Charitable Incorporated Organisation Name: SMILEZ (1187799)
Document Title: Data Protection Policy - GDPR
Document Version: Version 2

Policy Date: 24th January 2026
Policy Review Date: 23rd January 2029

---

1. Purpose

1.1 Smilez is committed to protecting the rights and privacy of individuals (data subjects) trustees, volunteers, supporters, beneficiaries and donors in accordance with UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, as amended.

1.2 We will be open and honest with individuals whose personal data we hold and we want our trustees and volunteers to be trained and supported so that they can handle personal data confidently and consistently.

1.3 This policy sets out how we make sure personal data is processed lawfully in accordance with GDPR principles.

2. Scope

2.1 This policy applies to all Smilez, trustees and volunteers. Compliance with it is a condition of being a trustee or volunteer.

2.2 The policy applies to Smilez, trustees and volunteers processing of data.

3. Training and acceptance of responsibilities

3.1 Trustees and volunteers will receive information and guidance about this policy and their responsibilities during induction to their roles and at least annually thereafter.

3.2 They will also be updated as and when regulations and / or advice is updated.

4. Training and acceptance of responsibilities

4.1 GDPR regulates the processing of personal data. It protects the rights and privacy of all living individuals (including children) for example by giving all individuals who are the subject of personal detail the general right of access to the personal data which relates to them.

4.2 Personal data is information relating to an individual and may be in hard or soft copy (paper / manual files, electronic records or photographs) and it may include facts or opinions about a person.

5. Responsibilities under the GDPR

5.1 Smilez is a data controller under the terms of GDPR. This means that the Charity is responsible for controlling the use and processing of personal data.

5.2 The charity has appointed a Trustee who is available to address any concerns regarding the data held by the charity and how it is processed and used.

5.3 The policy is approved by our Board of Trustees.

5.4 The nominated Trustee is responsible for all day-to-day data protection matters and for making sure all trustees and volunteers comply with the policy. Personal data is information relating to an individual and may be in hard or soft copy (paper / manual files, electronic records or photographs) and it may include facts or opinions about a person.

6. Fair and lawful processing

6.1 Smilez will process data fairly and lawfully in accordance with individuals' rights as prescribed under GDPR. These rights allow an individual to:

(a) withdraw consent to data processing at any time;

(b) receive certain information about the Smilez's data processing activities;

(c) request access to their personal data that we hold (see Subject Access Request below);

(d) prevent our use of their personal data for direct marketing purposes;

(e) ask us to erase their personal data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data

(f) restrict processing in specific circumstances;

(g) challenge processing which has been justified on the basis of our legitimate interests;

(h) request a copy of an agreement under which personal data is transferred outside the UK;

(i) prevent processing that is likely to cause them or anyone else damage or distress;

(j) be notified of a personal data breach which is likely to result in high risk to their rights and freedoms;

(k) make a complaint to the supervisory authority (the ICO); and

(l) in limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (see Data Portability below).

6.2 The identity of an individual requesting data under any of the rights listed above should be verified before any data is disclosed. No data will be disclosed to a third party without proper authorisation.

7. Conditions for processing

7.1 We will ensure any use of personal data is justified using at least one of the conditions of processing permitted under GDPR and this will be specifically documented. The conditions of processing will be available to individuals in the form of a privacy notice.

7.2 The most applicable conditions for processing for Smilez are:

(a) the data subject has given his or her consent;

(b) the processing is necessary for the performance of a contract with the data subject;

(c) to meet our legal compliance obligations;

(d) to protect the data subject's vital interests; and

(e) to pursue our legitimate interests for purposes where they are not overridden because the processing prejudices the interests or fundamental rights and freedoms of data subjects.

8. Consent as a basis for processing

8.1 A data subject consents to processing of their personal data if they indicate agreement clearly either by a statement or positive action to the processing. Consent requires affirmative action, pre-ticked boxes. If consent is given in a document which deals with other matters, then the consent must be kept separate from those other matters.

8.2 Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if we intend to process personal data for a different and incompatible purpose which was not disclosed when the data subject first consented.

9. GDPR Principles

9.1 The legislation places a responsibility on the charity to process any personal data in accordance with 6 GDPR principles. Smilez will:

9.2 A data subject consents to processing of their personal data if they indicate agreement clearly either by a statement or positive action to the processing. Consent requires affirmative action, pre-ticked boxes. If consent is given in a document which deals with other matters, then the consent must be kept separate from those other matters.

(a) **Process personal data lawfully, fairly and in a transparent manner**. We will ensure that individuals whose personal data we collect are informed of:

(i) The identify of the Data Protection Officer

(ii) The purpose of the processing

(iii) Any potential disclosures to third parties

(iv) The length of time their personal data will be kept

(b) **2. Process personal data for the specific and lawful purpose for which it's been collected.**
We will make sure that the reason for which we collected the data is the only reason for which we process that data. If a new processing purpose is identified for data that has already been collected, the Board of Trustees will make consider its use for the new purpose using the following criteria:

(i) Any link between the original purpose and the new processing purpose.

(ii) The context in which the personal data was collected, in particular, the nature of the relationship between the charity and the data subject.

(iii) The nature of the personal data, particularly whether it includes any special categories of personal data.

(iv) Possible consequence of the further processing for the individual(s).

(v) The existence of appropriate safeguards such as encryption or using pseudonyms.

(vi) If the new purpose is incompatible with the original purpose processing will only take place once a new consent has been obtained or if a legal obligation applies.

(vii) If the new purpose is considered compatible with the original purpose the reasons for the decision will be documented.

(c) **Ensure that personal data is adequate, relevant and not excessive in relation to the purpose for which it is processed.** We will not collect any personal data which is not strictly necessary for the purpose for which it was obtained.

(d) **Keep data accurate and where necessary keep it updated.** Any inaccuracy in personal data bought to the attention of the Board of trustees & notified to the trustee or volunteer who is able to correct the data. Corrections will be made to all relevant databases and systems.

(e) **Only keep personal data for as long as necessary.** We will not retain personal data for longer than is necessary to ensure compliance with legislation and any other statutory requirements. Retention periods for personal data will be agreed in accordance with these requirements.

(f) **Ensure the appropriate security of personal data.** Personal data will only be accessible to those who have a valid reason for using it.

(i) We will put appropriate technical and organisational measure in place against unauthorised or unlawful processing of personal data and against accidental loss or destruction of data.

(ii) Appropriate security measures will be in place such as ensuring back up of personal data is kept safe with controlled access, personal data held

electronically is password protected and that PC screens are not left unattended without a password protected screensaver being used. Mobile phones, laptops and tablets will be password protected. Login and password details should not be stored on any device that holds personal data.

(iii) We will ensure that any third-party hosting IT services on behalf of the charity are GDPR compliant.

(iv) In addition, we will ensure there are appropriate measures in place for deletion of personal data. Manuals records will be shredded or disposed of as confidential waste using accredited third parties only. Hard drives of redundant computers will be wiped clean before disposal or destroyed physically.

(v) All trustees and volunteers are responsible for ensuring any personal data which they hold is kept securely and not disclosed to any unauthorised third parties.

10. Data audit and register

10.1 Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

11. Retention of data

11.1 Retention period for data is dependent on the type of data held and whether we have a statutory or legal requirement to retain it. Data retention will be reviewed by the Board of Trustees, and a record of deletion will be kept.

12. Destroying personal data

12.1 Where personal data is held manually, records will be shredded or will be destroyed using a certified, confidential waste disposal service.

13. Subject access rights (SARs)

13.1 Individuals have a right to access any personal data relating to them which is held by us. Any individual wishing to exercise this right should apply in writing by emailing to **info@smilez.org.uk**

14. Data portability

14.1 Upon request, a data subject should have the right to receive a copy of their data in a structured format. These requests should be processed within 1 month, provided there is no undue burden, and it does not compromise the privacy of other individuals. A data subject may also request that their data is transferred directly to another system. This will be done for free.

15. Right to be forgotten

15.1 A data subject may request that any information held on there is deleted or removed, and any third parties who process or use that data must also comply with this request. A request to be forgotten will only be refused if an exemption applies.

16. Disclosure of data

16.1 Personal Data will not be shared with others except as permitted by applicable law or as follows:

(a) We will share Personal Data as necessary with third parties who provide services or functions on our behalf and who require the information to provide those specific services. These third parties may include social media advertising platforms such as Facebook and Google Adwords for the purpose of custom audience generation and the development of targeting criteria for other audiences.

(b) We have appropriate data privacy safeguards in place with third parties with whom we share personal data as described above and who are providing services or functions on our behalf.

17. Breach notifications

17.1 Any breeches of GDPR must be reported to the designated Trustee without delay who will then notify the Information Commissioners Office (ICO) within 72 hours of being made aware of the breach unless the breach is unlikely to result in any risk to the rights and freedoms of the individual. The designated Trustees will also report any breach to the individual(s) without any undue delay.

17.2 Notifications to the ICO and individuals impacted will made in accordance with the GDPR and will include information about the likely consequences of the breach and measures taken or proposed to address the breach including any measures to mitigate any possible adverse effects. A register of compliance failures will be kept and reviewed at Board level.

18. Policy review meetings

18.1 Board of Trustees will have regular meetings with regards to new and amendments of any policy's. Meetings will be minuted with summary and actions assigned to Trustees where necessary

19. Policy review

19.1 This policy will be reviewed every 3 years or earlier should law or guidance relating to it change.