Music Masters' privacy notice

Registered name: UK MUSIC MASTERS LTD

This privacy notice tells you what to expect us to do with your personal information.

You can quickly find the relevant part of the privacy notice using the links to key sections below:

- Contact details
- What information we collect, use, and why
- Lawful bases and data protection rights
- Where we get personal information from
- How long we keep information
- Who we share information with
- Sharing information outside the UK
- How to complain

1 Contact details

1.1 **Post:** Music Masters, First Floor, 10-11 Bishops Terrace, London, SE11 4UE, GB

1.2 **Telephone:** +44 (0)20 3643 5085

1.3 **Email:** contact@musicmasters.org.uk

2 What information we collect, use, and why

2.1 We collect or use the following information to provide services and goods, including delivery and third-party referrals:

(a) Names and contact details

(b) Gender

(c) Pronoun preferences

(d) Addresses

(e) Date of birth

(f) Emergency contact details

(g) Next of kin details

(h) Photographs or video recordings

(i) Call recordings

(j) Service use history

(k) Health information (including medical conditions, test results, allergies, medical requirements and medical history)

(l) Dietary information (including allergies and health conditions)

(m) Information about care needs (including disabilities, home conditions, dietary requirements and general care provisions)

(n) Information about work, home and living conditions

(o) Information about support requirements

(p) Information about lifestyle, interests or personal history – this may include details relevant to recruitment, such as educational and socio-economic background, or career history for safeguarding purposes.

(q) Criminal offence data

(r) Records of meetings and decisions

(s) Information about income and financial needs for funding or personal budget support

(t) Payment details (including card or bank information for transfers and direct debits)

(u) Website user information (including user journeys and cookie tracking)

(v) Information relating to compliments or complaints

(w) Assignment submissions, feedback forms from parents or carers and students; students completing evaluation forms.

(x) Where enabled, messages exchanged between our teachers and parents or carers through our secure messaging system. Email addresses are not visible to the other side, and messages are recorded and kept with your child's record.

2.2 We also collect or use the following information to provide services and goods, including delivery and third party referrals:

(a) Racial or ethnic origin

(b) Political opinions

(c) Religious or philosophical beliefs

(d) Health information

(e) Sexual orientation information

2.3 We collect or use the following information to receive donations or funding and organise fundraising activities:

(a) Names and contact details

(b) Addresses

(c) Payment or banking details

(d) Donation history

(e) Health information

(f) Tax payer information (for Gift Aid purposes)

(g) Whether the donor wants to remain anonymous or have a public acknowledgement of their gift; the terms under which the gift is made.

2.4 We also collect or use the following information to receive donations or funding and organise fundraising activities:

(a) Health information

2.5 We collect or use the following personal information for the prevention, detection, investigation or prosecution of crimes:

(a) Names and contact information

(b) Customer or client accounts and records

(c) Criminal offence data (including Disclosure Barring Service (DBS), Access NI or Disclosure Scotland checks)

(d) Video recordings of public areas (including indoor and outdoor spaces)

(e) Audio recordings of public areas (including indoor and outdoor spaces)

(f) Call recordings

(g) Financial transaction information

(h) Relevant information from previous investigations

(i) Witness statements and contact details

(j) Information relating to health and safety

2.6 We collect or use the following personal information for service updates or marketing purposes:

(a) Names and contact details

(b) Addresses

(c) Marketing preferences

(d) Recorded images, such as photos or videos

(e) Purchase history

(f) Donation history

(g) IP addresses

(h) Website and app user journey information

(i) Records of consent, where appropriate

(j) social media profiles or engagement; event attendance

2.7 We also collect or use the following information for service updates or marketing purposes:

(a) Racial or ethnic origin

2.8 We collect or use the following personal information for research or archiving purposes:

(a) Names and contact details

(b) Addresses

(c) Recorded images, such as photos or videos

(d) Call recordings

(e) Purchase history

(f) Records of consent, where appropriate

(g) photos of reflections from students that they have written down.

2.9 We also collect or use the following information for research or archiving purposes:

(a) Racial or ethnic origin

(b) Religious or philosophical beliefs

(c) Health information

(d) Sexual orientation information

2.10 We collect or use the following personal information to comply with legal requirements:

(a) Name

(b) Contact information

(c) Identification documents

(d) Financial transaction information

(e) Health and safety information

(f) Criminal offence data

(g) DBS check status - we record the outcome/status of DBS checks for safeguarding compliance. Where a DBS certificate is provided for verification, this is reviewed by authorised staff and securely deleted after verification, it is not stored. DBS applications are submitted through HR Connect, an online portal powered by Cantium, which acts as an umbrella body for DBS applications on our behalf.

2.11 We also collect or use the following information to comply with legal requirements:

(a) Health information

(b) Public liability insurance

(c) Signed policy declarations from teaching staff, which we are required to collect for safeguarding and operational compliance

2.12 We collect or use the following personal information for recruitment purposes:

(a) Contact details (eg name, address, telephone number or personal email address)

(b) Date of birth

(c) National Insurance number

(d) Copies of passports or other photo ID

(e) Employment history (eg job application, employment references or secondary employment) - including any gaps in employment, to ensure safeguarding compliance

(f) Education history (eg qualifications)

(g) Educational background, such as highest level achieved and whether first in family to attend university

(h) Right to work information

(i) Details of any criminal convictions (eg Disclosure Barring Service (DBS), Access NI or Disclosure Scotland checks)

(j) Security clearance details (eg basic checks and higher security clearance)

2.13 We also collect or use the following information for recruitment purposes:

(a) Racial or ethnic origin

(b) Health Information

(c) Disability Information (recognised under the Equality Act 2010)

(d) Neurodiversity

(e) Gender (including your pronouns)

(f) Age

(g) Sexual orientation

(h) Socio-economic background – e.g. family income

(i) Carer status

(j) Employment status

(k) Nationality

2.14 We collect or use the following personal information to employ our staff and manage our working relationship with them:

(a) Contact details, date of birth, emergency contact and next of kin details

(b) National Insurance number, bank details, salary, pension and tax information

(c) Signed employment contract, job title, working hours and location

(d) Right to work and DBS check status (see "to comply with legal requirements" and "How long we keep information")

(e) Records of annual leave, sickness absence and other leave, such as family leave

(f) Performance reviews, supervision and training records

(g) Records of grievances, disciplinary matters and investigations

(h) Signed policy declarations

(i) Photographs of staff

(j) Records of your use of our IT systems, including Salesforce activity logs (see "to keep our systems and the personal data we hold secure")

2.15 We also collect or use the following information to employ our staff:

(a) Health information, including sickness details, fit notes, occupational health reports and information needed to make reasonable adjustments

(b) Allergies and medical requirements, where you choose to share them for your safety at work

(c) Equality monitoring information, such as racial or ethnic origin, disability and sexual orientation, which you can choose not to provide

(d) Criminal offence data from DBS checks

We handle this information in line with our Appropriate Policy Document, which sets out the conditions we rely on under the Data Protection Act 2018.

2.16 When someone also expresses an interest in working with us and wishes to join our talent pool via the 'work with us' form on our website, we also collect or use the following personal information for the purpose for having them a part of our talent pool:

(a) Name and contact details

(b) Note: If someone contacts us speculatively to express an interest in working with us, or registers to receive updates about future opportunities, we will keep their details in our talent pool for up to two years so that we can contact them about suitable roles. At the end of this period, we will contact the person to confirm if they wish to remain in the talent pool. If we do not hear from the individual, their details will be deleted. We rely on the person's consent to process this information, and they can withdraw their consent at any time by contacting contact@musicmasters.org.uk. If someone withdraws their consent, their details will be removed immediately from the talent pool.

2.17 We collect or use the following personal information for dealing with queries, complaints or claims:

(a) Names and contact details

(b) Address

(c) Purchase or service history

(d) Video recordings of public areas

(e) Audio recordings of public areas

(f) Call recordings

(g) Witness statements and contact details

(h) Relevant information from previous investigations

(i) Customer or client accounts and records

(j) Financial transaction information

(k) Information relating to health and safety (including incident investigation details and reports and accident book records)

(l) Correspondence

(m) Incident report forms; event attendance; attendance to sessions and lessons; contracts that we store; gift agreements with funders; pledge information; video or photos of events.

2.18 We collect or use the following personal information about freelancers, consultants and contractors we engage:

(a) Contact details

(b) Right to work information, including identity documents, Home Office share codes, and the output of digital identity verification (including images of identity documents and a facial image provided by the individual)

(c) Criminal records check status, where the role requires it

(d) Evidence of public liability insurance

(e) Signed policy declarations and safeguarding training records

(f) Bank and invoicing details for payment

(g) Where a contractor arranges a substitute to deliver work on their behalf, the same information in respect of that substitute

(h) Records of your activity on our Salesforce system, including the Teacher Portal (see "keep our systems and the personal data we hold secure" below)

2.19 We collect or use the following personal information to keep our systems and the personal data we hold secure:

(a) Records of how employees, freelancers, contractors and other authorised users use our Salesforce system, including the Teacher Portal, such as:

- login and logout times, IP address, browser and approximate location

- records viewed, created, edited or deleted

- reports and list views run or exported

- files downloaded or previewed

- alerts about unusual activity, such as suspicious logins

(b) We use this information to detect and investigate unauthorised access and personal data breaches, and to maintain our systems. Access is limited to a small number of authorised staff. We do not use it to routinely monitor anyone's work, but we may use it as evidence when investigating a suspected data breach or misuse of personal data.

2.20 We collect or use personal information in connection with I'M IN, including:

(a) names and contact details

(b) organisation name, role and professional information

(c) account and login information

(d) subscription and service-use information

(e) records of activity and engagement with the I'M IN Platform

(f) communications with Music Masters and I'M IN Advisors

(g) booking and session information

(h) marketing and communication preferences

(i) payment and invoicing information where relevant.

(j) evaluation and feedback responses

(k) structured notes recorded by I'M IN Advisors following programme sessions and check-ins.

(l) We use this information to administer I'M IN subscriptions, provide access to the Platform, support users, facilitate contact with I'M IN Advisors, manage and evaluate the programme, improve the service, and communicate with users about I'M IN.

3 Our Cookie Policy

3.1 We use cookies and similar tracking technologies on our website to enhance your experience and to understand how our website is used. For detailed information on the cookies we use, how they work, and your options for managing them, please read our Cookie Policy by clicking here.

3.2 You can also adjust your cookie settings when you first visit our site or at any time through your browser.

4 Website Usage and Analytics Data

4.1 We may process data about your use of our website and services ("usage data"). The usage data may include your IP address, geographical location, browser type and version, operating system, referral source, length of visit, page views and website navigation paths, as well as information about the timing, frequency and pattern of your service use. The source of the usage data is our analytics tracking system. This usage data may be processed for the purposes of analysing the use of the website and services. The legal basis is our legitimate interests, namely monitoring and improving our website and services. This data helps us see which parts of our website are most helpful to our visitors and where we can make improvements.

4.2 We use Google Analytics to analyse the use of our website. Google Analytics gathers information about website use by means of cookies. The information gathered relating to our website is used to create reports about the use of our website. Google's privacy policy is available at: https://www.google.com/policies/privacy/. The relevant cookie is: collect

5 Lawful bases and data protection rights

5.1 Under UK data protection law, we must have a “lawful basis” for collecting and using your personal information. There is a list of possible lawful bases in the UK GDPR. You can find out more about lawful bases on the ICO’s website.

5.2 Which lawful basis we rely on may affect your data protection rights which are in brief set out below. You can find out more about your data protection rights and the exemptions which may apply on the ICO’s website:

(a) Your right of access - You have the right to ask us for copies of your personal information. You can request other information such as details about where we get personal information from and who we share personal information with. There are some exemptions which means you may not receive all the information you ask for. You can read more about this right here.

(b) Your right to rectification - You have the right to ask us to correct or delete personal information you think is inaccurate or incomplete. You can read more about this right here.

(c) Your right to erasure - You have the right to ask us to delete your personal information. You can read more about this right here.

(d) Your right to restriction of processing - You have the right to ask us to limit how we can use your personal information. You can read more about this right here.

(e) Your right to object to processing - You have the right to object to the processing of your personal data. You can read more about this right here.

(f) Your right to data portability - You have the right to ask that we transfer the personal information you gave us to another organisation, or to you. You can read more about this right here.

(g) Your right to withdraw consent – When we use consent as our lawful basis you have the right to withdraw your consent at any time. You can read more about this right here.

5.3 If you make a request, we must respond to you without undue delay and in any event within one month.

5.4 To make a data protection rights request, please contact us using the contact details at the top of this privacy notice.

6 Our lawful bases for the collection and use of your data

6.1 Our lawful bases for collecting or using personal information to provide services and goods, including delivery and third-party referrals are:

(a) Consent - we have permission from you after we gave you all the relevant information. All of your data protection rights may apply, except the right to object. To be clear, you do have the right to withdraw your consent at any time.

(b) Contract – we have to collect or use the information so we can enter into or carry out a contract with you. All of your data protection rights may apply except the right to object.

(c) Legal obligation – we have to collect or use your information so we can comply with the law. All of your data protection rights may apply, except the right to erasure, the right to object and the right to data portability.

(d) Legitimate interests – we're collecting or using your information because it benefits you, our organisation or someone else, without causing an undue risk of harm to anyone. All of your data protection rights may apply, except the right to portability. Our legitimate interests are:

(i) We use users' personal information to improve the efficiency and effectiveness of our programme delivery, ensuring we can provide high-quality services that meet the needs of our communities. By understanding which programmes receive the best feedback, identifying areas for improvement, and learning more about user preferences, we can better allocate resources and enhance the overall experience for our participants. This helps us ensure that our work remains impactful and relevant. We carefully assess the balance between our organisational needs and the rights of individuals, implementing strict data protection measures to protect user privacy and only collecting information that directly informs our service improvement efforts. Our commitment to secure data handling, transparency, and user choice ensures that the benefits to our community are achieved without undue impact on individual privacy.

(ii) For I'M IN, we rely primarily on our legitimate interests in administering and delivering the programme, supporting participating organisations and Platform users, maintaining appropriate records, evaluating and improving the programme, and understanding participation and engagement. Where an individual is themselves party to a contract with us, we may also rely on contract where the processing is necessary to perform that contract.

(iii) We use parents' and carers' contact details to communicate with them about their child's participation, including, where enabled, messages from their child's teacher through our secure messaging system.

(e) Vital interests – collecting or using the information is needed when someone's physical or mental health or wellbeing is at urgent or serious risk. This includes an urgent need for life sustaining food, water, clothing or shelter. All of your data protection rights may apply, except the right to object and the right to portability.

(f) Public task – we have to collect or use your information to carry out a task laid down in law, which the law intends to be performed by an organisation such as ours. All of your data protection rights may apply, except the right to erasure and the right to portability.

(g) Our lawful bases for collecting or using personal information to receive donations or funding and organise fundraising activities are:

(h) Consent - we have permission from you after we gave you all the relevant information. All of your data protection rights may apply, except the right to object. To be clear, you do have the right to withdraw your consent at any time.

(i) Contract – we have to collect or use the information so we can enter into or carry out a contract with you. All of your data protection rights may apply except the right to object.

(j) Legal obligation – we have to collect or use your information so we can comply with the law. All of your data protection rights may apply, except the right to erasure, the right to object and the right to data portability.

(k) Legitimate interests – we're collecting or using your information because it benefits you, our organisation or someone else, without causing an undue risk of harm to anyone. All of your data protection rights may apply, except the right to portability. Our legitimate interests are:

(i) We collect and use personal information to support our essential fundraising activities, including receiving donations and organising events that allow us to continue delivering impactful programmes. By understanding donor preferences, engagement history, and communication preferences, we can provide relevant updates, express gratitude, and share how donations contribute to our mission. This ensures donors feel valued and informed about the impact of their support. We recognise the importance of balancing our needs with the privacy of our supporters. Therefore, we implement secure data management practices, limit data collection to necessary details, and provide clear choices around communication preferences. This approach allows us to sustain our work while respecting the privacy rights of our donors and funders.

(l) Vital interests – collecting or using the information is needed when someone's physical or mental health or wellbeing is at urgent or serious risk. This includes an urgent need for life sustaining food, water, clothing or shelter. All of your data protection rights may apply, except the right to object and the right to portability.

(m) Public task – we have to collect or use your information to carry out a task laid down in law, which the law intends to be performed by an organisation such as ours. All of your data protection rights may apply, except the right to erasure and the right to portability.

6.2 Our lawful bases for collecting or using personal information for the prevention, detection, investigation or prosecution of crimes are:

( ) Legal obligation – we have to collect or use your information so we can comply with the law. All of your data protection rights may apply, except the right to erasure, the right to object and the right to data portability.

6.3 Our lawful bases for collecting or using personal information for service updates or marketing purposes are:

( ) Consent - we have permission from you after we gave you all the relevant information. All of your data protection rights may apply, except the right to object. To be clear, you do have the right to withdraw your consent at any time.

(a) Legal obligation – we have to collect or use your information so we can comply with the law. All of your data protection rights may apply, except the right to erasure, the right to object and the right to data portability.

(b) Legitimate interests – we're collecting or using your information because it benefits you, our organisation or someone else, without causing an undue risk of harm to anyone. All of your data protection rights may apply, except the right to portability. Our legitimate interests are:

(i) We collect and use personal information to provide timely service updates and relevant marketing communications, ensuring that our users, supporters, and partners remain informed about new programmes, opportunities, events, and other activities that align with their interests. By understanding user preferences, we can tailor our communications to share the most relevant updates and avoid overwhelming individuals with unnecessary information. This approach enhances engagement and supports our mission by connecting individuals with the services and resources that may benefit them. We take privacy seriously and are committed to respecting individuals' preferences by offering clear choices for opting in or out of marketing communications. Our secure data handling practices and transparent communication choices allow us to provide valuable updates while maintaining user trust and control over their personal information.

For I'M IN marketing communications, we rely on consent where consent is required. You can withdraw your consent or opt out of marketing communications at any time.

6.4 Our lawful bases for collecting or using personal information for research or archiving purposes are:

( ) Consent - we have permission from you after we gave you all the relevant information. All of your data protection rights may apply, except the right to object. To be clear, you do have the right to withdraw your consent at any time.

(a) Contract – we have to collect or use the information so we can enter into or carry out a contract with you. All of your data protection rights may apply except the right to object.

(b) Legitimate interests – we're collecting or using your information because it benefits you, our organisation or someone else, without causing an undue risk of harm to anyone. All of your data protection rights may apply, except the right to portability. Our legitimate interests are:

(i) We collect and use personal information for research and archiving to improve our understanding of the long-term impact of our programmes, inform future initiatives, and contribute valuable insights to the wider charity and educational sectors. By analysing past activity and outcomes, we can better identify trends, measure progress, and develop evidence-based improvements to our work, ultimately benefitting the communities we serve. In conducting research and archiving, we prioritise data security. Our approach ensures that while we gain meaningful insights to enhance our programmes, we maintain respect for individuals' privacy rights and keep data collection to what is essential for our research aims.

6.5 Our lawful bases for collecting or using personal information to comply with legal requirements are:

( ) Contract – we have to collect or use the information so we can enter into or carry out a contract with you. All of your data protection rights may apply except the right to object.

(a) Legal obligation – we have to collect or use your information so we can comply with the law. All of your data protection rights may apply, except the right to erasure, the right to object and the right to data portability.

(b) Vital interests – collecting or using the information is needed when someone's physical or mental health or wellbeing is at urgent or serious risk. This includes an urgent need for life sustaining food, water, clothing or shelter. All of your data protection rights may apply, except the right to object and the right to portability.

6.6 Our lawful bases for collecting or using personal information for recruitment purposes are:

( ) Consent - we have permission from you after we gave you all the relevant information. All of your data protection rights may apply, except the right to object. To be clear, you do have the right to withdraw your consent at any time.

(a) Contract – we have to collect or use the information so we can enter into or carry out a contract with you. All of your data protection rights may apply except the right to object.

(b) Legal obligation – we have to collect or use your information so we can comply with the law. All of your data protection rights may apply, except the right to erasure, the right to object and the right to data portability.

(c) Vital interests – collecting or using the information is needed when someone's physical or mental health or wellbeing is at urgent or serious risk. This includes an urgent need for life sustaining food, water, clothing or shelter. All of your data protection rights may apply, except the right to object and the right to portability.

6.7 Our lawful bases for collecting or using personal information for dealing with queries, complaints or claims are:

( ) Contract – we have to collect or use the information so we can enter into or carry out a contract with you. All of your data protection rights may apply except the right to object.

(a) Legal obligation – we have to collect or use your information so we can comply with the law. All of your data protection rights may apply, except the right to erasure, the right to object and the right to data portability.

6.8 Our lawful basis for collecting or using personal information to keep our systems and the personal data we hold secure is:

( ) Legitimate interests – we're collecting or using your information because it benefits you, our organisation or someone else, without causing an undue risk of harm to anyone. All of your data protection rights may apply, except the right to portability. Our legitimate interests are:

(i) Keeping the personal data we hold secure, much of which relates to children and young people, and meeting our legal duty to protect it with appropriate security measures. Logging system activity allows us to detect unauthorised access, investigate incidents and show that data has been handled properly. We have balanced this against the privacy of the people using our systems: the logs record system activity only, access is restricted to authorised staff, they are not used for routine performance monitoring, and they are deleted after a set period.

6.9 Our lawful bases for collecting or using personal information to employ our staff are:

( ) Contract – we need the information to carry out your employment contract, for example to pay you. All of your data protection rights may apply except the right to object.

(a) Legal obligation – we need the information to comply with employment, tax, pensions, health and safety and safeguarding law, for example reporting to HMRC, auto-enrolling you in a pension and checking your right to work. All of your data protection rights may apply, except the right to erasure, the right to object and the right to data portability.

(b) Legitimate interests – all of your data protection rights may apply, except the right to portability. Our legitimate interests are: managing our staff effectively, keeping our systems and data secure, and handling grievances, disciplinary matters and disputes fairly.

(c) Consent – for optional information such as equality monitoring and staff photographs used publicly. You can withdraw your consent at any time.

6.10 Where we get personal information from:

( ) Directly from you

(a) Regulatory authorities

(b) Family members or carers

(c) Other health and care providers

(d) Charities or voluntary sector organisations

(e) Schools, colleges, universities or other education organisations

(f) Insurance companies

(g) Publicly available sources - including organisation websites, professional directories, publicly available professional contact information and social media platforms.

(h) Councils and other public sector organisations

(i) Previous employers

(j) Market research organisations

(k) Providers of marketing lists and other personal information

(l) Suppliers and service providers

(m) Occupational health providers

(n) Third parties:

(i) Tools that we use for managing events, such as Jot Form.

(ii) Individuals nominating others to participate in a Music Masters programme; email correspondence that can form part of evaluation.

6.11 Some of the information we collect is considered sensitive under UK data protection law (also known as "special category data"). This may include health information, disability and ethnicity. We only collect this information where it is relevant and necessary, and we process it in line with our data protection obligations.

7 How long we keep information

7.1 This section sets out our data retention policies and procedure, which are designed to help ensure that we comply with our legal obligations in relation to the retention and deletion of personal data.

7.2 Personal data that we process for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

7.3 Notwithstanding the other provisions of this section, we may retain your personal data where such retention is necessary for compliance with a legal obligation to which we are subject, or in order to protect your vital interests or the vital interests of another natural person. For example, personal data related to financial transactions (e.g., donations) will be retained for seven years to comply with tax and auditing regulations. Likewise, Bursary applications are retained for seven years in line with financial record-keeping requirements, after which they are securely deleted. Recruitment records will generally be kept for six months after the recruitment process concludes, unless consent has been given for future opportunities. Expressions of interest and talent pool records will be kept for up to two years, after which we will contact you to confirm if you wish to remain in our records. If we do not hear from you, your details will be deleted. You may withdraw your consent at any time. Employee records will be retained for 6 years after they leave for legal reasons, like compliance with employment law. We retain student programme records for the duration of their participation in Music Masters. Once a student leaves, their record is securely deleted as part of our annual data clean-up process. Messages between our teachers and parents or carers are kept with the student's record and deleted at the same time. We may retain anonymised participation data for research and impact reporting. This information cannot

be used to identify individuals. Safeguarding records are retained separately and in line with our Safeguarding Retention Policy. DBS certificates provided for verification are not retained, only the DBS check status and reference number are recorded alongside the date the check was completed, the level and type of check completed and the decision made about whether the person was employed (with reasons). Right to work records are retained for the duration of the individual's employment or engagement and for a further two years, after which they are securely destroyed. This applies to employees, freelancers and contractors, and to any follow-up or repeat checks. Records are held in a format which cannot be manually altered, together with a record of the date on which each check was carried out.

7.4 System activity logs and records of individual system events are kept for one year, after which they are deleted automatically.

7.5 Personal information associated with an active I'M IN subscription or Platform account is retained for the duration of the 24-month Subscription Period while it is needed to provide the service. After the Subscription Period ends, access to the I'M IN Platform ends. We retain relevant organisational I'M IN data securely in Salesforce and may also retain relevant records in SharePoint where this is necessary to administer, evaluate and develop I'M IN, understand how organisations' practice changes over time, identify sector trends, and understand which parts of the sector we have reached. Free-text submissions and files uploaded to the I'M IN Platform are deleted from the Platform when the subscription ends and are not transferred to our other systems. Copies may remain in routine system backups for a limited period until they are overwritten in the normal course, and are not accessed or used during that time. Personal contact information associated with I'M IN participation, such as names, roles and email addresses, is reviewed periodically and deleted or updated when it is no longer needed. This does not prevent us from retaining relevant organisational I'M IN data for administration, evaluation and programme development. Anonymised and aggregated data may be retained for ongoing analysis, evaluation and sector insight. Individual organisations will not be identifiable in published information based on this data. Financial and other records may be retained for longer where required for legal, regulatory, accounting or governance purposes.

7.6 Where someone has expressed an interest in I'M IN or agreed to receive I'M IN marketing but has not become a subscriber, we retain their contact details and communication preferences for as long as they remain relevant to the purpose for which they were collected. We review these records periodically and delete them when they are no longer needed, or earlier where consent is withdrawn or the individual asks us to stop contacting them. We may retain a minimal suppression record where necessary to ensure that an opt-out is respected.

8 Who we share information with:

8.1 Data processors

( )

(a) JotForm: This data processor does the following activities for us:

(i) Category: Online form builder and data collection service.

(ii) Sector: Data collection and online forms, US-based.

(iii) Role: Jotform collects data from applications and feedback forms for recruitment and service delivery, used in event delivery too.

(b) Salesforce:

(i) Category: Customer Relationship Management (CRM) platform

(ii) Sector: CRM and nonprofit data management, US-based company, UK-hosted instance (GBR112)

(iii) Role: Salesforce is Music Masters' primary CRM system, used to store and manage records relating to programme participants, donors, supporters, volunteers, freelancers, contractors and I'M IN organisations and contacts. For I'M IN, Salesforce is used to manage subscriber and prospect records, organisational relationships, programme engagement, communications and relevant records retained after a subscription ends. The Nonprofit Success Pack (NPSP) is used to manage fundraising, programme delivery and contact records. Salesforce also records activity logs for users of the system, including the Teacher Portal, which we use for security purposes.

(c) QuestionPro**:** This data processor does the following activities for us:

(i) Category: Survey and data analytics platform.

(ii) Sector: Survey research and data analytics, US-based.

(iii) Role: QuestionPro supports data collection for research, impact evaluation, and user feedback.

(d) WhatsApp:

(i) Category: Communication and messaging platform.

(ii) Sector: Social communication and messaging, part of Meta (US-based).

(iii) Role: WhatsApp facilitates internal team communication, project updates, and outreach with certain partners or service users.

(e) Mailchimp:

(i) Category: Email marketing and automation platform.

(ii) Sector: Marketing and communications, US-based.

(iii) Role: Mailchimp sends newsletters, service updates, and other communications to supporters, partners, and users.

(f) Slack:

(i) Category: Team collaboration and communication tool.

(ii) Sector: Communication and project management, US-based.

(iii) Role: Slack is used for internal team communication and collaboration.

(g) Donorfy (now owned by The Access Group):

(i) Category: Donor management and CRM system.

(ii) Sector: Non-profit donor management, UK-based.

(iii) Role: Donorfy manages donor information, donation histories, and fundraising efforts.

(h) The Big Give:

(i) Category: Fundraising and donation platform.

(ii) Sector: Fundraising, UK-based.

(iii) Role: The Big Give processes and tracks donations made through specific fundraising campaigns.

(i) CAF (Charities Aid Foundation):

(i) Category: Charity banking and donation processing.

(ii) Sector: Financial services for non-profits, UK-based.

(iii) Role: CAF processes donations, manages charitable funds, and provides banking services.

(j) Microsoft / SharePoint / Outlook:

(i) Category: IT and productivity software provider.

(ii) Sector: Technology and productivity solutions, US-based.

(iii) Role: Microsoft provides platforms for document storage (SharePoint), email communications (Outlook), and general office software.

(k) Easyfundraising:

(i) Category: Fundraising support platform.

(ii) Sector: Charity fundraising, UK-based.

(iii) Role: Easyfundraising supports online fundraising by linking users to retailers and facilitating donation contributions.

(l) Xero:

(i) Category: Accounting software.

(ii) Sector: Financial management and accounting, New Zealand-based.

(iii) Role: Xero manages financial records, accounting processes, and expense tracking.

(m) Safe HR:

(i) Category: HR and payroll management software.

(ii) Sector: Human resources and payroll, UK-based.

(iii) Role: Safe HR handles HR records, payroll processing, and employee compliance management.

(n) Furlong Maestro: (previously used, not active)

(i) Category: School administration and management software.

(ii) Sector: Education management, UK-based.

(iii) Role: Furlong Maestro manages student records, school administration, and program logistics.

(o) Google Forms:

(i) Category: Online form and survey tool.

(ii) Sector: Data collection, part of Google Workspace, US-based.

(iii) Role: Google Forms collects responses for surveys, feedback, and event registrations.

(p) Dropbox:

(i) Category: Cloud storage and file sharing

(ii) Sector: Technology and data storage, US-based

(iii) Role: Dropbox stores and shares documents and files used by the organisation, including resources, reports, and any documents shared between team members or external collaborators.

(q) Google Drive:

(i) Category: Cloud storage and collaboration

(ii) Sector: Technology and data storage, US-based

(iii) Role: Google Drive provides storage for organisational files, supports team collaboration on shared documents, and facilitates secure document sharing.

(r) SharePoint:

(i) Category: Cloud storage and document management

(ii) Sector: Technology and data storage (Microsoft), US-based

(iii) Role: SharePoint stores documents, enables version control, and allows team collaboration through shared files and folders, often used for organisational knowledge management and internal resources.

(s) Outlook:

(i) Category: Email and calendar service

(ii) Sector: Communication and productivity software (Microsoft), US-based

(iii) Role: Outlook manages internal and external email communications, stores contact information, and organises calendar events and appointments.

(t) DBS (Disclosure and Barring Service)

(i) Category: Background checks

(ii) Sector: Government and public service, UK-based

(iii) Role: DBS performs criminal record checks for employees, contractors, or volunteers working with vulnerable groups, ensuring safeguarding compliance within the charity.

(u) HR Connect (Cantium / https://ukdbschecks.employmentcheck.org.uk)

(i) Category: DBS umbrella body and application portal

(ii) Sector: HR compliance and safer recruitment services, UK-based

(iii) Role: HR Connect, powered by Cantium, processes DBS applications on Music Masters' behalf as an umbrella body, enabling access to the Disclosure and Barring Service. Personal data submitted as part of a DBS application is processed through this platform.

(v) Rightcheck.io

(i) Category: Right to work and identity verification provider

(ii) Sector: Digital identity and compliance screening, UK-based

(iii) Role: Rightcheck carries out digital identity verification and right to work checks on Music Masters' behalf for employees, freelancers and contractors. This includes validating identity documents, checking Home Office share codes, and comparing the photograph on the identity document with an image provided by the individual. Data is hosted in the United Kingdom on Amazon Web Services and is not transferred outside the UK. Rightcheck uses no sub-processors for right to work checks.

(w) JustGiving:

(i) Category: Online fundraising platform

(ii) Sector: Fundraising and donations, UK-based

(iii) Role: JustGiving processes donations and manages fundraising campaigns, allowing supporters to contribute to the charity through dedicated online pages.

(x) Stripe:

(i) Category: Payment processing

(ii) Sector: Financial services and payment technology, US-based

(iii) Role: Stripe processes online payments, including payments for I'M IN subscriptions, as well as payments and donations relating to other Music Masters services and fundraising activities.

(y) PayPal:

(i) Category: Payment processing

(ii) Sector: Financial services and payment technology, US-based

(iii) Role: PayPal handles online transactions, allowing supporters to make donations and payments securely through its platform.

(z) Facebook:

(i) Category: Social media and advertising

(ii) Sector: Social media and digital advertising, US-based

(iii) Role: Facebook is used to engage supporters, share updates, run awareness campaigns, and collect insights on audience engagement through social media interactions and paid advertising.

(aa) LinkedIn:

(i) Category: Professional networking and recruitment

(ii) Sector: Social media and professional networking, US-based

(iii) Role: LinkedIn supports recruitment efforts, professional networking, and organisational promotion, connecting the charity with potential employees, partners, and donors.

(bb) X (formerly Twitter):

(i) Category: Social media and advertising

(ii) Sector: Social media and digital advertising, US-based

(iii) Role: X is used for outreach, audience engagement, and sharing real-time updates with followers.

(cc) Instagram:

(i) Category: Social media and advertising

(ii) Sector: Social media and digital advertising (part of Meta), US-based.

(iii) Role: Instagram is used for visual storytelling, audience engagement, and sharing updates on Music Masters' programmes and events.

(dd) TikTok

(i) Category: Social media and advertising

(ii) Sector: Social media and digital advertising, China-based

(iii) Role: TikTok is used for short-form video content to engage audiences and promote programmes

(ee) YouTube:

(i) Category: Social media and advertising

(ii) Sector: Video sharing and digital advertising, US-based (part of Google).

(iii) Role: YouTube is used to host and share video content, such as performances, programme highlights, and educational materials, and to gather audience engagement insights.

(ff) Vitanium:

(i) Category: Data backup and storage

(ii) Sector: IT services, UK-based

(iii) Role: Vitanium provides secure backup services as a sub-processor of Blue Lizard IT, backing up our SharePoint data. Backups are encrypted and stored within the UK, and are kept for up to 90 days.

(gg) Hubdoc Inc:

(i) Category: Document management and data extraction platform

(ii) Sector: Financial technology, Canada-based company owned by Xero; data hosted in the United States on Amazon Web Services

(iii) Role: Hubdoc is used to manage and extract data from financial documents, such as invoices and receipts. It supports our accounting processes by securely processing and storing financial information, which may include personal data, in compliance with data protection regulations.

(hh) Blue Lizard IT:

(i) Category: IT support and systems consultancy

(ii) Sector: IT services, UK-based

(iii) Role: Blue Lizard provides IT support, backup management and Salesforce development and support. This means it may access personal data held on our systems, including our

Salesforce records. All processing takes place in the UK. Blue Lizard uses Vitanium (above) as a sub-processor for backups, with our written consent.

(ii) Bubble:

(i) Category: No-code application development and hosting platform.

(ii) Sector: Technology and application hosting, US-based.

(iii) Role: Bubble hosts and operates the I'M IN Platform, including user accounts, organisational profile information, subscription information, Platform activity and other information required to provide the I'M IN service.

(jj) Zapier

(i) Category: Automation and integration platform.

(ii) Sector: Technology and systems integration, US-based.

(iii) Role: Zapier is used to automate the transfer of information between systems used to deliver and administer I'M IN.

(kk) I'M IN Advisors

(i) I'M IN Advisors who may have access to personal information held within the I'M IN Platform where this is necessary to deliver the programme and support subscribers. When accessing or using Platform information on Music Masters' behalf and under our instructions, Advisors act as processors for Music Masters.

(ii) I'M IN Advisors may also use their own booking, calendar and video-conferencing tools to arrange and hold sessions. Where they process personal information within those tools for their own purposes or under their own arrangements, they are responsible for complying with data protection law in relation to that processing.

(iii) I'M IN Advisors may use approved transcription or AI tools to help prepare notes and Report Packs. They do so under Music Masters' instructions and the terms of their agreement with us. Sessions will not be recorded or transcribed unless everyone attending has been told in advance and has agreed. Advisors must remove identifying details before entering information into an AI tool.

(ll) Others we share personal information with:

(i) Insurance companies, brokers and other intermediaries

(ii) HMRC

(iii) Other health providers (eg GPs and consultants)

(iv) Charities and voluntary organisations

(v) Organisations we need to share information with for safeguarding reasons

(vi) Emergency services

(vii) Professional advisors

(viii) Legal bodies or authorities

(ix) Local authorities or councils

(x) Relevant regulatory authorities

(xi) External auditors or inspectors

(xii) Organisations we're legally obliged to share personal information with

(xiii) Publicly on our website, social media or other marketing and information media

(xiv) Current employers

(xv) Previous employers

(xvi) Suppliers and service providers

(xvii) Professional consultants

(xviii) Third parties: Organisations that help us run music events or fundraising events, they may require some personal data from participants - e.g. allergy information - that, with consent, we would share with the relevant third party.

(xix) Nest Pensions

9 Sharing information outside the UK

9.1 Where necessary, we may transfer personal information outside of the UK. When doing so, we comply with the UK GDPR, making sure appropriate safeguards are in place.

9.2 For further information or to obtain a copy of the appropriate safeguard for any of the transfers below, please contact us using the contact information provided above.

( ) Organisation name: JotForm

(i) Category of recipient: Data collection platform

(ii) Country the personal information is sent to: US

(iii) How the transfer complies with UK data protection law: Addendum to the EU Standard Contractual Clauses (SCCs)

(a) Organisation name: Mailchimp

(i) Category of recipient: Marketing and email automation provider

(ii) Country the personal information is sent to: US

(iii) How the transfer complies with UK data protection law: Addendum to the EU Standard Contractual Clauses (SCCs)

(b) Organisation name: Salesforce

(i) Category of recipient: CRM and data management platform

(ii) Country the personal information is sent to: UK (primary). Where connected services or support arrangements involve transfers outside the UK, these are subject to appropriate safeguards.

(iii) How the transfer complies with UK data protection law: UK Addendum to the EU Standard Contractual Clauses (SCCs) where applicable.

(c) Organisation name: Microsoft (SharePoint and Outlook)

(i) Category of recipient: Cloud storage and communication provider

(ii) Country the personal information is sent to: United States / EU

(iii) How the transfer complies with UK data protection law: The country or sector has a UK data bridge (also known as Adequacy Regulations)

(d) Organisation Name: Google (Google Forms)

(i) Category of Recipient: Data collection and storage provider

(ii) Country the Personal Information is Sent to: United States

(iii) How the transfer complies with UK data protection law: Addendum to the EU Standard Contractual Clauses (SCCs)

(e) Organisation Name: Slack

(i) Category of Recipient: Team communication provider

(ii) Country the Personal Information is Sent to: United States

(iii) How the transfer complies with UK data protection law: Addendum to the EU Standard Contractual Clauses (SCCs)

(f) Organisation name: Dropbox

(i) Category of recipient: Cloud storage and file sharing provider

(ii) Country the personal information is sent to: United States

(iii) How the transfer complies with UK data protection law: Addendum to the EU Standard Contractual Clauses (SCCs)

(g) Organisation name: Google (Google Drive)

(i) Category of recipient: Cloud storage and collaboration provider

(ii) Country the personal information is sent to: United States

(iii) How the transfer complies with UK data protection law: Addendum to the EU Standard Contractual Clauses (SCCs)

(h) Organisation name: Microsoft (SharePoint)

(i) Category of recipient: Cloud storage and document management provider

(ii) Country the personal information is sent to: United States and EU (if EU data centre selected)

(iii) How the transfer complies with UK data protection law: Addendum to the EU Standard Contractual Clauses (SCCs)

(i) Organisation name: Microsoft (Outlook)

(i) Category of recipient: Email and calendar service provider

(ii) Country the personal information is sent to: United States and EU (if EU data centre selected)

(iii) How the transfer complies with UK data protection law: Addendum to the EU Standard Contractual Clauses (SCCs)

(j) Organisation name: Stripe

(i) Category of recipient: Payment processing provider

(ii) Country the personal information is sent to: United States

(iii) How the transfer complies with UK data protection law: Addendum to the EU Standard Contractual Clauses (SCCs)

(k) Organisation name: PayPal

(i) Category of recipient: Payment processing provider

(ii) Country the personal information is sent to: United States

(iii) How the transfer complies with UK data protection law: Addendum to the EU Standard Contractual Clauses (SCCs)

(l) Organisation name: Hubdoc

(i) Category of recipient: document management and data extraction platform

(ii) Country the personal information is sent to: United States

(iii) How the transfer complies with UK data protection law: Addendum to the EU Standard Contractual Clauses (SCCs).

(m) Organisation name: LinkedIn (Microsoft)

(i) Category of recipient: Professional networking and recruitment platform

(ii) Country the personal information is sent to: United States

(iii) How the transfer complies with UK data protection law: Addendum to the EU Standard Contractual Clauses (SCCs)

(n) Organisation name: Facebook (Meta)

(i) Category of recipient: Social media and advertising provider.

(ii) Country the personal information is sent to: United States

(iii) How the transfer complies with UK data protection law: Addendum to the EU Standard Contractual Clauses (SCCs)

(o) Organisation name: X (formerly Twitter)

(i) Category of recipient: Social media and advertising provider.

(ii) Country the personal information is sent to: United States

(iii) How the transfer complies with UK data protection law: Addendum to the EU Standard Contractual Clauses (SCCs)

(p) Organisation name: Instagram (Meta)

(i) Category of recipient: Social media and advertising provider.

(ii) Country the personal information is sent to: United States

(iii) How the transfer complies with UK data protection law: Addendum to the EU Standard Contractual Clauses (SCCs)

(q) TikTok:

(i) Category of recipient: Social media and advertising provider.

(ii) Country the personal information is sent to: United States and China

(iii) How the transfer complies with UK data protection law: Standard Contractual Clauses with supplementary measures.

(r) Youtube (Google):

(i) Category of recipient: Social media and advertising provider.

(ii) Country the personal information is sent to: United States

(iii) How the transfer complies with UK data protection law: Addendum to the EU Standard Contractual Clauses (SCCs).

(s) Bubble

(i) Category of recipient: No-code application development platform

(ii) Country the personal information is sent to: United States

(iii) How the transfer complies with UK data protection law: Addendum to the EU Standard Contractual Clauses (SCCs)

(t) Zapier

(i) Category of recipient: Automation and integration platform

(ii) Country the personal information is sent to: United States

(iii) How the transfer complies with UK data protection law: Addendum to the EU Standard Contractual Clauses (SCCs) / UK Extension to the EU-US Data Privacy Framework

9.3 Where necessary, our data processors may share personal information outside of the UK. When doing so, they comply with the UK GDPR, making sure appropriate safeguards are in place.

9.4 For further information or to obtain a copy of the appropriate safeguard for any of the transfers above, please contact us using the contact information provided above.

10 How to complain

10.1 If you have any concerns about our use of your personal data, you can make a complaint to us using the contact details at the top of this privacy notice.

10.2 If you remain unhappy with how we've used your data after raising a complaint with us, you can also complain to the ICO.

10.3 The ICO's address:

(a) Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

10.4 Helpline number:

(a) 0303 123 1113

10.5 Website:

(a) https://www.ico.org.uk/make-a-complaint

11 Last updated: October 2026