



## **Emily Tully Music General Data Protection Regulation Policy**

### **WHAT IS THE GENERAL DATA PROTECTION REGULATION (GDPR)?**

The General Data Protection (GDPR) comes into force on 25 May 2018 and seeks to evolve the existing principles within the Data Protection Directive by tightening laws specific to the governance of personal data (the Data Protection Act 1998 ('DPA 1998') being the most relevant). Examples include, but are not limited to:

- An introduction of burden upon businesses to be able to demonstrate compliance (the “accountability principle”).
- A stricter approach to those who simply rely on consent as a basis for processing personal data.
- More severe penalties for non-compliance.

Emily Tully Music is a Data Controller but is not a Data Processor. As such, Emily Tully Music has a number of further obligations in terms of responsibility and also procedures in place to facilitate third-parties/clients (who are Data Controllers) in their own compliance.

This guide sets out the aspects of GDPR which are relevant to Emily Tully Music and how compliance will be, or is already, ensured for data stored both physically and digitally.

### **GENERAL DEFINITIONS**

- Personal data – Information relating to a living individual.
- Personal Identifiable Information (PII) – Any data that could potentially identify a specific individual.
- Data subject – the person about whom the data relates.
- Data subject access request – the right of an individual to request a copy of their data under a formal process and payment of a fee.
- Data controller – an organisation or body which uses personal data.
- Data processor – an organisation or body which determines the purposes for which and the manner in which any personal data are, or are to be, processed.
- Processing of personal data – storage, transfer, viewing, access, analysis of personal data.

April 2023

- Notification – a formal process of notifying the Information Commissioner’s Office (ICO) by an organisation of the use of personal data.
- Sensitive personal data – data relating to religious or other beliefs, sexual orientation, health, race, ethnicity, political views, trades union membership, criminal record.

### **EXISTING PRINCIPLES OF THE DPA 1998**

Before GDPR can be considered, it is important to be reminded of the DPA 1998 and specifically the 8 principles for best practice in handling personal data:

1. Personal data must be processed fairly and lawfully.
2. Personal data shall only be used in accordance with the purposes for which it was collected.
3. Personal data must be adequate, relevant and not excessive. Do not collect data just in case it might be useful.
4. Personal data must be accurate and where necessary kept up to date.
5. Personal data must be kept for no longer than is necessary.
6. Personal data must be processed in accordance with the rights of data subjects.
7. Appropriate technical and organisational measures must be established to protect the data.
8. Personal data must not be transferred outside the EEA unless adequate provisions are in place for its protection.

### **AWARENESS**

Emily Tully Music is aware of GDPR and the likely ramification of the ‘strengthening’ of the rules in relation to data protection.

Emily Tully Music has performed integration of revised policies and procedures, to establish GDPR compliance within both Emily Tully Music as an educational entity.

### **AN AUDIT AND REGISTER OF INFORMATION HELD**

As an education supplier, Emily Tully Music represent students and pupils. As such, most personal information held concerns being able to contact students and parents of students in order to provide a service. A small proportion of the personal data hosted by Emily Tully Music, however, is of employees.

Data is stored digitally in three primary locations:

- On a password protected laptop with password protected files.
- On My Music Staff – an online system for booking lessons and storing data.
- On a password protected Mailchimp account for clear newsletter structures.
- On a mobile phone that is password protected.

April 2023

Physical data can be stored at Emily Tully Music sites, in secured and locked cupboards.

Data Stored on a password protected website called Mailchimp who provide a 'guaranteed service' in relation to data security. See - <https://mailchimp.com/legal/privacy/>

Data Stored on a password protected website called My Music Staff who provide a 'guaranteed service' in relation to data security. See - <https://www.mymusicstaff.com/privacy-policy/>

Personal data may be accessed for administrative purposes by Chris Guy who resides at the address, as he occasionally has to support Emily Tully Music and the daily running of the business. Chris Guy is a Solicitor with an up to date and annual DBS check with the Solicitors Regulation Authority.

Personal data can be accessed by teachers who work alongside Emily Tully Music for contact purposes. All teachers are DBS checked and hold their own public liability and professional indemnity insurance.

## PRIVACY NOTICES

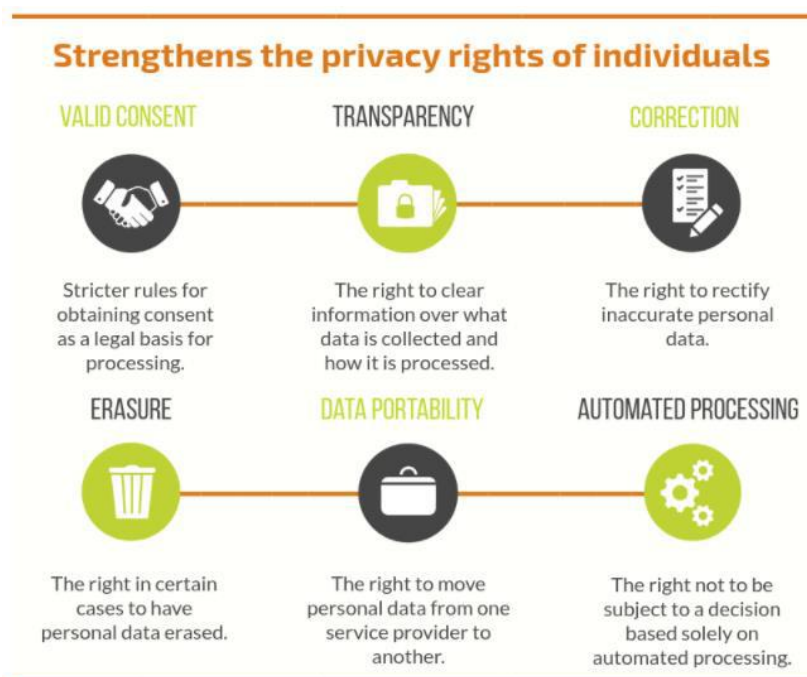
Personal data must be processed in a transparent manner under Article 5 GDPR. Privacy notices are the main way we comply with this obligation.

All of our new pupil forms provide notices which require acknowledgement before data can be processed.

Appendix 1 contains information given to staff to inform staff about how/where their personal data is stored and in what instances it can be used.

## INDIVIDUAL RIGHTS

The following infographic notes the 'strengthening' of privacy rights in relation to individuals.



## Collection of User Data

Data about pupils and staff is collected via new staff of new pupil forms. Pupils and staff are asked to complete the forms with their details which explains how they will be contacted and why Emily Tully Music requires their data in order for lessons to run smoothly.

## Valid Consent

In short, "default positive opt-ins" are no longer permitted. Instead, the ICO states that genuine consent is only obtained with a "very clear and specific statement". Often though consent is not needed and instead a different lawful basis for processing data can be chosen.

Emily Tully Music process data by having a legitimate interest. More information can be found below.

## **SUBJECT ACCESS REQUESTS (SARS)**

A SAR, also known as a 'subject access', is a request from an individual for information including:

- Whether any personal data is being processed.
- A description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people.
- A copy of the information comprising the data; and given details of the source of the data (where this is available).

There are 4 key types of SAR, all of which must be completed within 1 month as illustrated in the infographic on page 6 of this guide:

- 'Transparency Request'.
- Portability Request.
- Erasure Request.
- Correction Request.

### 'Transparency Request'

Every individual has a right to transparency, a requirement set out in GDPR Article 5.2: "A data controller must be able to demonstrate that personal data are processed in a transparent manner in relation to the data subject."

Appendix 2 summarises the information which is supplied by Emily Tully Music to any individual requesting what data is collected and how it is processed.

### Data Portability

The right to data portability refers to allowing individuals to obtain and reuse their personal data for their own purposes across different services.

The right to data portability only applies:

- To personal data an individual provided to a controller.
- Where the processing is based on the individual's consent or for the performance of a contract; and
- When processing is carried out by automated means.

This can then be supplied to the subject via appropriate means by directly inputting the information into the below organisation's online systems. Their online systems possess their own GDPR policies.

The only time data of pupils may need to be shared with external organisations is:

- Mailchimp- for newsletter production

- Sounds of Intent- to record musical progress of those with learning difficulties.
- Exam boards such as ABRSM and Trinity- so pupils can take their exams.

## Erasure Request

Also known as a 'right to be forgotten', an individual can request all relative data can be destroyed without delay if one of the following applies:

- The controller doesn't need the data anymore
- The subject withdraws consent for processing with which they previously agreed to (and the controller doesn't need to legally keep it)
- The subject uses their right to object (Article 21) to the data processing
- The control and / or its processor is processing the data unlawfully
- There is a legal requirement for the data to be erased
- The data subject was a child at the time of collection
- If a controller makes the data public, then they are obligated to take reasonable steps to get other processors to erase the data

In the event of an erasure request at Emily Tully Music, all information related to the pupil and/or their parent will be erased from all electronic systems and any paper copies will be destroyed.

- Any information on Mailchimp will be removed.
- A request will be sent to Sounds of Intent to have the pupil removed from Emily Tully account.
- The exam boards will be notified but pupils may have to contact them directly, as it may have an effect on the pupil's grades and qualification status.

Where Emily Tully Music has a legal or regulatory basis to retain records, such as where it is prudent to maintain records for six years, the erasure request will be refused.

Emily Tully Music performs all accepted erasure requests within 14-days, erasing all appropriate data identified across all digital storage platforms (phone, laptop, online systems).

## Correction Request

Individuals are entitled to have personal data rectified if it is inaccurate or incomplete.

If we have disclosed the personal data in question to others, each recipient to which the inaccurate data was disclosed to must be contacted and informed of the rectification.

The process for administering requests for correction is as below (subject to the initial request providing suitable identification proof). A pupil must fill out a new student form with all the changes highlighted for clarity for the data administrator. This will require the pupil to repeat their consent for marketing purposes

## Automated Processing

Emily Tully Music's does not perform calculations or analysis on pupil or client details or personal information.

## **LAWFUL BASIS FOR PROCESSING PERSONAL DATA**

GDPR Article 6(1) lists six legal grounds for processing personal data. For completeness, they are:

- a) the data subject has given consent to the processing of their personal data for one or more specific purposes;
- b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- c) processing is necessary for compliance with a legal obligation to which the controller is subject;
- d) processing is necessary in order to protect the vital interests of the data subject;
- e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- f) processing is necessary for the purposes of the legitimate interests pursued by a controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks.

At Emily Tully Music, we control and process data whilst fulfilling our requirements to provide music and singing lessons to pupils. As such we have a legitimate interest for processing the data in order to contact and bill students with regards to the lessons.

## **CHILDREN**

GDPR enforces a particular protection of children because of their lack of awareness of the risks involved.

Emily Tully Music is aware of the data risks to children generally but, as all information is processed and data protected in the same manner (regardless of age), no material change in process is required.

## CCTV

Emily Tully Music has a doorbell installed on the house that films and records motion on the drive, on the garden and at the door.

The principal purposes of the CCTV system are as follows:

- for the prevention, reduction, detection and investigation of crime and other incidents;
- to ensure the safety of staff, students and visitors.
- to enable teachers to know when pupils have arrived.

The CCTV system will be used to observe Emily Tully Music drive in order to identify incidents requiring a response. The CCTV is operated in a manner that is consistent with respect for the individual's privacy.

### Monitoring and Recording

Cameras can be monitored on two Phones which are both password protected belonging to Emily Tully and Chris Guy.

Images are recorded to a secure online cloud and can only be viewed by the holders of the phones. Images are deleted after 30 days of being recorded.

The cameras installed provide images of suitable quality for the specified purposes for which they are installed and all cameras are checked regularly to ensure images remain fit for purpose and the date and time stamp recorded on images is accurate.

All images recorded by the CCTV System remain the property and copyright of Emily Tully Music.



## DATA BREACHES

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Examples:

- Access by an unauthorised third party;
- Deliberate or accidental action (or inaction) by a controller or processor;
- Sending personal data to an incorrect recipient;
- Computing devices containing personal data being lost or stolen;
- Alteration of personal data without permission; and
- Loss of availability of personal data.



## Prevention and Detection of Breaches

Emily Tully Music takes a proactive approach towards preventing data breaches but, should the worst happen and one occurs, the procedures in place to detect these help facilitate a timely and managed response.

To prevent digital breaches occurring, Emily Tully Music restricts access to its data from outside of the constraints by protecting documents and electronic devices with passwords only known to Emily Tully.

## Notification of breach(es)

Breaches – both confirmed and potential – must be notified to the ICO within 72 hours after “becoming aware”.

The following must be included within any breach notification:

- A description of the nature of the personal data breach including, where possible. The categories and approximate number of individuals concerned; and
- The categories and approximate number of personal data records concerned.
- The name and contact details of the data controller

April 2023

- A description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

Breach notifications are typically processed by Emily Tully once all of the above has been obtained, collated and discussed (where necessary).

In certain instances, the notification of Breach will be sent to the individual(s) concerned. An example of which would be where the breach has caused a risk of identity fraud.

## **DATA PROTECTION BY DESIGN AND DEFAULT**

Emily Tully Music has made technical and organisational changes to ensure that from this point forward, all new projects or changes to existing projects, policies and procedures are all in line with the GDPR.

This includes:

- The need for personal data to be collated with ease in order to comply with SARs.
- The need for procedures to facilitate the requirements of us, as the Data Controller, to satisfy the portability requirements of the GDPR
- To ensure that not just current but future third-party suppliers and vendors are also GDPR compliant.

To ensure that `Data Protection by Design and Default` is an organisation-wide policy, understood and performed by all staff, regular reviews of organisational change are performed to check for full compliance.

Furthermore, annual training is provided to all members of staff to provide them a refresher of the regulatory requirements but also any changes in procedures from previous training sessions.

## ADDITIONAL MEASURES

Modified Data Protection Risk Assessments (repeated annually or earlier if necessary)

Each answer to the following assessment requires a clear note of where within Emily Tully Music directory the information can be found. The risk assessment (see Appendix 3) below is repeated annually or if / when any breach is reported.


### Training

In order to train staff in relation to GDPR, Emily Tully Music will remind staff of the procedures in place and their need to read the GDPR policy.

- What is personal data, and sensitive personal data?
- The sanctions if you breach data protection rights.
- Your core obligations, including the new accountability principle.
- Practical scenarios on the things that arise in educational practice, such as issues with disclosure and due diligence, your duty to redact information, risks with paper files, and marketing.
- “Subject access requests” including how they can be used on behalf of pupils.
- Data security issues.

To supplement the above, Emily Tully Music have developed our own training modules specifically in relation to Data Protection / GDPR.

## DOCUMENT CONTROL

DOCUMENT VERSION	DATE	VERSION CONTROLLED & APPROVE BY (Name & Signature)
V1.0	April 2023	Emily Tully 

## **APPENDIX 1 – PRIVACY NOTICE TO STAFF**

### **Data Protection**

This notice describes how we collect and use personal data about you both during and after your working relationship with us. It applies to everyone who works for us, including employees and contractors.

What information may we hold about you?

We may collect and use a wide range of personal data about you such as the following:

- Your contact details such as name, address, telephone number and email address.
- Your date of birth.
- Your gender.
- Emergency contact information.
- Financial information including your National Insurance number, bank account details, salary and payroll records, tax, pension and benefits information.
- The dates and location of your employment and annual leave.
- Employment records (including job titles, work history, working hours, training records and professional memberships).
- Information about your performance, including performance reviews, and disciplinary and grievance information.
- Information about your use of our information and communications systems.
- Photographs.

We will only collect and use sensitive personal data (for example about your race or ethnicity, religious beliefs, sexual orientation and political opinions, trade union membership, health and sickness records) with your explicit consent or if that is necessary for prescribed purposes laid down by law.

How do we use personal data about you?

- We only use your personal data when the law allows, for example:
  - For the purposes of your contract of employment or other contract we have with you.
  - To comply with a legal obligation.
  - Where it is necessary for our legitimate interests or those of a third party and your interests and fundamental rights do not override those interests.
  - With your consent.

We will only use your personal data for the purposes for which we collected it, unless we consider that we need to use it for another reason and that reason is compatible with the original purpose.

April 2023

If we hold sensitive personal data about you (e.g. health records) we will only use that information for proper purposes allowed by law, for example:

- We may use information about leaves of absence, including sickness absence or family related leaves, to comply with our legal obligations.
- We may use information about your health or disability status to ensure your health and safety in the workplace, to assess your fitness to work, to provide appropriate adjustments, to monitor and manage sickness absence and related purposes.
- We may use information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation, for equal opportunity monitoring and reporting.

Will we share information about you with anyone?

We take your privacy seriously. We will never sell your personal data to anyone, and we take precautions to keep it secure.

It will sometimes be necessary for us to pass on information to third parties. For example:

- We have legal obligations to pass on to government agencies certain information, such as tax and National Insurance information.
- We may need to pass on information to service providers, such as payroll service providers, pension providers and our legal advisers.
- We may be audited or checked by third parties in some circumstances, which may enable them to see some information about you.
- If we were in the future considering a merger or sale of our business information might have to be disclosed to the other party to the transaction, or their advisers, as part of the due diligence process.

Such third parties are required to maintain confidentiality in relation to your information.

Your rights

You have a right of access under data protection law to the personal data that we hold about you. We seek to keep that personal data correct and up to date. You should let us know if you believe the information we hold about you needs to be corrected or updated.

**APPENDIX 2 – INFORMATION REQUEST SUMMARY REQUEST**

<b>What information must be supplied?</b>	<b>Data obtained directly from data subject (e.g. Emily Tully Music employees)</b>
Businesses contact details of Emily Tully Music	Yes
Purpose of the processing and the lawful basis for the processing	Yes
The legitimate interests of the controller or third party, where applicable	Yes
Categories of personal data	No
Any recipient or categories of recipients of the personal data	Yes
Retention period or criteria used to determine the retention period	Yes
The existence of each of data subject’s rights	Yes
The right to withdraw consent at any time, where relevant	Yes
The right to lodge a complaint with a supervisory authority	Yes
The source the personal data originates from and whether it came from publicly accessible sources	No
Whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data	Yes
The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences	Yes
When should information be provided?	At the time the data is obtained

**APPENDIX 3 - RISK ASSESSMENT TEMPLATE**

ISSUE	YES / NO?
<p><b>Back up:</b> Is information appropriately backed up? This includes electronic information being backed up on an external hard drive, and copies of important paper documents being made and kept separate from originals.</p>	Yes
<p><b>Retention:</b> Do we keep information for appropriate times? Do we have clear time limits for retention of records? Do we safely dispose of confidential information when those time limits expire? For example,</p> <ul style="list-style-type: none"> <li>• Are documents shredded rather than being placed intact in the refuse?</li> <li>• Are electronic devices thoroughly cleared of information before they are disposed of?</li> </ul>	Yes
<p><b>Security of Electronic Records:</b> Do we have effective safeguards against hacking, malware, phishing and other cybercrime. For example:</p> <ul style="list-style-type: none"> <li>• Do we have a firewall?</li> <li>• Do we have up-to-date anti-virus software?</li> <li>• Do we install software upgrades promptly?</li> <li>• Do our systems have suitable password protection?</li> <li>• Are passwords managed effectively? In particular do we ensure passwords are of sufficient complexity and changed from time to time?</li> <li>• Do our staff understand the risks and their responsibilities in respect of information security?</li> <li>• Do staff understand the importance of reporting any breach security?</li> </ul>	Yes
<p><b>Security of Paper-Based Records:</b> Do we have appropriate security arrangements to protect paper-based records? For example:</p> <ul style="list-style-type: none"> <li>• Are paper files well organised to minimise the risk of documents being lost?</li> <li>• Is access to our premises appropriately controlled?</li> <li>• Do we give staff clear guidelines about the risks involved in taking confidential papers out of the office e.g. to home or offsite visits?</li> </ul>	Yes
<p><b>Collecting Personal Data:</b> Do we only collect and process personal data when we have a lawful basis for doing so?</p>	Yes
<p><b>Transparency:</b> Do we use appropriate privacy notices or other means where practicable to let people know the use we make of personal data we hold about them?</p>	Yes
<p><b>Training:</b> Overall, are staff adequately trained so that they understand their obligations under the GDPR in respect of data protection, confidentiality, security and reporting of breaches?</p>	Yes
<p><b>Third Parties:</b> Have we considered the risks associated with us sending personal data and confidential information to third parties? Is it adequate in all the circumstances for us to rely on the general data protection and confidentiality obligations of those third parties? Otherwise, have we taken appropriate precautions? This may include the following:</p> <ul style="list-style-type: none"> <li>• Checking they have appropriate data protection procedures in place, including adequate security arrangements.</li> <li>• Requiring them to agree to contractual terms</li> </ul>	Yes
<p><b>Marketing:</b> Do we ensure we do not send marketing communications without opt-in consent where that is necessary?</p>	Yes