

Data Protection Policy

Last reviewed 2023

Contents

1. Introduction and status of this policy	3
2. Data Protection Principles	3
3. Personal data processed by Youth Music	3
4. Principle 1 - Fair, lawful and transparent processing.....	4
Legal basis	4
Transparency.....	4
5. Principle 2 - Processing data for the original purpose	5
6. Principle 3 - Personal data should be limited to what is necessary.....	5
7. Principle 4 - Accuracy of data.....	6
8. Principle 5 - Retention of data	6
9. Principle 6 – Data Security	6
10. Consent	7
Recording consent	7
11. Data subjects’ rights.....	8
12. Beneficiaries and grant organisations.....	8
13. Communications with contacts and supporters	8
Business Cards.....	9
14. Higher-risk processing.....	9
15. Sensitive personal data	9
16. Sharing data with third parties	10
17. Transferring data outside the EEA	11
18. The Information Commissioner’s Office	11
Monitoring and review of the policy	11
Schedule 1: Definitions	11
Schedule 2: Data subjects' rights	14
Schedule 3: Data Processing Agreement minimum requirements under GDPR.....	18

1. Introduction and status of this policy

- 1.1. Youth Music is committed to complying with privacy and data protection laws. The main legislation is the General Data Protection Regulation (“GDPR”) and the Privacy and Electronic Communications Regulations 2003 (“PECR”) (which is particularly relevant to electronic direct marketing).
- 1.2. This is an internal policy. Anyone who handles personal data in any way on behalf of Youth Music must ensure that they comply with this policy. Any breach of this policy will be taken seriously and may result in disciplinary action or more serious sanctions.
- 1.3. This policy may be amended from time to time to reflect changes in the law or in internal policy. As a staff member or trustee of Youth Music, it is your responsibility to familiarise yourself with this policy and to check it periodically.
- 1.4. Please familiarise yourself with the important definitions in Schedule 1, including in particular the definitions of personal data and of processing.

2. Data Protection Principles

Anyone processing data must comply with the seven data protection principles set out in the GDPR. Youth Music is required to comply with these principles, summarised below. Personal data should be:

- a) processed fairly, lawfully and transparently;
- b) collected for specified, explicit and legitimate purposes (you should be clear with the individuals how you will be using the data you collect) and not processed in a way which is incompatible with those purposes;
- c) adequate, relevant and limited to what is necessary for the purposes for which it is held;
- d) accurate and, where necessary, kept up to date;
- e) kept for no longer than is necessary; and
- f) processed in a manner that ensures appropriate security of the personal data.
- g) The Data Controller (Youth Music) is required to comply, and be able to demonstrate compliance, with these principles (including appropriate record keeping).

3. Personal data processed by Youth Music

The types of personal data that Youth Music may handle include information about current, past and prospective (and unsuccessful applicants where relevant):

- a) Employees (and trustees)
- b) Donors
- c) Contacts
- d) Network users

- e) Grant applicants and grant holders
- f) Grant beneficiaries, which may include children and young people.

And anyone else that we communicate with. These individuals are generally referred to as data subjects throughout this policy (see definitions).

4. Principle 1 - Fair, lawful and transparent processing

Legal basis

4.1 Processing will only be lawful where Youth Music can rely on at least one of the following lawful bases for each instance of processing:

- a) The data subject has given their consent (see section 10).
- b) The processing is necessary to perform a contract with the data subject.
- c) The processing is necessary to comply with a legal obligation on Youth Music.
- d) The processing is necessary to protect the “vital interests” of a data subject – vital means essential for the data subject’s life and so is likely to be relevant only in emergency medical situations.
- e) The processing is necessary for the performance of a task carried out in the public interest – this is unlikely to apply to the day-to-day work of Youth Music.
- f) The processing is necessary for the purposes of Youth Music, or a third party’s, legitimate interests – provided those interests are not overridden by the interests or rights and freedoms of the data subject.

4.2 Most of the processing Youth Music does will be on the basis of its legitimate interest. This requires us to balance our interest against the rights of the individual, taking into account their reasonable expectations as to how we will process their data. For processing that is particularly intrusive or unexpected, this may not be lawful.

4.3 In some cases, particularly where we are communicating with data subjects electronically, we may specifically require consent.

Transparency

4.4 Every time Youth Music collects personal data about a person directly from that data subject, which Youth Music intends to keep, we need to provide that person with a notice containing “fair processing information”. In other words we need to tell them:

- a) who we are and give our contact details;
- b) why we are collecting their personal data and what we intend to do with it e.g. to process donations or send mailing updates about our activities;
- c) our legal basis for collecting their information (see sections 4.1 – 4.3 above) – if we rely on the lawful basis of legitimate interests, those interests must be specified);

- d) whether the provision of their personal data is part of a statutory or contractual obligation and details of the consequences of the data subject not providing that data;
- e) the period for which their personal data will be stored (if it is not possible to give a finite period of time, it is acceptable to provide the criteria which will be used to decide that period – usually Youth Music uses criteria related to the purposes for which the personal data is collected/processed);
- f) the existence of the rights of data subjects (please see section 10 below for the rights that must be referred to);
- g) details of people/organisations, or categories of people/organisations, with whom we may share their personal data;
- h) if relevant, the fact that we will be transferring their personal data outside the EEA and details of relevant safeguards (see section 16 below);
- i) The right to lodge a complaint with the Information Commissioner’s Office;
- j) The right to withdraw consent if consent is the lawful ground that has been relied upon; and
- k) the existence of any automated decision-making, including behavioural profiling, involving their personal data (it is unlikely Youth Music will be undertaking automated decision making).

4.5 This should all be contained in Youth Music’s [Privacy Notice](#), which is available on its website and made available prior to any data subject providing us with their personal data or, where the personal data is collected from a third party, as soon as reasonably possible thereafter.

5. Principle 2 - Processing data for the original purpose

5.1 Personal data can only be processed for the specific, explicit and legitimate purposes determined when it is first collected, or for a compatible purpose.

5.2 This means that Youth Music should not collect personal data for one purpose and then use it for another incompatible purpose. If it becomes necessary to process a person’s personal data for a new purpose, the individual should be informed of the new purpose beforehand. For example, if Youth Music collects a contact number or email address, in order to update someone about our activities it should not then be used for any new purpose, for example to share it with other organisations for marketing purposes, without first getting the individual’s consent.

6. Principle 3 - Personal data should be limited to what is necessary

Personal data processed by Youth Music should be limited to what is necessary in relation to the purposes for which it is processed. This means that - considering the purposes specified in our Privacy Notice - we can only collect the amount/type of personal data that is strictly necessary to achieve the purpose(s) in question.

7. Principle 4 - Accuracy of data

Youth Music is required to take reasonable steps to ensure that inaccurate personal data is corrected and that out of date personal data is updated – [our Privacy Notice sets out means for data subjects to do this, but] if you are aware that any personal data processed by Youth Music is inaccurate and/or out of date, please take steps to amend it accordingly and record those steps and the fact that the personal data has been amended.

8. Principle 5 - Retention of data

8.1 Youth Music must not keep personal data for longer than required for the purpose for which it was collected. This means that the personal data that Youth Music holds should be destroyed/erased from our systems when it is no longer needed.

8.2 For guidance on how long particular types of personal data that Youth Music collects should be kept before being destroyed/erased, please contact Angela Linton. As a general rule:

- a) Contact information should be kept for 3 years following the last contact or engagement.
- b) Financial records should be kept for 6 years from the end of the relevant financial year (e.g. the year in which a one-off donation is made, a direct debit is cancelled, or the relevant payroll year in the case of P45s etc.).
- c) Other personnel records shall be retained for no more than 3 years following termination of employment.

9. Principle 6 – Data Security

9.1 Youth Music must keep secure any personal data that it holds, using “organisational” and “technical” measures. Organisational measures include training and the use of this policy. Technical measures include IT measures such as anti-virus software.

9.2 Youth Music currently has the following security procedures and monitoring processes that must be followed at all times:

- a) Databases should only be accessed via Youth Music’s servers which are subject to the charity’s general privacy and password protections, or via the secure servers of its approved suppliers with whom Youth Music has a compliant contract (see Section 16).
- b) Contact lists should be:
 - i. password protected before being sent to a third party (e.g. mailing house);
 - ii. not be retained in the employee’s general files;
 - iii. any copies deleted once you have completed your work on the list;
 - iv. not be put on unencrypted memory sticks

- c) Personal data should not be emailed to home computers or other networks that may lack the required level of security, or to third parties with whom we do not have a compliant data processing agreement.
- d) Personnel records can only be accessed on request to the Chief Operating Officer, the Chief Executive, or the line manager of the relevant employee.
- e) Staff/trustees should ensure that individual monitors do not show confidential information or sensitive personal data to passers-by and that they log off or lock their computer when it is left unattended.
- f) Printed documents should be shredded and electronic documents securely erased when they are no longer required.
- g) Desks and cupboards should be kept locked if they hold confidential or sensitive personal data.
- h) Staff must keep data secure when travelling or using it outside the offices.
- i) [Regular back-ups should be taken of all data on the system and storing data on local drives or removable media should be avoided where possible, as these will not be backed up.]
- j) [If you are working from home, you should ensure that the laptop or computer you are using is securely protected from theft while you are away from it.]

10. Consent

10.1 In some cases, such as to send electronic direct marketing (see section 13, or to process sensitive personal data, Youth Music must have obtained the consent of individuals to process their data.

10.2 To be valid, consent must be:

- a) Freely given
- b) Specific
- c) Informed
- d) Unambiguous
- e) A statement or clear affirmative action

10.3 In practice this means that (a) we must provide clear and comprehensive information about the consent we are seeking and (b) there must be a clear indication of consent, such as an affirmative response or a tick in a box.

Recording consent

10.4 We must keep records so we can demonstrate that we have adequate consent if necessary (i.e. who consented, when and how the consent was obtained, and what they were told their consent was for). Our process for contacts is to annotate our contact list with a cross reference to the date consent was obtained, as well as the specific form or method used to obtain the consent (e.g. Cambridge Headphones 2016) so that we can show what was agreed to. Consent information for data subjects related to grants administration is stored

on the grant management database.

11. Data subjects' rights

11.1 GDPR gives data subjects a number of specific rights in relation to organisations' use of their personal data (for example, a 'subject access' right to a copy of the data they hold). They can exercise these rights by contacting the charity, and everyone who processes data on behalf of Youth Music should be aware of these rights and recognise when a request has been made.

11.2 These rights are listed and explained in Schedule 2.

12. Beneficiaries and grant organisations

12.1 Sometimes, grant recipients will provide us with personal data in respect of individual beneficiaries. For example: in individual case studies or photographs.

12.2 Our grant agreements require the grant recipient to comply with data protection laws, and to have its own, clear data protection policy.

12.3 Where we are provided with information in case studies and photographs, which contain personal data, we take steps to ensure the grant recipient has consent from the individual to share this information with us.

12.4 Where this includes children's personal data, we must ensure that we have parental/legal guardian consent for children (under 16).

12.5 Email addresses and other personal data relating to grantees should be purged from the grants database at regular intervals according to the timelines shown in clause 8.2.

13. Communications with contacts and supporters

13.1 "Direct Marketing" has a wide definition and will include any communications that promote Youth Music's aims and ideals, including fundraising materials, newsletters, and invitations to events. There are specific rules we must comply with when sending direct marketing communications.

13.2 People have the right to ask us to stop processing their data for direct marketing – we should record all as "do not contact" on our system and comply with these requests within 28 days.

13.3 When adding contacts to our databases, we must ensure that they are notified of who we are and how we will use their data – see section 4.4.

13.4 The Code of Fundraising Practice requires us to include an "opt-out" statement on every fundraising communication, the same size as the donation amount or, if none, minimum font size 10. For example: "To opt-out of receiving these communications, please [reply to this email indicating "unsubscribe" in the subject box] OR [click here]."

13.5 By post – we do not require consent, but individuals still have a right to ask organisations to

stop processing their data for direct marketing, as above. You should also not send unsolicited direct mail by post to anybody registered with the MPS (Mailing Preference Service).

13.6 By email or SMS – Youth Music must have consent (see section 10) before making this kind of approach by email, and all such emails must include a clear opt-out/unsubscribe option.

13.7 By telephone – You should never make marketing telephone calls to an individual who has told Youth Music they do not want calls from us, or to numbers listed on the TPS (Telephone Preference Service) (unless we have specific consent, which can override the TPS).

13.8 The new Fundraising Preference Service (FPS) has now been launched. More information can be found here. We must comply with the FPS by ensuring that we comply with any notifications from the FPS that a supporter has opted-out of marketing communications from Youth Music (and marking on the system as a “do not contact”).

Business Cards

13.9 Contact information is often collected from business cards when networking and in other contexts. This is acceptable; we are able to contact these individuals in a business to business context (whereas for personal contacts we would require consent – as above in section 10). However, we must ensure that:

- a) It is clear from what is said between you that you intend to use the business card to contact them (e.g. “would you like to be included on our mailing list?”)
- b) On sending the first communication to them, signpost to our Privacy Notice (by link in an email, or by attaching a copy to an email or letter), and include an option to opt-out.

14. Higher-risk processing

Certain processing undertaken by charities has been the subject of much scrutiny and in some cases investigations and fines by the ICO.² It is Youth Music policy not to undertake the following types of processing without the express consent of the Chief Executive Officer or Chief Operating Officer:

- a) Profiling contacts;
- b) Wealth screening;
- c) Sharing marketing lists with third parties;
- d) Data matching (e.g. matching contact lists against telephone databases to obtain further information the data subject did not provide us with).

15. Sensitive personal data

15.1 On some occasions Youth Music may collect information that is defined by the GDPR as special categories of personal data (also known as “sensitive personal data”), and special rules will apply to the processing of this data. The categories of sensitive personal data are set out in the definition in Schedule 1.

15.2 Financial information is not defined as sensitive personal data by the GDPR, but particular care should be taken when processing such data, as the ICO will treat a breach relating to financial data very seriously. Data about criminal offences is also subject to stricter rules. Grantee bank account information stored electronically in the grants management database cannot be accessed outside of the organisation's servers.

15.3 To process sensitive personal data, Youth Music must, in addition to meeting one of the legal bases in Section 4.1, also satisfy one of the following conditions (there are others but these are the most relevant to our work):

- a) explicit consent of the data subject;
- b) processing in compliance with employment law obligations;
- c) vital interests (usually, life or death) of the data subject;
- d) information made public by the data subject; and
- e) legal advice and establishing/defending legal rights.

15.4 Please note that (i) depending on the circumstances, there may be other conditions available and (ii) the conditions above are only available in limited circumstances. If you have any doubts as to the availability of the conditions, or whether/how a condition can be relied on, please contact Angela Linton in the first instance.

16. Sharing data with third parties

16.1 Youth Music uses third party suppliers, who are data processors (see definition), to carry out certain data processing activities on its behalf – for example, payroll service providers.

16.2 Youth Music can engage data processors, and share data with them, provide we comply with some specific obligations:

- a) We must be satisfied that the data processor offers sufficient guarantees to keep data secure and protect data subjects' rights. If you have any doubt over our third party suppliers, please contact Angela Linton.
- b) We must have a written agreement in place which sets out (i) the subject matter, duration, nature and purpose of the processing; (ii) the types of personal data and (iii) the categories of data subjects whose data will be processed.
- c) The contract must include the provisions set out in Schedule 3.

16.3 Youth Music can also share personal data when required to comply with a legal obligation – for example, reporting to its regulators or bodies such as HMRC.

16.4 Before introducing two business contacts to each other by email, you must ask first whether they are happy for you to do so in principle – i.e. you should obtain their consent.

16.5 Do not share data with a third party without the express consent of the Chief Executive Officer or the Chief Operating Officer, and unless standard form contracts, approved by the Chief Operating Officer, are in place.

16.6 It is Youth Music policy not to share data with third parties for the purposes of profiling,

wealth screening, sharing marketing lists or data matching (e.g. matching contact lists against telephone data bases etc.). See Section 15.

17. Transferring data outside the EEA

17.1 When organisations transfer personal data outside the EEA or other countries specified by the European Commission, they take steps to ensure that the data is properly protected. For us, this is most likely to occur if we are using a data processor that is based, or has its servers, outside the EEA.

17.2 Ensuring the data is properly protected, in practice, usually means it will be necessary to enter into an EC-approved agreement, OR seek the explicit consent of the data subject, OR rely on one of the other derogations under the GDPR that apply to the transfer of personal data outside the EEA. If you know or become aware that personal data will be transferred outside the EEA, please speak Angela Linton before carrying out any such transfer.

18. The Information Commissioner's Office

18.1 There is no obligation for Youth Music to make an annual notification to the ICO under the GDPR. There may be a requirement to pay an annual fee to the ICO.

18.2 Youth Music must report data security breaches (other than those which are unlikely to be a risk to individuals) to the ICO, usually within 72 hours of becoming aware of the breach. A data security breach may have occurred where personal data has been compromised in some way (for example misplacing a laptop in a public place which contains personal data).

18.3 Youth Music is required to notify affected data subjects where the breach is likely to result in a high risk to their rights and freedoms. This notification may not be required in certain circumstances where the personal data is encrypted or Youth Music has taken subsequent measures to ensure that the high risk to data subjects is not likely to materialise.

18.4 If you think a data security breach has occurred, or you are unsure, please immediately notify Angela Linton, Chief Operating Officer on 020 7902 1095 or email: angela.linton@youthmusic.org.uk

Monitoring and review of the policy

- Reviewed by F&A: 27 February 2018
- Ratified by Board of Trustees: 3 April 2018
- This policy will next be reviewed by F&A: October 2019
- Review cycle: annually

Schedule 1: Definitions

data subjects include all living individuals in the EU about whom Youth Music holds personal data, for instance an employee, donor or contact. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.

personal data means any information relating to a living person who can be identified directly or indirectly from that information (or from that information combined with other information in our possession). Personal data can be factual (such as a name, address or date of birth) or can be an opinion (such as a performance appraisal).

Examples of the types of personal data processed by Youth Music are as follows:

- 1) Full names of, for example, employees, donors, contacts, network users and beneficiaries;
- 2) Contact details, such as postal addresses, telephone numbers and email address;
- 3) Financial information, such as credit/debit card details;
- 4) Personal descriptions/photographs;
- 5) Any other information shared with us by/collected in relation to data subjects which satisfies the definition of “personal data”.

Sensitive Personal Data (which is defined as “special categories of personal data” under the GDPR) includes information about a person's:

- a) racial or ethnic origin;
- b) political opinions;
- c) religious, philosophical or similar beliefs;
- d) trade union membership;
- e) physical or mental health or condition;
- f) sexual life or orientation;
- g) genetic data;
- h) biometric data; and
- i) such other categories of personal data as may be designated as “special categories of personal data” under the legislation.

Data Controllers are the people or organisations that decide the purposes and the means for which any Personal Data is processed. They have a responsibility to process personal data in compliance with the legislation. Youth Music is the data controller of all personal data that processed in connection with our work and activities.

Data Processors are any person or organisation that processes personal data on behalf of a data controller (excluding employees). This could include suppliers such as website hosts, payroll providers or others, for example third party payment processing service providers. Processors also have obligations under the legislation.

European Economic Area (or EEA) includes all countries in the European Union as well as Norway, Iceland and Liechtenstein.

Information Commissioner’s Office (or ICO) (the regulatory authority which oversees data protection regulation in the UK).

Processing is any activity that involves use of personal data, whether or not by automated means. Its definition is very broad, and includes but is not limited to collecting, recording, organising, structuring, storing, adapting or altering, retrieving, disclosing by transmission, disseminating or otherwise making available, alignment or combination, restricting, erasing or destruction of personal data.

Schedule 2: Data subjects' rights

Right	Explanation	Practical guidance
Right of Access	<p>The right to:</p> <ul style="list-style-type: none"> - confirm whether Youth Music is processing their personal data; and - request a copy of that personal data; or - (on the rare occasions that Youth Music is processing their data for another), obtain information about the purposes and manner of the processing. 	<p>Make a note of when the request has been made. We must provide the information within 1 month (2 months if the request is complex and we have told them of our intention to extend). We cannot charge a fee unless the requests are “manifestly unfounded or excessive” – which is a high threshold.</p>
Right to Rectification	<p>The right to have inaccurate or incomplete personal data amended.</p>	<p>Make a note of when the request has been made. We must reply within 1 month (2 months if the request is complex and we have told them of our intention to extend).</p>
Right to Erasure	<p>Also known as the right to be forgotten.</p> <p>The right to request that all their personal data is deleted or removed from our systems where there is no compelling reason for its continued processing. The right is only available where:</p> <ul style="list-style-type: none"> a) It is no longer necessary for us to process the personal data in relation to the purpose for which it was originally collected/processed. b) The only lawful basis for processing the personal data was consent and the data subject withdraws that consent. c) The data subject objects to the processing and there is no overriding legitimate interest for continuing the processing. d) The personal data was unlawfully processed. e) The personal data has to be erased to comply with a legal obligation. f) The personal data is processed in relation to the offer of information society services to a child. An information society service is any 	<p>There are exceptions which can allow us to refuse to comply with a request for erasure. These exceptions apply where the personal data in question is processed:</p> <ul style="list-style-type: none"> a) so that we can exercise the right of freedom of expression and information. b) so that we can comply with a legal obligation for the performance of a task in the public interest or in the exercise of official authority. c) for public health purposes in the public interest. d) for archiving purposes in the public interest; scientific or historical research or statistical purposes; or e) the exercise or defence of legal claims <p>If you receive a request for erasure, and consider that Youth Music must comply, please check whether personal data in question has been disclosed to any third parties – we may need to</p>

	<p>online service normally provided for remuneration, made at the individual request of the recipient of a service.</p> <p>If the above categories involve processing that causes unwarranted and substantial damage or distress to the data subject, this will likely make the case for erasure stronger.</p>	<p>request that they also delete the data.</p>
Right to Restrict Processing	<p>The right to block/suppress processing of personal data in certain circumstances.</p> <p>The right only applies in the following personal circumstances:</p> <ul style="list-style-type: none"> a) Where a data subject contests the accuracy of personal data, you should restrict any further processing operations in relation to that personal data until we have verified its accuracy. b) Where an individual has objected to the processing (see below) and we are considering whether we have legitimate grounds to refuse the request. c) When the processing in question is unlawful but the data subject prefers restriction as the solution instead of erasure. d) Where Youth Music no longer requires the personal data, but the data subject requires the data to establish, exercise or defend a legal claim. 	<p>When the right is exercised, Youth Music can continue to store the personal data, but engage in no other form of processing. Youth Music can store only enough personal information about the data subject such that the restriction can be respected in the future.</p> <p>Where we have disclosed the personal data in question to a third party, Youth Music obliged to inform them about the restriction on the processing of the personal data, unless to do so is impossible or involves disproportionate effort. Please therefore consider whether we have disclosed the personal data in question to a third party.</p>
Right to data portability	<p>Data subjects are entitled to obtain and reuse their personal data across different services. This right therefore allows them to move, copy or transfer their personal data easily from one IT system to another in a smooth, safe and secure way.</p> <p>The right only applies where:</p> <ul style="list-style-type: none"> a) the data subject in question has provided the personal data in question to Youth Music 	<p>This is highly unlikely to apply to Youth Music given it only applies where there is “automated” processing (e.g. it is relevant to credit agencies where the data is processed by a computer algorithm to produce a credit score).</p> <p>If the unlikely event you receive a request to port data, consider taking legal advice.</p>

	<p>(i.e. directly);</p> <p>b) where our lawful basis for processing is either consent or for the performance of a contract; and</p> <p>c) where the processing in question is carried out by automated means (highly unlikely to apply to Youth Music’s processing).</p>	
<p>Right to object</p>	<p>The right to object to the processing of personal data in three different circumstances. These are where:</p> <ol style="list-style-type: none"> 1. Youth Music is relying on its legitimate interests to process the data; <p>In this case we must stop processing their personal data unless:</p> <ol style="list-style-type: none"> i. Youth Music can demonstrate compelling legitimate grounds for continuing the processing, which override the interests, rights and freedoms of the data subject; or ii. the processing is for the establishment, exercise or defence of legal claims. <ol style="list-style-type: none"> 2. Youth Music is processing their data for purposes of direct marketing. <p>In this case as we receive an objection, processing for the purposes of direct marketing must stop – there are no exemptions or grounds to refuse to comply.</p> <ol style="list-style-type: none"> 3. Youth Music is processing their data for the purposes of scientific or historical research and statistics. <p>To exercise this right, data subjects must show that their objection is based on grounds relating to his or her particular situation. If they can do this, then Youth Music must stop the processing, unless it is</p>	<p>If you receive an objection to direct marketing, you must adhere to the “opt out”.</p> <p>If you receive a broader objection to processing, speak to Angela Linton in the first instance.</p> <p>c) is highly unlikely to apply to Youth Music’s work.</p>

	conducting research where the processing of personal data is necessary for the performance of a task in the public interest, in which case we may continue the research in question.	
Rights related to automated decision making (including profiling)	<p>The GDPR contains provisions which apply to “automated decision making”. The ICO’s guidance on this, including the definition of “automated decision making”, can be found here.</p> <p>Automated decision making is, broadly, decision making without any human involvement.</p>	These are unlikely to be relevant to Youth Music’s current activities, but this should be reconsidered whenever this policy is reviewed.
Right to lodge a complaint with the ICO	A general right to lodge a complaint with the ICO about any aspect of Youth Music’s use of their personal data.	<p>Youth Music provides the ICO’s contact details in its privacy notice.</p> <p>Any communications we receive from the ICO should be directed to Angela Linton.</p>
Right to withdraw consent	Where our processing is done solely on the basis of consent – for example, in relation to direct marketing.	<p>Youth Music informs data subjects of this right in its privacy notice and should do so whenever it collects consent.</p> <p>If you are obtaining a data subject’s consent, please make sure they are expressly informed about their right to withdraw this consent at any time.</p> <p>If a request to exercise this right is received, please contact Angela Linton immediately.</p>

Schedule 3: Data Processing Agreement minimum requirements under GDPR

In relation to the data processor (i.e. the third party supplier/contractor who is processing data on behalf of Youth Music), the agreement must provide:

1. that the data processor will not engage another data processor (i.e. subcontract) without the prior written authorisation of Youth Music;
2. that the data processor will only process personal data based on documented instructions from Youth Music;
3. that the person(s) authorised to process the personal data on Youth Music's behalf (e.g. the processor's employees) commit to the confidentiality of the personal data;
4. that the data processor will take organisational and technical security measures appropriate to the nature, scope, context and purposes of processing, the type(s) of personal data involved and the associated risks to data subjects;
5. that the data processor will facilitate Youth Music's obligations to comply with data subjects' request to exercise their rights;
6. that, bearing in mind the nature of the processing and information available to the data processor, the data processor will assist Youth Music in complying with the following obligations:
 - a) its security obligations;
 - b) its obligation to report security breaches – in particular, the data processor must notify us without undue delay after becoming aware of a security breach and, where appropriate, must provide information as to the nature of the breach, the categories and approximate numbers of data subjects involved and the measures taken to mitigate potential adverse effects; and
 - c) where appropriate, conducting a data protection impact assessment ("DPIA") and/or consulting with the ICO prior to commencing processing likely to result in a high-risk to the rights and freedoms of natural persons;
7. that the data processor is obliged, at the choice of Youth Music, to delete or return all the personal data concerned to Youth Music at the end of the provision of data processing services; and
8. makes available to Youth Music all information necessary to demonstrate compliance with obligations under the legislation.

YOUTH MUSIC

THE NATIONAL FOUNDATION FOR YOUTH MUSIC
STUDIO LG01, THE PRINT ROOMS
164-180 UNION STREET, LONDON, SE1 0LH

REGISTERED CHARITY NUMBER: 1075032
LIMITED COMPANY NUMBER: 3750674