

EDULINCS

GENERAL TERMS AND CONDITIONS 2025/2026

Schedule 1: Lincolnshire Music Service

Please complete the detail below and return to musicservice@lincolnshire.gov.uk

Name	
Job Title	
Signature	
Date	

PART 1: SERVICE SPECIFIC CONDITIONS

Lincolnshire Music Service will seek to apply all relevant charges for requested services to the School SpeedAdmin dashboard under 'charges'. Schools can constantly monitor and view charges up until the dates set out in section 1.7 below, at which point LCC will seek to invoice the school for this termly amount.

1.1 Lincolnshire Music Service Instrument Lesson and Instrument Hire Terms and Conditions

This Agreement sets out the legal terms and conditions on which we, Lincolnshire County Council ("LCC") through our in-house team the Lincolnshire Music Service ("LMS"), provide music lessons and instrument hire. LMS will work with schools in Lincolnshire, and parents/legal guardians/carers to facilitate this Agreement.

In requesting a music lesson and hiring instruments from LMS, you agree to be bound by our terms and conditions.

Service	Charge
Instrumental and Vocal Lessons (Block Booking Model Direct to Schools)	£51.30 per hour
Instrumental and Vocal Lessons (Direct to Families)	Individual 15 mins - £10.65 Individual 20 mins - £14.00 Individual 30 mins - £21.10 Shared 20 mins - £7.10 Shared 30 mins - £10.65 Group 30 mins - £6.70
Instrument Hire	£19.00 per instrument per term (3 per year)

1.2 Other services

Lincolnshire Music Service also delivers the following services direct to schools:

Service	Charge
Lincolnshire Music Education Hub School Partnership*	£100 per annum
Whole Class Ensemble Teaching (WCET)	£51.30 per session (45 mins + 15 mins set-up)
Whole Class Ensemble Tuition 'Performer Level 1' In House CPD Package	£300
Music Curriculum Delivery	£51.30 per hour
Together Through Music SEND Provision	£51.30 per hour
Infant Music Programme (IMP)	£51.30 per session (45 mins + 15 mins set-up)
Block Booking Instrumental and Vocal Tuition	£51.30 per hour (minimum of 3 hours requirement per week)
School Ensemble Leadership	£51.30 per hour
Music Industry Speaker	Price on application
Musician in Residence	Price on application

*A 20% discount is applied to Lincolnshire Music Education Hub School Partnership and related services for schools with less than 100 pupils on roll (Please note this discount is not applicable to special schools due to the nature of their settings). This discount cannot be applied to commercial licenses such as Charanga, Sing Up (tbc), Music Express, Kapow, Sparkyard and Music First.

1.3 Deadlines for requesting and ceasing tuition:

For your information: New students, as well as existing students wishing to cease, must give notice. Applications must be received by the following deadlines to take effect at the start of each term.

TERM	Deadline to Request or Cease Lessons	Date from which Lessons Start or Cease
Autumn 1	11 th July 2025	8 th Sept 2025
Autumn 2	10 th Sept 2025	3 rd Nov 2025
Spring 3	7 th Nov 2025	6 th Jan 2026
Spring 4	16 th Jan 2026	23 rd Feb 2026
Summer 5	23 rd Feb 2026	21 st April 2026
Summer 6	21 st April 2026	1 st June 2026

Schools who purchase Instrumental and Vocal Lessons (Block Booking Model Direct to Schools) can facilitate the booked time according to their needs. There is not the requirement for a notice period for individual students. Schools must, however, abide by the notice periods outlined above to make changes to the time purchased from LMS.

1.4 Variation: Cancelling Tuition

The (County) Council cannot accept any responsibility for lessons cancelled by the Client, although every effort will be made to rearrange timetables to accommodate the requirements of the Client.

The Client will not be charged if tuition is cancelled by the Council's Lincolnshire Music Service ("LMS"), or due to Staff absence if cover cannot be provided.

1.5 Teaching Weeks

LMS will teach a maximum of 36 weeks during the course of 2025/26 academic year. Additional sessions can be delivered with agreement of all parties involved.

1.6 Teaching Weeks

LMS INSET dates will be as follows:

- 4th September 2025
- 5th September 2025
- 5th January 2026
- 20th April 2026

TERM	TERM STARTS	TERM ENDS
Autumn 1	8th September 2025	17th October 2025
Autumn 2	3 rd November 2025	19 th December 2025
Spring 3	6 th January 2026	13 th February 2026
Spring 4	23 rd February 2026	27 th March 2026
Summer 5	21 st April 2026	22 nd May 2026
Summer 6	1 st June 2026	17 th July 2026

1.7 Invoicing Details for LMS 2025/2026

LMS has a 36-week delivery model and therefore the reconciliation of the account will be carried out at the end of the academic year. LMS will not issue refunds/credits until the end of the academic year.

All Schools should check schedules regularly and notify Lincolnshire Music Service of any changes required and submit any Purchase Orders required for invoicing.

Term	Invoices issued to Schools	LCC Internal Schools Journal
Autumn	w/c Monday 8 th December	w/c Monday 8 th December
Spring	w/c Monday 2 nd March	w/c Monday 2 nd March
Summer	w/c Monday 20 th July	w/c Monday 20 th July

- For LCC schools, the Transfer Journals will be taken from the 'Budget Share' cost centre code ending '00', department M091 (Music Tuition) unless you have advised us otherwise and we have agreed to this.
- For Academies, invoices for spring Term will be issued by 31st March at the latest, in order to meet financial period end requirements.

All Charges are exclusive of VAT which will be levied and payable additionally, where applicable.

1.8 Partnership Working

As part of the agreement between LMS and its partner schools, LMS commits to provide staff that are:

- Subject to a safer recruitment process and enhanced DBS disclosures
- Trained and certificated in Safeguarding for children and young people
- Expected to wear LMS identification
- Highly skilled and qualified music professionals that participate in ongoing CPD and keep up to date with developments in their practice

The management, administration and organisational infrastructure to support LMS delivery includes:

- All appropriate employer's liability and public liability insurances
- Management of staff and resolution of concerns or disputes
- Timetabling including communications with families
- Administration
- All matters relating to NJCs, holiday pay, absences, sickness, maternity or paternity leave, etc.
- Subsidised costs – through National Music Grant and additional fundraising from other sources – including some access to bursaries and fees remissions for students Access for young people, to a wide range of progression routes and other opportunities.

By inviting LMS to work in partnership with your school, you must commit to:

- Ensure that there is a designated contact person to liaise with LMS, and to provide their name and contact details

- Offer a direct line of communication with LMS tutors and make them feel valued as members of staff in the school
- Ensure your LMS teachers are aware of relevant dates in the school calendar, e.g. INSET days, school trips, concerts, and similar
- Provide your LMS tutors with all relevant medical and social information about pupils being taught, and Health and Safety information relating to your site
- Provide the necessary data for individual students for SpeedAdmin and the annual DfE Data Return.
- Ensure there is an appropriate space and environment for the project or teaching to take place, with suitable visibility for safeguarding purposes, where music making can take place uninterrupted, and without disturbing others
- Where appropriate, enable concerts and sharing of work with parents and audiences – for example at the end of a project – and to liaise with LMS tutors over the administration, presentation and delivery of these
- Where students participating in small group and individual lessons are provided with an instrument, support the requirement for this to be registered on SpeedAdmin
- Ensure there is appropriate supervision and support in place for the delivery of whole-class ensemble teaching as well as an appropriate space large enough for the delivery.
- From time to time be invited, as representatives from the school, to attend concerts or events and experience LMS's work in practice, particularly if the school's students are performing
- From time to time, LMS may ask schools to disseminate information to students about our services, products and other activities.

PART 2: PROCESSING, PERSONAL DATA AND DATA SUBJECTS

2. GDPR relationship for the Service is: Joint Data Controllers

SECTION A

Definitions:

Client's Personal Data means the Personal Data supplied by the Client to the Council and/or Personal Data collected by the Council on behalf of the Client for the purposes of or in connection with the Agreement.

Controller takes the meaning given in the GDPR.

Data Protection Legislation means (i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time; (ii) the DPA to the extent that it relates to processing of personal data and privacy; (iii) all applicable Law about the processing of personal data and privacy.

Data Protection Impact Assessment means an assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data.

Data Protection Officer takes the meaning given in the GDPR.

Data Loss Event means any event that results, or may result, in unauthorised access to Personal Data held by the Council under this Agreement, and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach.

Data Subject takes the meaning given in the GDPR.

Data Subject Request means a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation.

DPA means the Data Protection Act 2018.

ICT means information and communications technology.

ICT Environment means the Client's system and the Council system.

Information has the meaning given under section 84 of the FOIA and includes Personal data as defined under Data Protection Legislation.

Information Commissioner's Office means the office of the Information Commissioner whose role is to uphold information rights in the public interest, and responsible for data protection in England, Scotland and Wales in accordance with provisions set out in the DPA.

Joint Controllers means where two or more Controllers jointly determine the purpose and means of processing.

LED means the Law Enforcement Directive (*Directive (EU) 2016/680*).

Personal Data takes the meaning given in the GDPR.

Personal Data Breach takes the meaning given in the GDPR.

Processing takes the meaning given in the GDPR.

Processor takes the meaning given in the GDPR.

Protective Measures means appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of such measures adopted by it including those outlined in Part 2 of Schedule 1.

Sub-processor means any third party appointed to process Personal Data on behalf of the Council

related to this Agreement.

SECTION B

1. The Parties acknowledge that for the purposes of the Data Protection Legislation, the Client and the Council are Joint Controllers.
2. Where Personal Data relating to a Data Subject are collected from the Data Subject, or, someone other than the Data Subject, by either of the Joint Controllers, the Controller obtaining the Personal Data shall, at the time when Personal Data is obtained, be it from the other Controller, Data Subject or any other party provide the Data Subject with all of the following information:-
 - (a) the identity and the contact details of the Controller and, where applicable, of the Controller's representative;
 - (b) the contact details of the Data Protection Officer, where applicable;
 - (c) the purposes of the processing for which the Personal Data are intended as well as the legal basis for the processing;
 - (d) the legitimate interests pursued by the Controller or by a third party;
 - (e) the recipients or categories of recipients of the Personal Data, if any;
 - (f) the categories of Personal Data concerned (this relates to Personal Data obtained from someone other than the Data Subject only);
 - (g) where applicable, the fact that the Controller intends to transfer Personal Data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or where a transfer requires safeguards under [Article 46](#) or [47](#), or the second subparagraph of [Article 49\(1\)](#), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available; and
 - (h) the existence of automated decision-making, including profiling, and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the Data Subject (this only relates when the Personal Data has not been obtained from the Data Subject).
3. In addition to the information referred to in paragraph 2 the Controller who has obtained the Personal Data from the Data Subject shall, at the time when Personal Data is obtained, provide the Data Subject with the following further information necessary to ensure fair and transparent processing:-
 - (a) the period for which the Personal Data shall be stored, or if that is not possible, the

criteria used to determine that period;

- (b) the existence of the right to request from the Controller access to and rectification or erasure of Personal Data or restriction of processing concerning the Data Subject or to object to processing as well as the right to Personal Data portability;
 - (c) where the processing is based on the Data Subject having given consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
 - (d) the right to lodge a complaint with the Information Commissioner's office or any other relevant supervisory authority;
 - (e) whether the provision of Personal Data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the Data Subject is obliged to provide the Personal Data and of the possible consequences of failure to provide such Personal Data; and
 - (f) the existence of automated decision-making, including profiling, and, at least in these cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the Data Subject.
4. Where the Controller intends to further process the Personal Data obtained from the Data Subject for a purpose other than that for which the Personal Data was collected, the Controller shall provide the Data Subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2. Paragraphs 2 and 3 shall not apply where and insofar as the Data Subject already has the information.
5. The Controller who has obtained the Personal Data from someone other than the Data Subject shall provide the information referred to in paragraph 2 (a) to (h):-
- (a) within a reasonable period after obtaining the Personal Data, but at the latest within one (1) Month, having regard to the specific circumstances in which the Personal Data are processed;
 - (b) if the Personal Data is to be used for communication with the Data Subject, at the latest at the time of the first communication to that Data Subject; or
 - (c) if a disclosure to another recipient is envisaged, at the latest when the Personal Data are first disclosed.
6. Where the Controller who has obtained the Personal Data from someone other than the Data Subject intends to further process the Personal Data for a purpose other than that for which the Personal Data was obtained, the Controller shall provide the Data Subject prior to that further processing with information on that other purpose and with any relevant further

information as referred to in paragraph 2 (a) to (h).

7. Paragraph 2 (insofar as it relates to Personal Data obtained from someone other than the Data Subject) and paragraphs 4 to 6 shall not apply where and insofar as:-
 - (a) the Data Subject already has the information;
 - (b) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or in so far as the obligation referred to in paragraph 2 of this part 2 of Schedule 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the Controller shall take appropriate measures to protect the Data Subject's rights and freedoms and legitimate interests, including making the information publicly available;
 - (c) obtaining or disclosure is expressly laid down by Union or Member State law to which the Controller is subject and which provides appropriate measures to protect the Data Subject's legitimate interests; or
 - (d) where the Personal Data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.
8. Subject to paragraph 9, either Party shall notify the other Party and the point of contact identified in section C of part 2 of Schedule 1 immediately if it:-
 - (a) receives a Data Subject Request (or purported Data Subject Request) including a request to rectify, block or erase any Personal Data any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation with the details of any such request;
 - (b) receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under this Agreement;
 - (c) receives a request from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or
 - (d) becomes aware of a Data Loss Event.
9. The obligation to notify under paragraph 8 shall include the provision of further information to the other Party in phases, as details become available.
10. The Party receiving a request as identified in paragraph 8, shall be responsible for responding to the Data Subject provided that the receiving Party shall at all times consult with the other

Party with regards the response unless otherwise agreed between the Parties.

11. The Party who becomes aware of a Data Loss Event shall inform the other Party of the breach and the Parties shall identify which Party would be most appropriate to report the Data Loss Event to the Information Commissioner's Office and to inform the Data Subject(s).
12. Both Parties shall comply with their obligations under Article 30 of the GDPR and shall maintain complete and accurate records and information to demonstrate its compliance with this part A.
13. Each Party shall designate its own Data Protection Officer if required by the Data Protection Legislation.
14. The Council shall remain fully liable for all acts or omissions of any Sub-processor.
15. The Council may, at any time on not less than thirty (30) Working Days' notice, revise this part A by replacing it with any applicable controller to controller standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to this Agreement).
16. The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Council may on not less than thirty (30) calendar days' notice to the Client amend this Agreement to ensure that it complies with any guidance issued by the Information Commissioner's Office.
17. The Parties acknowledge that, in the event that either of them breaches (or attempts or threatens to breach) its obligations relating to Personal Data, the other Party may be irreparably harmed (including harm to its reputation). In such circumstances, the Party not in breach may proceed directly to court and seek injunctive or other equitable relief to remedy or prevent any further breach (or attempted or threatened breach).
18. In the event of a Sub-Contractor of the Council being in liquidation then it is the responsibility of the Council to recover records and Client Personal Data held by the Sub-Contractor and/or Sub-processor and provide assurance to the Client that they have been recovered.
19. The provision of this part A shall apply for the duration of this Agreement and indefinitely after its expiry.

SECTION C

1. The Client and Council have jointly determined the purpose and means of processing as set out in this Schedule 1.
2. The point of contact for Data Subjects is Amy Jaines, Data Protection Officer, Lincolnshire County Council, or her successor.

Description	Details
Identity of the Client and the Council	The Parties acknowledge that for the purposes of the Data Protection Legislation that they are Joint Data Controllers.
Subject matter of the processing	The processing is needed in order to ensure that the Council can effectively deliver the Agreement.
Duration of the processing	Duration of the Agreement.
Nature and purposes of the processing	The nature of the processing means any operation 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 of data (whether or not by automated means). The purpose of the processing of Personal Data is to enable the provision of public services which includes: • maintaining the Client's own accounts and records • supporting and managing employees • promoting services provided by the Client • marketing local tourism • carrying out health and public awareness campaigns • managing property • providing leisure, cultural and/or heritage services • provision of education • carrying out surveys • licensing and regulatory activities • local fraud initiatives • the provision of social services • crime prevention and prosecution offenders including the use of CCTV • corporate administration and all activities we are required to carry out as a data controller and public authority • undertaking research • the provision of all commercial services including the administration and enforcement of parking regulations and restrictions • the provision of all non-commercial activities including refuse collections from residential properties, • internal financial support and corporate functions • managing archived records for historical and research reasons

	• data matching under local and national fraud initiatives • statutory obligation • recruitment assessment
Type of Personal Data	The type of Personal Data which is Processed under this Agreement may include: • Personal details e.g. name, address, date of birth, NI number, telephone number, images, biometric data; • family detail e.g. personal details of relatives, legal guardians and friends; • financial details e.g. pay, bank details, credit/debit card details • lifestyle and social circumstances e.g. physical or mental health details, racial or ethnic origin, trade union membership, political affiliation, political opinions, offences (including alleged offences), religious or other beliefs of a similar nature, criminal proceedings, outcomes and sentences; • employment and education details; • student and pupil records; • business activities; • case file information.
Categories of Data Subject	Categories of Data Subject may include: • customers of the service • suppliers • staff • temporary workers • persons contracted to provide a service • claimants • volunteers • agents • service users • patients • complainants, enquirers or their representatives • professional advisers and consultants • students and pupils • carers, representatives or legal guardians • landlords • recipients of benefits • witnesses • offenders and suspected offenders • licence and permit holders • traders and others subject to inspection • people captured by CCTV images

	• representatives of other organisations • members of the public • users of a particular website
Plan for return and destruction of the data once the processing is complete UNLESS requirement under union or member state law to preserve that type of data	Upon termination or expiry of the Contract each Controller will retain information in line with its own retention schedules.

SECTION D MINIMUM INFORMATION SECURITY CONTROLS

The minimum security controls detailed within this part B of Schedule 1 are to be in place at all times when processing Information for the purpose of or in connection with the delivery of the Services. Such Information includes Personal Data and other Confidential Information or data.

1. GENERAL

- 1.1 Both Parties shall have a security policy in place which sets out management commitment to information security, defines information security responsibilities, and ensures appropriate governance.
- 1.2 All Staff shall complete data protection and information security training commensurate with their role.

2. ICT INFRASTRUCTURE

Boundary Firewall and Internet Gateways

- 2.1 Information, applications and devices shall be protected against unauthorised access and disclosure from the internet, using boundary firewalls, internet gateways or equivalent network devices.

Secure Configuration

- 2.2 ICT systems and devices shall be configured to reduce the level of inherent vulnerabilities and provide only the services required to fulfil their role.

User Access Control

- 2.3 User accounts shall be assigned to authorised individuals only, managed effectively, and they shall provide the minimum level of access to applications, devices, networks, and Personal Data.
- 2.4 Access control (username & password) shall be in place. A password policy shall be in place which includes provisions to ensure:-
- (a) avoidance of the use of weak or predictable passwords;
 - (b) all default passwords are changed;
 - (c) robust measures are in place to protect administrator passwords; and
 - (d) account lock out or throttling is in place to defend against automated guessing attacks.
- 2.5 End user activity shall be auditable and include the identity of end-users who have accessed systems.

Malware Protection

- 2.6 Mechanisms to identify detect and respond to malware on ICT systems and devices shall be in place and shall be fully licensed, supported, and have all available updates applied.

Patch Management and Vulnerability Assessment

- 2.7 Updates and software patches shall be applied in a controlled and timely manner and shall be supported by patch management policies.
- 2.8 The Council shall adopt a method for gaining assurance in its organisation's vulnerability assessment and management processes, for example by undertaking regular penetration tests.
- 2.9 Software which is no longer supported shall be removed from ICT systems and devices.

Cloud Services

- 2.10 The Council shall ensure that the controls applied to the use of cloud services satisfactorily supports the relevant security principles set out in the National Cyber Security Centre Cloud Security Principles:
<https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles>

3. PROTECTING INFORMATION

Electronic Information

- 3.1 Electronic copies of Information shall be encrypted at rest to protect against unauthorised access.

- 3.2 When transmitting Information over the internet, over a wireless communication network e.g. Wi-Fi, or over an untrusted network the Parties shall use an encrypted communication protocol.
- 3.3 The Parties shall only use ICT which is under its governance and subject to the controls set out in this Schedule.

Hard Copy Confidential Information

- 3.4 Hard copy Confidential Information shall be stored securely when not in use and access to it shall be controlled.
- 3.5 Hard copy Confidential Information shall be transported in a secure manner commensurate with the impact a compromise or loss of information would have and which reduces the risk of loss or theft.

Secure Destruction of Information

- 3.6 Electronic copies of Information shall be securely destroyed when no longer required, including Information stored on servers, desktops, laptops or other hardware and media.
- 3.7 Hard copy Information shall be securely destroyed when no longer required.
- 3.8 Secure destruction means destroying Information so it cannot be recovered or reconstituted.
- 3.9 A destruction certificate may be required by the Client to provide the necessary assurance that secure destruction has occurred.

4. COMPLIANCE

- 4.1 Each Party shall inform the other of any non-compliance with the controls set out in this Schedule. Any deficiencies in controls shall be subject to a documented risk management process and where appropriate a remediation plan shall to be implemented with the aim of reducing, where possible, those deficiencies.
- 4.2 Independent validation which has been used as evidence of appropriate security controls by each Party shall be maintained by each Party for the duration of the Agreement.
- 4.3 Each Party shall inform the other of any expired or revoked evidence used as independent validation.