Data Protection Policy

This policy describes to staff our policies regarding personal data and what all staff need to do when dealing with personal data. Remember that personal data is any information about a person, or any information from which a person could be identified, so that includes obvious things such as their name, contact details and mobile phone number, but also details of their physical and mental condition, their background, and details of meetings, their location, and any other information that describes them or their activities.

Personal data needs to be stored and used securely, and in accordance with legal restrictions. This policy sets out how we at The Music Works make sure that happens.

Board Champion	Alexander Ross
Data Protection Lead	Jessica Fairclough
Data Protection Administrator	Ben O'Sullivan
Last Reviewed	January 2023
Next Review Date	January 2025

1. Our policy

The Music Works delivers lots of different programmes and we need to collect, store and use personal data (including information, photographs and videos) of the people we work with. We do this in order to be sure:

- that we are delivering the right things to the right people in a way that helps them
- that we can share, celebrate and evidence the impact of our work and the work of the people we support.

Some of this data might be 'special category' personal data, for example about an individual's ethnicity or religion or mental health status (see appendix 1 for a full list of what is classified as special category personal data). We may also sometimes need to pass on data to other organisations for specific purposes, for example if we're working

as part of an NHS programme. This data may also include information about our audiences, participants, staff or other organisations that we work with.

This policy sets out how we make sure we are protecting our team members' data and the data of the people we work with by meeting all relevant laws and guidelines.

1.1 The General Data Protection Regulation

Under the Data Protection Act 2018 the UK incorporated the European General Data Protection Regulation ('GDPR') into UK law, and we at The Music Works have a legal responsibility to ensure that all individuals' data is handled lawfully, fairly and in a transparent manner and in accordance with the GDPR. Individuals are sometimes called 'data subjects' when talking about data protection law.

We can only collect and use personal data when we have a lawful basis for doing so. The GDPR sets out the six lawful bases on which data may be collected, used and held. These are:

- Consent (when a data subject gives consent)
- Contract (in order to be able to enter into or deliver on a contract with someone)
- Legal obligation (where the law requires it)
- Vital interests (to protect someone's life)
- Public task (to perform a task in the public interest or for official functions)
- Legitimate interests (for example when we need certain information to deliver a session or a programme safely and to maximise outcomes), unless there is a good reason to protect the individual's personal data which overrides those legitimate interests

In addition to the above, where we are using special category personal data, we must also meet one or more of these additional criteria:

- The person has given explicit consent for us to process their special category personal data
- Vital interests - the use is necessary to protect someone's life
- It is necessary for us to collect and hold this data so that we can comply with employment law
- It is necessary for monitoring equality of opportunity and is carried out with appropriate safeguards for the rights of individuals

The GDPR also sets out rules for how we collect and hold data. It must be:

- Collected for specific, clear and legitimate purposes and only used in the ways which were specified when the data was originally collected
- Relevant and limited only to the data that we need
- Accurate as far as is reasonable and kept up to date where required
- Only kept for as long as is necessary and securely destroyed afterwards
- Processed securely

2. Responsibilities and procedures

2.1 Responsibilities

- The lead member of staff for data protection is the operations manager but all staff are responsible for delivering the policy. The data protection lead (DPL) will have overall responsibility to ensure that our policy is up to date and being delivered across the organisation. They will set staff access levels. They will also liaise with the board champion for data protection and the other trustees where necessary.
- The marketing and communications team are responsible for ensuring the marketing elements of this policy are delivered.

- The data protection administrators are responsible for recording different access levels for staff, ensuring this policy is being delivered across any systems we use (such as Upshot, M365 and IT hardware), and removing password access when staff or freelancers leave the organisation or no longer need access due to a role change.

2.2 Procedures

2.2.1 Staff induction and training:

We will:

- Explain this data protection policy and our data protection notice on induction and provide more detailed training if relevant to a particular role
- Explain our policy to any volunteers that may be collecting or handling data, for example evaluation forms
- Provide core staff training every three years
- Keep up to date on legislation through the DPL and provide briefings when there are significant updates or changes to legislation
- Include data protection on board agendas when relevant

2.2.2 Third party contracts and data sharing agreements

GDPR compliance will be demonstrated through contracts and data sharing agreements with all team members and third parties where relevant, for example having specific data protection clauses included in contracts with external companies.

If a team member or third party does not adhere to these contracts and data sharing agreements the DPL will look into it and try to resolve any issues. If this isn't possible, then we may have to start disciplinary procedures with the team member or terminate the third party contract.

2.2.3 Access

The Music Works DPL will assess what personal data any team members need to have access to. We use SharePoint and Upshot to store data digitally, and team members will only have access to the data they need. All special category will be kept secure and can only be accessed if the DPL requests so. Access will automatically be withdrawn if a team member leaves the organisation. The data protection administrator is responsible for this.

2.2.4 Participant data

The DPL will:

- ensure participants' personal data is only processed with their consent, except where another lawful basis of use applies
- ensure participants' personal data is only shared with staff members on a need-to-know basis, for example medical information

ensure all team members are briefed regarding their data protection responsibilities regardless of how short their contract is **2.2.4 Staff data**

The DPL will

- ensure all staff have a private personnel file, only accessible to SLT
- ensure a record of all personal work-related documents are kept in private personnel files

2.2.5 Operations

The DPL will:

- ensure audits, staff training and briefings are regularly carried out
- ensure IT policies are in place and compliant and staff are briefed on their content
- ensure IT software and hardware is audited and offers sufficiently robust security

- ensure suitable procedures are in place for responding to data breaches, subject access requests and requests for the right to be forgotten (or other such requests) and to support staff in responding to such requests
- ensure all hard copies of data are kept in the office filing cabinet before they are uploaded online before being shredded

2.2.6 All team members must:

- ensure personal data is updated as soon as inaccuracies are discovered, for example if you receive an email bounce back
- ensure unnecessary duplicates of personal data are not created, for example multiple versions of a mailing list
- use strong passwords and password protect files and password protect access to computers that contain personal data
- when using the *to* or *cc* field in email ensure that it is either reasonable to expect all recipients on the email to know each other or to reasonably expect their data to be shared. If this is in doubt use the BCC field.
- Ensure any hard copies of personal data are never left out on view
- Ensure any devices are not left on and open in shared spaces

2.2.7 Storing personal data securely

- All personal data on paper will be stored in the office filing cabinet before being inputted digitally, scanned and uploaded online
- Once personal data has been uploaded online, it will be shredded
- If external data drives or memory sticks are used for storing data they will be encrypted
- Computer access passwords must be strong, not shared outside of the organisation and changed regularly

- Where personal data is stored on a cloud-based system or network, restrictions on access and use of passwords will apply
- All login details and passwords for accounts that access systems that process personal data must be administered by the DPL and available to the senior management team
- You must only use third-party processors, which includes cloud-based systems, where this has been audited and agreed
- Any devices (owned by staff or owned by TMW) that are used to access personal data must be encrypted. You do this by:
    - **Mac**: Using the fire-vault. This is already enabled by default. Instructions on how to enable it here: https://www.youtube.com/watch?v=hFUpCE6-8Ro
    - **Windows**: Encrypt all TMW related folders by using 'properties'. Instructions on how to enable it here: https://www.youtube.com/watch?v=Y0pN0rN8MEM
    - We reserve the right to check your device if we feel it's necessary, however we will always respect all private information in doing so.

2.2.8 Transferring data to third parties securely

Where it is necessary to transfer personal data all team members and third parties must adhere to their information sharing agreements specifying:

- what information will be exchanged with third parties
- the purposes for which it will be used
- how it will be protected and safely handled and stored
- retention periods and disposal/destruction methods

All transfers of personal data must be authorised by the DPL who has been designated this authorisation level, and should only contain information that is absolutely necessary.

All referral forms shared outside of the organisation must be encrypted during electronic sharing using *Egress data security services*.

Transfers must not be made to countries not approved by the Information Commissioner's Office (ICO) unless under a contract that complies with the ICO requirements.

2.3 Reviewing

2.3.1 New programmes or new technology:

We will carry out a Data Protection Impact Assessment (DPIA) if and when new forms of personal data are collected *or* if we start using new technology. The DPIA will check compliance with this policy by listing:

- What personal data we intend to process
- Why we intend to process it
- How we have communicated this information to those whose data we're collecting
- Whether any special category personal data is involved (see appendix)
- A confirmation that this is the minimum data required to complete the task
- How we intend to keep the data securely
- How long we intend to hold the data for
- How we intend to check the data for accuracy and keep it up to date
- How consent will be given (if applicable) and where this is recorded
- How people can easily withdraw their consent, for example by unsubscribing or emailing us to say they no longer wish their image to be used in photograph or video.
- Whether, taking into account the above information, the proposed processing carries a risk for data subjects, and if so how that risk can be reduced
- Any other actions required

2.3.2 Third-party processors

We will also carry out an audit of any third-party processors which details:

- the type of personal data shared
- the reason for sharing it
- confirm that it will be transferred securely using *Egress data security services*.
- how we know the processor complies with data protection law with reference to their policies.

We will also check that the processor does not transfer personal data outside the UK and if so that their data protection is at least equal to that of companies inside the UK and how data subjects are informed of this.

After each audit the DPL will develop an action plan and work with all relevant staff to make any changes needed.

2.4 Data Destruction

All personal data must only be retained for as long as is necessary. SharePoint will detail all personal data that is currently stored with expected dates for when it will no longer be necessary to keep the data. The project will be maintained and managed by the data protection administrator and reviewed in line with this policy by DPL. When this requirement has passed, all personal data must be destroyed securely and absolutely.

2.5 Breaches

In the event of a security breach, the DPL must be informed immediately.

Depending on the circumstances of the breach action will include:

- completing an incident report
- taking action to address the cause of the breach
- taking action to minimise the damage that may be caused by the breach
- possible disciplinary action

If the breach is likely to result in a risk to people's rights and freedoms, for example discrimination, damage to reputation or financial loss, it must be reported to the ICO within 72 hours. If the breach is likely to result in a high risk to people's rights and freedoms, they must also be told about the breach without undue delay. The DPL will make these reports when necessary and also report to the CEO and trustee data protection champion.

A breach may also need to be reported to the Charities Commission as a serious incident that has been reported to a third-party regulator.

If a member of staff realises that they have been processing data in a way not compatible with this policy, or not for the purpose for which it was originally collected, they must also inform the DPL as soon as possible so a plan of action can be agreed.

2.6 Individual rights

Individuals can withdraw their consent to their personal data being held and used at any time. They can also request to restrict data use, for example that we can use their data to send them information about one type of activity but not another. They should also be able to quickly and easily request that the data we hold about them is updated and any corrections made.

In instances where consent was actively given and used as the legal basis for data collection and use, it must be easy to withdraw consent and this must be acted on immediately.

Individuals also have the right to be forgotten, which means all personal data held about them must be deleted, and the right to data portability, which means we as an organisation must provide their data in a format which is then suitable to be transferred to another organisation, or that we do that transfer for them.

If the personal data is being held/used for any other purposes or reasons, for example, due to a legal obligation, then we may reject certain requests by individuals. The DPL will decide if we are able to do this.

Individuals can also submit a subject access request, in which case we must provide details all of the personal data we hold on that individual. This will be done free of

charge and within one month of the request. We can extend this period by a further two months where requests are complex or numerous. If this is the case, we will tell the individual making the request within one month of getting the request and explain the reasons why.

If a request is refused we will respond within one month to explain the reasons for this decision and tell the individual of their right to complain to a supervisory authority or take legal action.

Data protection lead (DPL) contact details:

If you want to speak to the data protection lead (DPL), here are her contact details:

Jessica Fairclough

jfairclough@themusicworks.org.uk; 01452 923 951

In the event that you are unable to contact Jess, please contact Ben O'Sullivan:

bosullivan@themusicworks.org.uk ; 01452 923 953

Registration

The Music Works is registered with ICO – the Information Commissioner's Office.

Registration Number ZA796732.

This registration is reviewed in line with ICO recommendations annually by data protection lead and renewed for the 15th October each year.

APPENDIX 1

There is stronger legal protection for special category personal data, which is:

- personal data revealing racial or ethnic origin;
- personal data revealing political opinions;
- personal data revealing religious or philosophical beliefs;
- personal data revealing trade union membership;
- genetic data;
- biometric data (where used for identification purposes);
- data concerning health;
- data concerning a person's sex life; and
- data concerning a person's sexual orientation.

There are separate safeguards for personal data relating to criminal convictions and offences.