West Sussex Music Trust

Data Protection Policy

Compliant with GDPR, effective 25 May 2018

Version:	2
Date:	1 September 2020
Review date:	1 September 2022
Author:	James Underwood, Chief Executive, West Sussex Music Trust
Responsible Trustee:	Chairman of West Sussex Music Trust

Purpose of the policy

West Sussex Music Trust (the Trust) is committed to complying with privacy and data protection laws including:

1. The General Data Protection Regulation ("**the GDPR**") and any related legislation which applies in the UK, including, without limitation, any legislation derived from the Data Protection Bill 2017;
2. The Privacy and Electronic Communications Regulations (2003) and any successor or related legislation, including without limitation, E-Privacy Regulation 2017/0003; and
3. All other applicable laws and regulations relating to the processing of personal data and privacy, including statutory instruments and, where applicable, the guidance and codes of practice issued by the Information Commissioner's Office ("ICO) or any other supervisory authority

   (together "**the Legislation**")

This policy sets out what we do to protect individuals' personal data.

Anyone who handles personal data in any way on behalf of the Trust must ensure that we comply with this policy. The 'definitions' section of this policy describes what comes within the definition of 'personal data'. Any breach of this policy will be taken seriously and may result in disciplinary action or more serious sanctions.

This policy may be amended from time to time to reflect any changes in legislation, regulatory guidance or internal policy decisions.

About this policy

The types of personal data that we may handle include, without limitation, details of pupils, parents, employees, candidates, contractors, suppliers and partners.

James Underwood is Chief Executive of the Trust and is responsible for ensuring compliance with GDPR. The Senior Leadership Team is responsible for day to day data protection matters and will be responsible for ensuring that all members of staff and relevant individuals abide by this policy.

Definitions

Business purposes	The purposes for which personal data may be used by us: Personnel, administrative, financial, regulatory, payroll and business development purposes. *Business purposes include the following but not limited to:* - *Compliance with our legal, regulatory and corporate governance obligations and good practice* - *Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests* - *Ensuring business policies are adhered to (such as policies covering email and internet use)* - *Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of commercially sensitive information, security vetting, credit scoring and checking* - *Investigating complaints* - *Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments* - *Monitoring staff conduct, disciplinary matters* - *Marketing our business* - *Improving services*
Data subjects	All living individuals about whom we hold personal data, for instance, an employee or a pupil. A data subject need not be a UK resident or UK national. All data subjects have legal rights in relation to their personal data
Personal data	'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. *Personal data we gather may include: individuals' phone number, address, email address, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV.*
Special categories of personal data	Special categories of data include information about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings, and genetic and biometric information — any use of special categories of personal data should be strictly controlled in accordance with this policy.

Data controller	'Data controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by law.
Data processor	'Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Processing	'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Supervisory authority	This is the national body responsible for data protection. The supervisory authority for our organisation is the Information Commissioners Office.

Scope

This policy applies to all staff, who must be familiar with this policy and comply with its terms.

This policy supplements our other policies relating to the "Acceptable use of IT". We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.

Data Controller

The Trust is classified as a data controller. We must maintain our appropriate registration with the Information Commissioners Office (ICO) in order to continue lawfully controlling data.

Our ICO registration reference is ZA026335.

As data controller, we must exercise overall control over the purpose for which, and the manner in which, personal data are processed.

The Principles

The Trust shall comply with the principles of data protection (the Principles) enumerated in the EU General Data Protection Regulation. We will make every effort possible in everything we do to comply with these principles in respect of any personal data that we deal with as a data controller.

The Principles are:

1st Principle: Lawful, fair and transparent

Data collection must be fair, for a legal purpose and we must be open and transparent as to how the data will be used.

2nd Principle: Limited for its purpose

Data can only be collected for a specific purpose and not further processed in a way which is incompatible with those purposes.

3rd Principle: Data minimisation

Any data collected must be adequate, relevant and limited to what is necessary for the purpose for which it is held.

4th Principle: Accurate

The data we hold must be accurate and kept up to date.

5th Principle: Retention

We cannot store data longer than necessary.

6th Principle: Integrity and confidentiality

The data we hold must be kept safe and secure.

Our procedures

1st Principle: Fair and lawful processing

We must process personal data fairly and lawfully in accordance with individuals' rights under the first Principle. This generally means that we should not process personal data unless the individual whose details we are processing has consented

to this happening and is processed for the purposes that the data subject has been told about.

If we cannot apply a lawful basis (explained below), our processing does not conform to the first principle and will be unlawful. Data subjects have the right to have any data unlawfully processed erased

Lawful basis for processing data

There must be a lawful basis for processing data. Ensure that any data you are responsible for managing has a written lawful basis. It is your responsibility to check the lawful basis for any data you are working with and ensure all of your actions comply the lawful basis. At least one of the following conditions must apply whenever we process personal data:

1. **Consent**
   We hold recent, clear, explicit, and defined consent for the individual's data to be processed for a specific purpose.

2. **Contract**
   The processing is necessary to fulfil or prepare a contract for the individual.

3. **Legal obligation**
   We have a legal obligation to process the data (excluding a contract).

4. **Vital interests**
   Processing the data is necessary to protect a person's life or in a medical situation.

5. **Public function**
   Processing necessary to carry out a public function, a task of public interest or the function has a clear basis in law.

6. **Legitimate interest**
   The processing is necessary for our legitimate interests. This condition does not apply if there is a good reason to protect the individual's personal data which overrides the legitimate interest.

Deciding which condition to rely on

To make an assessment of the lawful basis, it must first be established that the processing is necessary. This means the processing must be a targeted, appropriate way of achieving the stated purpose. A lawful basis cannot be relied upon if it is reasonable achieve the same purpose by some other means.

More than one basis may apply, and what will best fit the purpose should be relied upon, not what is easiest.

The following factors should be considered:

- What is the purpose for processing the data?

- Can it reasonably be done in a different way?
- Is there a choice as to whether or not to process the data?
- Who does the processing benefit?
- After selecting the lawful basis, is this the same as the lawful basis the data subject would expect?
- What is the impact of the processing on the individual?
- Are you in a position of power over them?
- Are they a vulnerable person/child?
- Would they be likely to object to the processing?
- Are you able to stop the processing at any time on request, and have you factored in how to do this?

It must be ensured that individuals whose data is being processed by us are informed of the lawful basis for processing their data, as well as the intended purpose. This occurs via the Trust's privacy notice. This applies whether we have collected the data directly from the individual, or from another source.

Special categories of personal data

Previously known as sensitive personal data, this means data about an individual which is more sensitive, so requires more protection. This type of data could create more significant risks to a person's fundamental rights and freedoms, for example by putting them at risk of unlawful discrimination. The special categories include information about an individual's:

- race
- ethnic origin
- politics
- religion
- trade union membership
- genetics
- biometrics (where used for ID purposes)
- health
- sexual orientation

In most cases where we process special categories of personal data we will require the data subject's *explicit* consent to do this unless exceptional circumstances apply or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

The condition for processing special categories of personal data must comply with the law. If there is no lawful basis for processing special categories of data that processing activity must cease.

2nd Principle: Limited for its purpose

This requires that personal data is only processed for the explicit, specific and legitimate purposes that the individual was told about when their information was first obtained.
This means that we shall not collect personal data for one purpose and then use it for another. If it becomes necessary to process a person's information for a new purpose, the individual should be informed of the new purpose beforehand. For example, if we collect personal data such as a contact number or email address, in

order to update a person about our activities it should not then be used for a new purpose.

3rd Principle: Data minimisation

Any data collected must be adequate, relevant and limited to what is necessary for the purpose for which it is held. Data should be limited to what is necessary in relation for the purposes for which it was collected.

4th Principle: Accurate

Inaccurate or out of date data should be destroyed securely, and we must take every reasonable step to ensure that personal data which is inaccurate is corrected.

5th Principle: Data retention

We must retain personal data for no longer than we need for the purpose it was collected for. This means that personal data that we hold should be destroyed or erased from our systems when it is no longer needed.

6th Principle: Data security

You must keep personal data secure against loss or misuse.

We are required to put in place procedures to keep personal data we hold secure, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage using appropriate measures.

Storing data securely

- In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it
- Printed data should be shredded when it is no longer needed
- Data stored on a computer should be protected by strong passwords that are changed regularly. We encourage all staff to use a password manager to create and store their passwords.
- Data stored on CDs or memory sticks must be encrypted or password protected and locked away securely when they are not being used
- The Trust must approve any cloud used to store data
- Servers containing personal data must be kept in a secure location, away from general office space
- Data should be regularly backed up in line with the company's backup procedures
- Data should never be saved directly to mobile devices such as laptops, tablets or smartphones
- All servers containing sensitive data must be approved and protected by security software
- All possible technical measures must be put in place to keep data secure

Transferring data internationally

There are restrictions on international transfers of personal data. You must not transfer personal data abroad, or anywhere else outside of normal rules and procedures without express permission from the Trust.

Rights of individuals

Individuals have rights to their data which we must respect and comply with to the best of our ability. We must ensure individuals can exercise their rights in the following ways:

1. Right to be informed

- Providing privacy notices which are concise, transparent, intelligible and easily accessible, free of charge, that are written in clear and plain language, particularly if aimed at children.
- Keeping a record of how we use personal data to demonstrate compliance with the need for accountability and transparency.

2. Right of access

- Enabling individuals to access their personal data and supplementary information
- Allowing individuals to be aware of and verify the lawfulness of the processing activities

3. Right to rectification

- We must rectify or amend the personal data of the individual if requested because it is inaccurate or incomplete.
- This must be done without delay, and no later than one month. This can be extended to two months with permission from the Trust.

4. Right to erasure

- Individuals have the right to have all personal data erased (the right to be forgotten) unless certain limited conditions apply.
- We must delete or remove an individual's data if requested and there is no compelling reason for its continued processing.

5. Right to restrict processing

- We must comply with any request to restrict, block, or otherwise suppress the processing of personal data.
- We are permitted to store personal data if it has been restricted, but not process it further. We must retain enough data to ensure the right to restriction is respected in the future.

6. Right to data portability

- We must provide individuals with their data so that they can reuse it for their own purposes or across different services.

- We must provide it in a commonly used, machine-readable format, and send it directly to another controller if requested.

7. Right to object

- We must respect the right of an individual to object to data processing based on legitimate interest or the performance of a public interest task.
- We must respect the right of an individual to object to direct marketing, including profiling.
- We must respect the right of an individual to object to processing their data for scientific and historical research and statistics.

8. Rights in relation to automated decision making and profiling

- We must respect the rights of individuals in relation to automated decision making and profiling.
- Individuals retain their right to object to such automated processing, have the rationale explained to them, and request human intervention.

Additional information regarding the rights of individuals

1. Data portability requests

We must provide the data requested in a structured, commonly used and machine-readable format. This would normally be a CSV file, although other formats are acceptable. We must provide this data either to the individual who has requested it, or to the data controller they have requested it be sent to. This must be done free of charge and without delay and no later than one month. This can be extended to two months for complex or numerous requests, but the individual must be informed of the extension within one month and you must receive express permission from the Chief Executive first.

2. Right to erasure

What is the right to erasure?

Individuals have a right to have their data erased and for processing to cease in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected and / or processed
- Where consent is withdrawn
- Where the individual objects to processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed or otherwise breached data protection laws
- To comply with a legal obligation
- The processing relates to a child

How we deal with the right to erasure

We can only refuse to comply with a right to erasure in the following circumstances:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The exercise or defence of legal claims

If personal data that needs to be erased has been passed onto other parties or recipients, they must be contacted and informed of their obligation to erase the data. If the individual asks, we must inform them of those recipients.

3. The right to object

Individuals have the right to object to their data being used on grounds relating to their particular situation. We must cease processing unless:

- We have legitimate grounds for processing which override the interests, rights and freedoms of the individual.
- The processing relates to the establishment, exercise or defence of legal claims.

We must always inform the individual of their right to object at the first point of communication, i.e. in the privacy notice. We must offer a way for individuals to object online.

4. The right to restrict automated profiling or decision making

We may only carry out automated profiling or decision making that has a legal or similarly significant effect on an individual in the following circumstances:

- It is necessary for the entry into or performance of a contract.
- Based on the individual's explicit consent.
- Otherwise authorised by law.

In these circumstances, we must:

- Give individuals detailed information about the automated processing.
- Offer simple ways for them to request human intervention or challenge any decision about them.
- Carry out regular checks and user testing, to ensure our systems are working as intended.

Subject Access Requests

What is a subject access request?

An individual has the right to receive confirmation that their data is being processed, access to their personal data and supplementary information which means the information which should be provided in a privacy notice.

How we deal with subject access requests

We must provide an individual with a copy of the information in the request, free of charge. This must occur without delay, and within one month of receipt. We endeavour to provide data subjects access to their information in commonly used electronic formats, and where possible, provide direct access to the information through a remote accessed secure system.

If complying with the request is complex or numerous, the deadline can be extended by two months, but the individual must be informed within one month. Only the Chief Executive can extend the deadline.

We can refuse to respond to certain requests, and can, in circumstances of the request being manifestly unfounded or excessive, charge a fee. If the request is for a large quantity of data, we can request the individual specify the information they are requesting. This can only be done with express permission from the Chief Executive.

Once a subject access request has been made, you must not change or amend any of the data that has been requested. Doing so is a criminal offence.

Third parties - using third party controllers and processors

As a data controller, we must have written contracts in place with any third party data processors that we use. The contract must contain specific clauses which set out our and their liabilities, obligations and responsibilities.

As a data controller, we must only appoint processors who can provide sufficient guarantees under GDPR and that the rights of data subjects will be respected and protected.

Criminal offence data - criminal record checks

Any criminal record checks are justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject. We cannot keep a comprehensive register of criminal offence data. All data relating to criminal offences is considered to be a special category of personal data and must be treated as such. You must have approval from the Chief Executive prior to carrying out a criminal record check.

Contracts

Our contracts must comply with the standards set out by the ICO and, where possible, follow the standard contractual clauses which are available. Our contracts with data processors must set out the subject matter and duration of the processing, the nature and stated purpose of the processing activities, the types of personal data and categories of data subject, and the obligations and rights of the controller.

At a minimum, our contracts must include terms that specify:

- Acting only on written instructions
- Those involved in processing the data are subject to a duty of confidence
- Appropriate measures will be taken to ensure the security of the processing
- Sub-processors will only be engaged with the prior consent of the controller and under a written contract
- The controller will assist the processor in dealing with subject access requests and allowing data subjects to exercise their rights under GDPR
- The processor will assist the controller in meeting its GDPR obligations in relation to the security of processing, notification of data breaches and implementation of Data Protection Impact Assessments
- Delete or return all personal data at the end of the contract
- Submit to regular audits and inspections, and provide whatever information necessary for the controller and processor to meet their legal obligations.
- Nothing will be done by either the controller or processor to infringe on GDPR.

Audits, monitoring and training

Data audits

Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

Monitoring

Everyone must observe this policy. You must notify the Chief Executive of any breaches of this policy. You must comply with this policy fully and at all times.

Responsibilities

Our responsibilities

- Analysing and documenting the type of personal data we hold
- Checking procedures to ensure they cover all the rights of the individual
- Identify the lawful basis for processing data
- Ensuring consent procedures are lawful
- Implementing and reviewing procedures to detect, report and investigate personal data breaches
- Store data in safe and secure ways

- Assess the risk that could be posed to individual rights and freedoms should data be compromised
- Keeping the board updated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures and policies on a regular basis
- Arranging data protection training and advice for all staff members and those included in this policy
- Answering questions on data protection from staff, board members and other stakeholders
- Responding to individuals such as clients and employees who wish to know which data is being held on them by us
- Checking and approving with third parties that handle the company's data any contracts or agreement regarding data processing

Your responsibilities

- Fully understand your data protection obligations
- Check that any data processing activities you are dealing with comply with our policy and are justified
- Do not use data in any unlawful way
- Do not store data incorrectly, be careless with it or otherwise cause us to breach data protection laws and our policies through your actions
- Comply with this policy at all times
- Raise any concerns, notify any breaches or errors, and report anything suspicious or contradictory to this policy or our legal obligations without delay.

Training

You will receive adequate training on provisions of data protection law specific for your role. You must complete all training as requested.

Reporting breaches

Any breach of this policy or of data protection laws must be reported as soon as practically possible. This means as soon as you have become aware of a breach. The Trust has a legal obligation to report any data breaches to ICO within 72 hours.

All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the ICO of any compliance failures that are material either in their own right or as part of a pattern of failures

Any member of staff who fails to notify of a breach, or is found to have known or suspected a breach has occurred but has not followed the correct reporting procedures will be liable to disciplinary action.

Failure to comply

We take compliance with this policy very seriously. Failure to comply puts both you and the organisation at risk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures which may result in dismissal.

If you have any questions or concerns about anything in this policy, do not hesitate to contact a member of SLT.

Monitoring and review

The Trust will keep this policy under review and amend or change it as required.

++

I confirm that it is my responsibility to read, understand and comply with this policy.

Employee signature:

Print name:

Date: