Data Protection Compliance Officer immediately.

20.3 When receiving subject access requests by telephone, 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 that information is only given to a person who is entitled to it.

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

Our employees, volunteers and contractors will refer a request to the Data Protection Compliance Officer for assistance in difficult situations.

21.0 Data storage location and Microsoft 365

The charity uses a cloud based server to securely store and back up all files.

Microsoft 365 is used by the charity and configured to support UK GDPR compliance.

22.0 Changes to this policy

We reserve the right to change this policy at any time in line with changes to changes in GDPR UK regulations and associated laws. Any changes will be reflected in amendments to this document.

23.0 Policy publication and review dates

Version 2	March 2025
Version 3	June 2026

The policy shall be reviewed and updated as necessary every 2 years.