Data Protection Policy

Version number 2
Last updated 17 December 2020

Definitions

SMART	means SMART (Suffolk Music & Arts Alumni Trust), registered charity number 1177728.
GDPR	means the General Data Protection Regulation.
Personal Data	means any information relating to an identified or identifiable individual, such as name and contact details. Some private information, such as race or ethnic origin, health data, sexual orientation or criminal behaviour is "special category" data and subject to more stringent requirements.
Processing	means any action involving personal data, including collecting, using, accessing, viewing and even deleting them.
Responsible Person	means the Trustee Compliance Officer - Rebecca Reidy (admin@suffolksmart.org)

1. Introduction and data protection principles

a. This document records the data protection framework established by the Trustees of SMART. The Trustees are committed to managing personal data in a professional, lawful and ethical way.

b. The Trustees recognise that part of their role as Trustees will involve processing

personal data. The Trustees are the data controller in relation to all personal data processed by SMART and the Trustees. As such, the Trustees are responsible for, and must be able to demonstrate compliance with, the principles for processing of personal data set out in Article 5 of GDPR, as set out in Appendix 1.

c. In line with the requirements of Article 30 of GDPR, this document records the Trustees' processing activities that are not occasional, are likely to result in a risk to the rights and freedoms of individuals, or involve special category data.

2. General provisions

a. This policy applies to all personal data processed by SMART and the Trustees regardless of the media on which that data is stored.
b. The Responsible Person shall take responsibility for SMART and the Trustees' ongoing compliance with this policy.
c. This policy shall be reviewed at least annually.
d. The Trustees shall register SMART with the Information Commissioner's Office as an organisation that processes personal data.

3. Lawful, fair and transparent processing

a. To ensure SMART's processing of data is lawful, fair and transparent, the Trustees shall maintain at Appendix 2 a register of all systems or contexts in which personal data is processed by the Trustees, including the main purposes of processing, categories of data subject and categories of personal data processed.
b. The Trustees process personal data in order to administer and manage membership of SMART and to manage applications for funding from potential and existing beneficiaries of SMART.
c. The Trustees and SMART use personal data for the following purposes:
    i. To deal with enquiries about SMART and its work
    ii. To correspond with non-member supports about SMART's work
    iii. To process donations towards SMART's work
    iv. To administer membership applications and communicate with members about SMART membership / SMART's work / SMART social and fundraising events
    v. To assess applications for funding from potential beneficiaries
    vi. To process Trustee nominations
    vii. To communicate with Trustees
    viii. To publish member profiles on SMART's website
    ix. To communicate with regional alumnus groups and coordinating get-togethers, support/friendship to those new to an area and arranging fundraising events
    x. In publicity about SMART's work
    xi. Complying with any present or future laws or regulations applicable to SMART.
d. Individuals have the right to access their personal data and any such requests made to SMART shall be dealt with in a timely manner.

4. Lawful basis for processing

a. The Trustees process personal data on the following grounds:

i. the data subject has given explicit consent to the processing (GDPR Article 6(1)(a)) (this is a requirement in relation to special category data); and/or
ii. the processing is necessary for the performance of contractual obligations to which the data subject is a party, or at the data subject's request prior to entering a contract (GDPR Article 6(1)(b)); and/or
iii. the processing is necessary for compliance with a legal obligation to which the Trustees are subject (GDPR Article 6(1)(c)); and/or
iv. the processing is in the legitimate interests of the Trustees for the purposes described in (3) above and those interests are not overridden by the interests or fundamental rights and freedoms of the data subject (GDPR Article 6(1)(f)).

a. Appendix 2 sets out the appropriate lawful basis for each category of personal data processed by the Trustees.
b. In most cases, the processing undertaken by the Trustees and other processors on behalf of SMART is in the legitimate interest of the Trustees as data controller. In some cases an alternative or additional ground may apply.
c. Where processing is carried out in the legitimate interests of the Trustees, the Trustees have identified the relevant legitimate interests, have identified that the processing is necessary to achieve the legitimate interests**,** and understand that they must balance SMART's legitimate interests against the interests, rights and freedoms of data subjects.
d. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
e. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent shall be clearly available and SMART shall have systems in place to ensure such revocation is reflected accurately in the personal data held.

5. Data minimisation

a. The Trustees shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

6. Accuracy

a. The Trustees shall take reasonable steps to ensure personal data is accurate.
b. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

7. Disclosure and transfers of personal data: categories of recipient

a. The Trustees may share or disclose personal data to any of the following recipients, where relevant:

i. We use Mailchimp's email marketing tool, so we draw your attention to their Privacy Policy**.** Mailchimp also deploy cookies and similar tracking technologies (like web beacons or pixels) lawfully on and collect data in accordance with and as described in their Cookie Statement.

ii. Our website provider is Wix, so we draw your attention to Wix's Privacy

Policy. Wix also uses cookies as set out in their Privacy Policy.

iii. We also use Paypal for payment processing and Membermojo for our membership database. We do not transfer data to these parties as any information is provided directly by you.

b. The Trustees have identified the following situations where personal data may be transferred, stored or proceed at a destination outside the European Economic Area:

i. Mailchimp, who provide our email marketing tool, have servers located in the US. Mailchimp certifies compliance with the EU-US Privacy Shield framework, so can lawfully receive EU data.

ii. Wix, our website provider, have servers located in the US and Israel as well as Europe. Wix certifies compliance with the EU-US Privacy Shield framework, so can lawfully receive EU data. Israel is considered by the European Commission to be offering an adequate level of protection for the Personal Information of EU Member State residents.

8. Archiving / removal

a. To ensure that personal data is kept for no longer than necessary, the Trustees shall set a data retention policy for each area in which personal data is processed and review this process annually. This is set out in Appendix 2.
b. The data retention policy shall consider what data should/must be retained, for how long, and why.
c. Where data retention is no longer required, data will be securely and irreversibly deleted. Where applicable, the Trustees also require third parties to delete such data.

9. Security

a. The Trustees implement and maintain reasonable and appropriate security procedures and safeguards to prevent unauthorised access to personal data held by SMART and the Trustees.
b. Access to personal data shall be limited to personnel who need access and appropriate security shall be in place to avoid unauthorised sharing of information. Data is anonymised wherever possible.
c. When personal data is deleted this should be done safely such that the data is irrecoverable.
d. Appropriate back-up and disaster recovery solutions shall be in place.

11. Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, the Trustees have put in place procedures to promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO and/or to notify data subjects. A summary of the process can be found at Appendix 3.

Appendix 1

Principles relating to processing of personal data

The Trustees shall be responsible for, and be able to demonstrate compliance with Article 5 GDPR (**accountability**).

Article 5 of GDPR requires that personal data shall be:

a. processed lawfully, fairly and in a transparent manner in relation to individuals (**lawfulness, fairness and transparency**);

b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (**data minimisation**);

d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (**accuracy**);

e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals (**storage limitation**); and

f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (**integrity and confidentiality**)

Appendix 2

Register of all systems or contexts in which personal data is processed by SMART and details of lawful basis on which such data is processed and retention periods

Purposes of processing	Categories of individuals	Categories of personal data (key elements)	Systems used (including details of where data is located and stored)	Lawful basis for processing	Retention period
Enquiring about SMART and its work	Potential supporters and members	Personal and contact details, email message	Google drive, Google email account (@suffolksmart.org)	Legitimate interests	Up to 1 year - annual review to delete data
Subscribing to email updates about our work	Non-member supporters	Personal and contact details	Google drive, Google email account (@suffolksmart.org), Mailchimp	Consent	Until consent is withdrawn
Making a donation	Supporters and members	Personal and contact details, financial information	Membermojo, PayPal, Google drive, Google email account (@suffolksmart.org)	Legitimate interests	6 years after the end of the tax year of the donation, as required by HMRC
Administering membership applications and communicating with members about SMART membership / SMART's work / SMART social and fundraising events	Members	Personal and contact details, years with Suffolk Youth Music, membership records	Google drive, Google email account (@suffolksmart.org), Membermojo, Mailchimp, Paypal, Wix website (suffolksmart.org)	Contract / Consent / Legitimate interests	6 years after the end of the tax year in which the final membership fee was paid, as required by HMRC
Website functionality	Potential supporters and members and potential beneficiaries	Website activity collected through cookies	Wix website (suffolksmart.org)	Consent	As set out in Wix Privacy Policy
Applying for funding from SMART	Potential beneficiaries	Personal and contact details, financial information, special category data	Google drive, Google email account (@suffolksmart.org)	Legitimate interests, and explicit consent in relation to special category data	Up to 3 years from date of application, to allow Trustees to ascertain if multiple applications made

Purposes of processing	Categories of individuals	Categories of personal data (key elements)	Systems used (including details of where data is located and stored)	Lawful basis for processing	Retention period
Communicating with beneficiaries awarded funding from SMART	Beneficiaries	Personal and contact details, financial information, special category data	Google drive, Google email account (@suffolksmart.org)	Legitimate interests, and explicit consent in relation to special category data	6 years after end of tax year in which final payment made to beneficiary
Nomination as a Trustee of SMART	Potential Trustees	Personal and contact details	Google drive, Google email account (@suffolksmart.org)	Legitimate interests	Up to 1 year - annual review to delete data
Communications with Trustees	Trustees	Personal and contact details	Google drive, Google email account (@suffolksmart.org)	Legitimate interests	Up to 1 year after Trustee resigns
Publishing member profiles on SMART's website	Members	Website profile information, photo	Membermojo, Wix website (www.suffolksmart.org)	Consent	Until consent is withdrawn
Communicating with regional alumnus groups and coordinating get-togethers, support/friendship to those new to an area and arranging fundraising events	Members	Personal and contact details	Google drive, Google email account (@suffolksmart.org), Membermojo	Consent	Until consent is withdrawn
Publicity about SMART's work and fundraising events	Members	Photos, videos of participation in SMART-related events	Google drive, Google email account (@suffolksmart.org), www.suffolksmart.org Wix website	Consent	Until consent is withdrawn

Personal and contact details may include: name, date of birth, email address, postal address, telephone or mobile number, social media contact details, regional area

Membership records may include information about start and end dates of membership

Financial information may include bank account and/or credit card details to process payments or administer funding grants, gift aid declaration

Website profile information may include information about your time with Suffolk Youth Music, the instrument(s) you play, your education and your career path and/or information about yourself and why you support SMART, and/or any personal website or social media page you want linked to your profile

Special category data may include information about race, ethnic origin, religion, health or other sensitive information, which applicants for funding may choose to disclose as being relevant to the reason they wish to seek funding.

Appendix 3

Data security breach response procedure

In the event of a security breach in relation to personal data for which the Trustees are responsible as data controller, the Trustees must assess the risks to data subjects and may be required to notify data protection authorities and affected data subjects. A security breach in this context means the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

Key actions must occur within 72 hours of the first point at which the data controller establishes with a reasonable degree of certainty that a security breach involving personal data has occurred. All actions must be completed as soon as reasonably possible

1. Initial risk assessment

If there is a reasonable basis to conclude that a security breach involving personal data has occurred, the Trustee Compliance Officer (Rebecca Reidy) (the breach officer) must be informed as soon as possible and in any event within 24 hours.

On becoming aware or being informed, with a reasonable degree of certainty, that a security breach involving personal data has taken place, the breach officer will immediately carry out an initial assessment of the risks associated with the breach. The breach officer will identify, so far as possible:

a. the nature of the incident
b. the type and number of data records potentially at risk
c. the categories and number of data subjects affected
d. the likely consequences of the security breach, including the sensitivity of the data and potential damage that could result from misuse of the data; and
e. any immediate actions to mitigate or remedy the breach.

Unless the breach officer determines that the breach is unlikely to result in a risk to data

subjects, he or she will, as a matter of urgency and in any event within 24 hours of commencing the above investigation, inform the Trustees and if appropriate seek legal advice. (More information is available on the ICO website.)

2. Investigation

The breach officer will document all activities, findings and actions forming part of the breach investigation and within 48 hours of becoming aware of the breach will prepare a response plan for the Trustees indicating what reporting and other mitigation/response actions are required.

The response plan will include arrangements for notifying the Information Commissioner's Office if the breach may result in a risk to data subjects. If the security breach is likely to result in a high risk to data subjects (for example, if it leaves them open to discrimination, fraud or financial loss), the response plan will include arrangements for notifying data subjects.

3. Response

The Trustees shall prioritise any actions identified in the response plan. In particular, the Trustees must notify the breach to the Information Commissioner's Office without undue delay and (where feasible) within 72 hours of the breach officer (or, if earlier, the Trustees as data controller) becoming aware of the breach, except where the breach is unlikely to result in a risk to the rights and freedoms of individuals.

If the breach creates a high risk for data subjects, the Trustees must notify affected data subjects without undue delay, describing the nature and likely consequences of the breach and measures to address it or to mitigate its potential adverse effects.

4. Record-keeping

The breach officer will ensure that records are maintained including:

a. the key facts and causes of the data security breach;
b. response measures taken and any contact with the Information Commissioner's Office and/or data subjects affected; and
c. any enhancement of technical, physical, organisational security and contractual measures or other steps (including training) to be taken in response to the breach.