APPENDIX – HUB PARTNERSHIP AGREEMENTS
CHESHIRE WEST AND WIRRAL

GUIDANCE FOR SCHOOLS AND PROVIDERS

INTRODUCTION

As lead organisation of the Cheshire and Wirral music hub, the Love Music Trust has a responsibility to support all state schools in the borough to deliver the aims and objectives of the National Plan for Music Education: The Power of Music to Change Lives (NPME2). To do this effectively, the Trust receives an annual grant from the Department for Education via Arts Council England, who monitor the work and activity of the Trust. The NPME2 sets out three aims and five strategic functions (pages 48-49 of NPME2) which encompass delivery in and beyond schools.

We continue to define music delivery in schools by these four roles:

1. First Access *(sometimes referred to as Whole Class Instrumental/Ensemble Teaching or Wider Opportunities)*
2. Ensembles
3. Progression
4. Singing

The Love Music Trust's agreed approach for First Access and Progression is to make grants available to all primary schools on an annual basis.

WHAT IS A 'HUB PARTNERSHIP AGREEMENT'?

All schools receiving support from the Trust are deemed to be partners of the Music Hub in Cheshire and Wirral. Where this involves financial support, we are required to formalise this through the creation of a hub partnership agreement. In real terms, for schools, this means that:

- The school is demonstrating its commitment to providing high quality music education.
- The school agrees to abide by the parameters of the funding laid out in this document.

The school agrees that the grant-supported First Access and Progression teaching which takes place in school will be subject to a quality assurance process. The exact nature of this is still to be confirmed but schools will be notified in due course.

WHAT IS 'FIRST ACCESS'?

First Access is Whole Class Ensemble Teaching. This is defined in NPME2 as 'A programme of teaching on musical instruments delivered to a whole class, learning and playing together.'

To be eligible for a First Access Grant from the Trust, a project must:

- give all children in at least one year group the opportunity to learn a musical instrument.
- give children the practical use of their own musical instrument for the duration of each session.
- run for a minimum of ten consecutive weeks (notwithstanding staff illness, school closures, trips etc.) in sessions which are a minimum of 40 minutes in duration.

WHAT IS 'PROGRESSION'?

Progression is where pupils have the opportunity to progress their musical education after the original First Access programme, such as in a smaller group developing their practice on the same or a different instrument.

The Progression Grant must:

- support pupils who have previously participated in a First Access programme to continue to learn an instrument.
- be spent on provision which the school provides itself or purchases from an independent tutor or an external provider; it cannot be claimed where parents/carers make payment directly to a third party.

Here are some examples of how schools have chosen to apply their Progression Grant:

- Small group / individual tuition.
- Instrument hire for pupils continuing into small group / individual lessons.
- A school ensemble, as long as the group is musically accessible to pupils who have completed a First Access programme.
- A First Access programme which is delivered to two (or more) year groups. This is particularly helpful for smaller schools (with smaller budgets) who have mixed year group classes as they can effectively 'pool' the First Access and Progression Grants. It cannot, however, be claimed for a First Access programme which is delivered to the same year group for two or more terms.

We are happy to consider all proposals that genuinely support as many children as possible to carry on with their instrumental learning. If you are unsure whether your proposed programme meets the eligibility criteria, please speak to a member of the Love Music Trust.

WHO WILL DELIVER THE TUITION?

Where a school accesses music hub funding for First Access and Progression tuition, they are the commissioner of services.

CONDITIONS OF GRANT FUNDING

1. You (the school) are responsible for ensuring that you undertake safer recruitment and right to work checks for any tutors engaged through programmes delivered with grant funding.
2. Where schools enter in to a grant funding agreement, it is understood that this constitutes the school working as a partner of the Cheshire and Wirral Music Hub.
3. Your school agrees that copy invoices / statements will be provided to finance@lovemusictrust.com to show that the total grant given has not exceeded the amount spent by a school. This will need to be done before grant funding is released.
4. Your school will agree to engage in a process of Quality Assurance for the tuition covered by one or both of these grants. More information about this will be available in due course.
5. By accepting the grant and engaging a tutor you acknowledge that the conduct and actions of the tutor are not the responsibility of the Love Music Trust. The Love Music Trust has no direction or control over the tutors within the directory
6. It is the responsibility of the tutor and the school to establish and agree the teaching timetable
7. As above, the tutor is free to negotiate their hourly rate directly with the school
8. Grants are paid to schools if:
    - The specific parameters contained within this document are adhered to.
    - The project(s) have commenced (e.g. a grant for a one-term project in the Summer Term will only be paid in the Summer term).
    - The tutor delivering your First Access programme has received a quality assurance visit.

DATA PROCESSING AGREEMENT

FOR HUB PARTNERSHIP AGREEMENTS

BACKGROUND

A. The Controller uses the services of the Processor to provide musical education and the assessment associated with such education to its pupils (the "Service").
B. The terms of the Agreement, as amended by this Addendum, are to apply to all data processing carried out for the Controller by the Processor and to all personal data held by the Processor in relation to such processing.
C. From 25 May 2018 onwards, agreements between controllers and processors must comply with the requirements of the GDPR (as defined in clause 1) and any relevant domestic legislation, including the Data Protection Act 2018.

1. Interpretation

"controller", "processor", "personal data" and "processing"	shall have the meanings given to them in the GDPR;
"school"	the school or academy named in this document;
"data subjects"	means the individuals whose personal data is processed by the Processor on behalf of the Controller pursuant to the terms of the Agreement;
"EEA"	European Economic Area;
"GDPR"	means the General Data Protection Regulation (EU) 2016/679;
"Data Privacy Laws"	means: either the GDPR; the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended) and any superseding legislation; and all other applicable laws and regulations relating to the processing of personal data and/or governing individuals' rights to privacy, including (but not limited to) the Data Protection Act 2018 and statutory instruments.

IT IS HEREBY AGREED as follows:

2. Variation

2.1. In consideration of the sum of £1 (receipt of which the Processor hereby acknowledges), the Parties agree that this Addendum shall be incorporated into the Agreement and shall become binding on the Parties.
2.2. Except as set out in section 2.3 below, the Agreement and its terms shall continue in full force and effect.
2.3. To the extent there is any conflict between any term of the Agreement and any term of this Addendum, the terms of the Addendum shall prevail.

3. **Specific Processing**

3.1. The details of the specific processing are set out in Schedule 1.

4. **Processor obligations**

4.1. The Processor shall process personal data received from or processed on behalf of the Controller in connection with the Service (the "**Protected Data**") only on the documented instructions of the Controller. These may be specific instructions or instructions of a general nature as set out or provided for in the Agreement. For the avoidance of doubt, this does not prevent the Processor processing Protected Data where required under applicable EU or UK law and, in such circumstances, the Processor shall notify the Controller of that legal requirement unless applicable law prohibits such notification on important public interest grounds.
4.2. The Processor shall inform the Controller immediately if, in its opinion, an instruction issued in accordance with section 4.1 would result in either the Controller or the Processor breaching the Data Privacy Laws.
4.3. All Protected Data shall be treated as strictly confidential by the Processor and may not be copied, disclosed or processed in any way (i) without the express authority of the Controller or (ii) unless required by law or any relevant regulatory body.
4.4. The Processor warrants that all individuals who it authorises to process Protected Data on behalf of the Controller, including employees, are obliged to protect the confidentiality of such Protected Data.
4.5. The Processor warrants that it, and its employees and agents, will comply at all times with the Data Privacy Laws and shall not perform its/their obligations under the Agreement (as amended by this Addendum or otherwise) in such a way as to cause the Controller to breach any of its obligations under the Data Privacy Laws.
4.6. Where the Processor processes Protected Data (whether stored in the form of physical or electronic records) on behalf of the Controller it shall:
4.6.1. process Protected Data only to the extent, and in such a manner, as is necessary in order to comply with its obligations under the Agreement (as amended by this Addendum or otherwise);
4.6.2. implement appropriate technical and organisational measures to protect the Protected Data against unauthorised or unlawful processing and against accidental loss, destruction, damage, alteration or disclosure in compliance with obligations set out in the Data Privacy Laws, including, where appropriate:
(a) the pseudonymisation and encryption of Protected Data;
(b) ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services;
(c) restoring the availability and access to Protected Data in the event of a physical or technical incident; and
(d) regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring security of the processing;
1.1.1. in furtherance of its obligations in section 4.6.2, implement and maintain as a minimum the security measures set out in Parts I and 2 of Schedule 2 to this Addendum;
1.1.2. if so requested by the Controller, within a reasonable timeframe supply details of the technical and organisational measures in place to safeguard the Protected Data, and otherwise make available to the Controller all information necessary to demonstrate

compliance with the obligations set out in the Agreement, whether amended by this Addendum or otherwise, and/or the Data Privacy Laws;

1.1.3. on reasonable prior notice, permit persons authorised by the Controller to enter into any premises on which Protected Data is processed on behalf of the Controller and to inspect the Processor's systems to ensure that sufficient security measures are in place (noting that, without prejudice to the Agreement as modified by this Addendum or otherwise, this clause will survive the termination of the Agreement);

1.1.4. not process or transfer Protected Data outside the EEA without the prior written consent of the Controller and, where the Controller consents to any such transfer, the Processor shall put in place measures to ensure the Protected Data remains adequately protected as required under the Data Privacy Laws (in addition to any relevant obligations placed on a processor under the Data Privacy Laws); and

1.1.5. not transfer or disclose any Protected Data to any third party or sub-contract any processing function without verifying that the sub-contractor can provide sufficient guarantees to protect the Protected Data and without the prior written consent of the Controller (and for the avoidance of doubt, not to add or replace any sub-contractor without the Controller's consent) and ensure that any third party to which it sub-contracts any processing has entered into a written contract with the Processor which contains all the obligations that are contained in this Agreement, as amended by this Addendum; permits both the Processor and the Controller to enforce those obligations; is governed by UK law and automatically terminates upon termination of this Agreement as amended by this Addendum.

1.1.6. For the avoidance of doubt, the Processor remains fully liable to the Controller for the performance of the obligations of any sub-contractor appointed by the Processor to assist with the performance of the Services under the Agreement.

2. **Complaints and rights of data subjects**

2.1. The Processor shall ensure that it protects the rights of data subjects under the Data Privacy Laws and shall:

2.1.1. promptly notify the Controller in writing (within at least two working days) if it receives:

(a) a request from a data subject to have access to his or her Protected Data or to exercise any of his or her rights under Articles 15-22 GDPR; or

(b) a complaint or request relating to the Controller's obligations under the Data Privacy Laws; and

2.1.2. provide the Controller with full co-operation and assistance in relation to any such complaint or request made, including by:

(a) promptly providing the Controller with full details of any complaint or request and any additional information requested by the Controller;

(b) taking all steps necessary to enable the Controller to comply with a request from a data subject within the relevant timescale set out in the Data Privacy Laws and in accordance with the Controller's reasonable instructions;

(c) providing the Controller with any Protected Data it holds in relation to a data subject (within the timescales required by the Controller);

(d) using appropriate technical and organisational measures as far as this is possible, to assist the Controller to respond to requests from data subjects to exercise their rights; and

(e) ensuring that (other than as set out above) no reply or other communication is made in response to such complaint or request unless approved by the Controller.

3. **Notification of Data Security Breaches**

3.1. A "**Data security Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Protected Data. This includes breaches that are the result of both accidental and deliberate causes.

3.2. The Processor shall notify the Controller without undue delay after any Data Security Breach occurs and in any event no later than 12 (twelve) hours after the Data Security Breach has occurred, and shall include in that notification a full description of:

3.2.1. the nature of the Data Security Breach including details of the Protected Data and data subjects affected;

3.2.2. the likely consequences of the Data Security Breach; and

3.2.3. the measures taken or proposed to be taken by the Processor to address the Data Security Breach, including, where appropriate, measures to mitigate its possible adverse effects.

3.3. The Processor shall provide reasonable assistance to the Controller in the event that the Controller is required to notify affected data subjects.

4. **Data protection impact assessments / consultations with the ICO**

4.1. The Processor shall provide reasonable assistance to the Controller with any data protection impact assessments and prior consultations with the ICO which the Controller reasonably considers to be required by the Data Privacy Laws, in each case solely in relation to Protected Data processed pursuant to this Agreement and taking into account the nature of the relevant processing activity and information available to the Processor.

5. **Duration of processing**

5.1. The Processor shall process the Protected Data as required under the Agreement in accordance with this Addendum until the sooner of:

5.1.1. the Agreement, as amended by this Addendum, terminating for any reason; or

5.1.2. the Controller reasonably requesting (orally or in writing) that the Processor stops processing the Protected Data.

5.2. The Processor agrees that, on termination or expiration of this Agreement or in the event that it is notified by the Controller that it is not required or permitted to process any further Protected Data, the Processor shall:

5.2.1. transfer a copy of all Protected Data held by it in relation to this Agreement to the Controller in a format reasonably requested by the Controller;

5.2.2. and/or, at the Controller's request, and unless legally required to retain the information, the Processor shall destroy all such Protected Data (including back ups and copies) using a secure method which ensures that it cannot be accessed by any third party and shall provide the Controller with a written confirmation of secure disposal.

Schedule 1
Specific Processing Details

The subject-matter of this processing is set out in the Hub Partnership Agreement and this Appendix. The duration of this processing is the term set out in the Agreement. The nature and purpose of this processing is to:

- Support student learning;
- Protect student welfare and meet our legal obligations relating to child protection and safeguarding;
- Manage applications for financial support;
- Carry out research;
- Comply with contractual / regulatory obligations e.g. reporting to the Arts Council;
- Help achieve the Trust's charitable aims: to offer a broad music education curriculum to all pupils in Cheshire and Wirral which as a minimum fulfils the requirements of the NPME; to provide opportunities for music tutors to grow and develop their skills and therefore deliver ever better activities; to encourage "joined up" progression through pupils' musical development up to and including the most prestigious National levels; to encourage prominent "role model" musicians to work with Cheshire and Wirral pupils; to support and encourage appropriate breadth and depth of ensembles; to encourage as many primary schools as possible to engage with the first musical step of "Wider Opportunities"; to identify and support emerging talent; to encourage greater involvement at all levels in singing, including to the highest levels; to apply the best of new thinking to all of musical education, including the increasing use of digital technologies.

The types of Protected Data processed in furtherance of the Agreement are school teachers.

Schedule 2
Security Schedule

Part 1
Standard of Security Measures to be adopted by the Processor

1. The Processor will ensure that in respect of all Protected Data it receives from or processes on behalf of the Controller it maintains security measures to a standard appropriate to:
   1.1. the risk to the rights and freedoms of the data subjects that might result from unlawful or unauthorised processing or accidental loss, alteration, disclosure, damage or destruction of the Protected Data; and
   1.2. the nature of the Protected Data.
2. The Processor will maintain data security by protecting the confidentiality, integrity, availability and resilience of the Protected Data, where:
   (a) "confidentiality" means that only individuals who are authorised to use the Protected Data can access it;
   (b) "integrity" means that the Protected Data should be accurate and suitable for the purpose for which it is processed;
   (c) "availability" means that the Protected Data should be available to be accessed and used when required; and
   (d) "resilience" means that the systems processing Protected Data should be able to withstand threats and attacks.
3. In particular the Processor shall:
   3.1. have in place and comply with a security policy which:
      3.1.1. defines security needs based on a risk assessment;
      3.1.2. allocates responsibility for implementing the policy to a specific individual; or
      3.1.3. is provided to the Controller on or before the commencement of this Agreement or on request;
      3.1.4. is disseminated to all relevant staff; and
      3.1.5. provides a mechanism for feedback and review.
   3.2. ensure that appropriate security safeguards and virus protection are in place to protect the hardware and software which is used in processing the personal data in accordance with best industry practice;
   3.3. prevent unauthorised access to the Protected Data;
   3.4. ensure its storage of Protected Data conforms with best industry practice such that the media on which Protected Data is recorded (including paper records and records stored electronically) are stored in secure locations and access by personnel to Protected Data is monitored and controlled;
   3.5. have secure methods in place for the transfer of Protected Data whether in physical form (for instance, by using couriers rather than post) or electronic form (for instance, by using encryption or pseudonymisation);
   3.6. put password protection on computer systems on which Protected Data is stored and ensure that only authorised personnel are given details of the password;
   3.7. take reasonable steps to ensure the reliability of any employees or other individuals who have access to the Protected Data; members of staff;
   3.8. ensure that any employees or other individuals required to access the Protected Data are informed of the confidential nature of the Protected Data and comply with the obligations set out in the Agreement as amended by this Addendum;
   3.9. ensure that none of the employees or other individuals who have access to the Protected Data publish, disclose any of the Protected Data to any third party unless directed in writing to do so by the Controller;
   3.10. have in place methods for detecting and dealing with breaches of security (including loss, damage or destruction of Protected Data) including having a proper procedure in place for investigating and remedying breaches of the data protection principles contained in the Data Privacy Laws;

3.11. providing the Controller with all assistance reasonably required to allow the Controller to notify the ICO and/or a data subject of a data security breach where the Controller determines that it is required under the Data Privacy Laws;
3.12. have a secure procedure for backing up and storing back-ups separately from originals;
3.13. have an appropriate system in place to ensure that access to the Protected Data can be restored in a timely manner in the event of any physical or technical incident;
3.14. implement an effective system of regularly testing, assessing and evaluating the effectiveness of the measures used to ensure the security of the processing carried out under the Agreement as amended by this Addendum; and
3.15. have a secure method of disposal for unwanted Protected Data including for back-ups, disks, print outs and redundant equipment.

Part 2
Description of Security Measures to be implemented by Processor

The Trust has substantial security measures and policies in place which detail that:

- Data must not be transferred from the LMT network on to a portable memory device or disc;
- Staff and contractors must 'lock' their computer when away from their desk;
- Staff and contractors must ensure that the use of personal devices conforms to the points noted above;
- Staff and contractors shall not knowingly introduce malicious software into company computers;
- Any unsolicited email (spam) should be deleted unopened;
- Staff and contractors shall not open files of unknown origin on any machine attached to the network.
- Incoming memory sticks or optical disks must be scanned for viruses before they are read.
- Be especially aware of the potential dangers of email attachments and malicious websites.
- Any member of Staff and contractors who suspects that his/her workstation has been infected by a virus shall immediately power off the workstation and seek further advice from colleagues as appropriate.
- Staff and contractors should not perform any equipment installations, disconnections, modifications, or relocations without sufficient experience and expertise.
- Disks/memory sticks should be stored out of sight when not in use. If they contain highly sensitive or confidential data, they must be encrypted or locked away.
- Personal laptops, tablets and smartphones may only be used to access data if they have antivirus software installed (and regular – i.e. weekly – scans are undertaken) and can be 'locked' by a fingerprint or passcode known only to the contractor when not in use. It is suggested that individual 'logins' are set up when using a personal laptop.
- It is only acceptable to access LMT data through an app (i.e. Google Drive app, Gmail app, iOS mail app) if the contractor is the only person who uses or is able to access that device, or if it is possible to password protect access to the app in question.
- If a staff member or contractor's personal device can be accessed by another person (i.e. a family member), then the contractor must log in via google.com (with 'password saving' disabled) to access the data they need. The staff member or contractor must ensure that they log out upon completion.
- In all circumstances, devices must be 'locked' when not in use.

Where it is legally required, or necessary for the reasonable undertaking of our business activities (and it complies with data protection law) we may share personal information with:

- Financial organisations (e.g. GoCardless, Xero, Stripe) - to enable payment processing and debt collection;
- Suppliers and service providers (e.g. SpeedAdmin, G Suite, Sound Advice, Sandbach School, Current RMS) – to enable them to provide the service we have contracted them for;
- Central government (e.g. the Department for Education, Arts Council England, the Charity Commission) – to meet the obligations of our hub funding agreement;
- Local government (e.g. Cheshire East Council, Cheshire West and Chester Council, Wirral Borough Council) - to meet our legal obligations to share certain information with it, such as safeguarding concerns;
- Our auditors (e.g. WR Partners) – to meet our legal obligation as a business and registered charity to be regularly audited;
- Health and social welfare organisations;
- Professional advisers and consultants;
- Police forces, courts, tribunals;

Where data sharing and third-party processing is undertaken on a contractual basis, the Trust has ensured that a Data Protection Agreement that is at least comparable to this agreement in its detail and scope is in place between it and the third party processor.