Data Protection and Privacy Policy

Policy information

Policy applies to	Charity-wide
Policy status	Revision of existing May 2018 policy
Policy Sponsor	Finance Director
Policy Owner	Data Protection Manager
Approval date	30/05/2019 – Development Director
Effective date	25/05/2019
Date of policy review*	30/04/2020
Related policies, procedures, guidelines	Data Protection Framework, including: Data Security in the Workplace Policy Information Security and Acceptable Use Policy Safeguarding policies Whistleblowing Policy Data Protection Training – staff and volunteer Data Processing Inventory Privacy notices at data collection points, including for employee & recruitment, volunteers, supporters

* Unless otherwise indicated, this policy will still apply beyond the review date.

sustrans
JOIN THE MOVEMENT

Purpose

At Sustrans, we are committed to protecting individuals' privacy, being transparent about how we collect and use personal data, and fulfilling our obligations under data protection and privacy legislation, which is applicable to all areas of our work.

This not only protects the individuals, but safeguards our reputation and avoids potential fines from the UK's regulatory body – The Information Commissioner's Office (ICO).

This policy sets out how we will meet our obligations in relation to processing personal data.

This policy applies to the personal data of all individuals who come into contact with our work. It applies to our supporters, volunteers, project participants, job applicants, employees, workers, contractors, apprentices and anyone who had any of these roles in the past. It also applies to our clients, funders, online shop customers, members of the public or other personal data processed for business purposes.

Legal definitions of the terminology used in data protection can be found in Article 4 of the General Data Protection Regulation (GDPR): https://gdpr-info.eu/art-4-gdpr/

A public-facing privacy notice will be issued on www.sustrans.org.uk/privacy, and will mirror this policy as appropriate for external audiences to include other organisations and individuals themselves. It is this online policy that will be referred to in our privacy notices, not this full company policy intended for an internal audience.

Policy

1. **Process personal data lawfully:** Personal data must be processed in accordance with the principles of data protection legislation (the General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA 2018)):

    a. **Lawfulness, fairness and transparency principle:** Process personal data lawfully, fairly and in a transparent manner.

    b. **Purpose limitation principle:** Collect personal data only for specified, explicit and legitimate purposes, data will not be further processed in a manner that is incompatible with those purposes.

    c. **Data minimisation principle:** Process personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.

    d. **Accuracy principle:** Keep accurate personal data and take all reasonable steps to ensure that inaccurate personal data is rectified and that individuals can efficiently and without delay check, and if needed erase or rectify, the data we have on them.

e. **Storage limitation principle:** Keep personal data only for the period necessary for processing.

f. **Integrity and confidentiality (security) principle:** Appropriate technical and organisational measures must be adopted, and regularly reviewed, to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

g. **Accountability principle:** We must take responsibility for what we do with personal data and how we comply with the other principles. We must have appropriate measures and records in place to be able to demonstrate our compliance.

2. **Uphold the rights of individuals:** Individuals have the following rights under data protection legislation, which must be respected, and exercised as appropriate, across all our work:

    a. The right to be informed
    b. The right of access
    c. The right to rectification
    d. The right to erasure
    e. The right to restrict processing
    f. The right to data portability
    g. The right to object
    h. Rights in relation to automated decision making and profiling.

Accountability

3. **Accountability for processing lies with the Data Controller:** The Data Controller of the processing sets our ways of working, and this can be ourselves or a third party. The Data Controller's privacy policy may take precedence over ours, and it is the policy referred to at the point of collection of personal data that will take precedence.

4. **Sustrans has a named Data Controller:** Accountability for data protection within Sustrans lies with our Finance Director as our Data Controller.

5. **Day to day co-ordination for Sustrans' data protection compliance lie with our Data Protection Manager:** Questions about this policy, or requests for support, should be directed to the Data Protection Manager on dataprotection@sustrans.org.uk or 0117 915 0320.

6. **Everyone has a role to comply with data protection legislation:** All our people (staff, temporary workers, contractors and volunteers) have a responsibility for data protection compliance. Sustrans will provide all appropriate guidance and tools but relies on our people to help meet our data protection obligations.

7. **Everyone has a role to report concerns:** Our people must notify the Data Protection Manager if they consider any of our working practices surrounding personal data to not be consistent with current legislation.

Assessment of processing

8. **Assess processing before it begins:** A formal data assessment must be carried out prior to the start of any processing of personal data we carry out, to protect the personal data and protect against a personal data breach. We must assess new, or changes to existing, systems and ways or working. This assessment must cover the legally required Legitimate Interest Assessment and Data Privacy Impact Assessment with Exec sign off as appropriate. This is done in compliance with our 'Personal Data Assessment Form'.

9. **Log all processing centrally:** All processing of personal data we undertake must legally be logged centrally on our Data Processing Inventory through the Data Protection Manager.

10. **Comply with the measures identified:** All protective measures identified during the data assessment must be implemented for the processing to ensure that data protection compliance is built into the whole processing.

Operational measures

11. **Provide privacy information to individual at the point of data collection:** When collecting personal data we must provide individuals with information about our purposes for processing their personal data, the lawful basis for processing their personal data, our retention periods for that personal data, who it will be shared with and, where relevant, if we intend to transfer the personal data outside the EEA.

    This must be concise, transparent, intelligible, easily accessible, and it must use clear and plain language.

    Where we are providing the policy, the privacy information must also link to our public-facing Data Protection and Privacy Policy at www.sustrans.org.uk/privacy, which provides further Sustrans-wide privacy information to complete our obligations in a layered manner.

12. **Restrict access to personal data:** Access must be restricted to those people who are required and authorised to process the data.

13. **Ensure the integrity of our people processing personal data:** Our people are to undergo appropriate background checks or additional requirements prior to processing personal data, this may include the use of financial probity and criminal records checks for roles with access to sensitive personal data.

14. **Adequately train our people:** Our people are to undertake initial and then regular training in data protection, appropriate to their involvement in processing personal data as outlined in our data protection training needs

assessment matrix. All staff must undertake the mandatory online data protection training as part of their initial induction.

15. **Safeguard the sharing of personal data:** Personal data must never be sold. We may share personal data, under strictly defined circumstances, when:
    a. A data sharing agreement is in place with the third party, either as part of our contract or as a standalone agreement, which ensures sufficient safeguards are in place to comply with data protection legislation and privacy legislation. Examples of third parties are data controllers such as funders, project partners, or sub-processors such as mailing houses and data centres.
    b. Required under law.

16. **Protect personal data transfers outside the EEA:** Personal data must not be transferred outside the European Economic Area unless appropriate safeguards are in place and individual rights are enforceable with effective legal remedies. This is usually done through accreditation under schemes such as the US-EU Privacy Shield Framework or equivalent, or Standard Contractual Clauses or Binding Corporate Rules. The affected individuals also need to be informed.

17. **Retain personal data for no longer than required:** Our Data Retention Policy and Schedule sets the retention limits for all data types, and what is to happen to the data before that time point (deletion or anonymisation), and must be complied with.

Technical measures

18. **Appropriate technical measures must be put in place:** Our technical measures across Sustrans must, at a minimum, meet the requirements of Cyber Essentials, the UK government scheme that encourages good practice in information security. These measures cover access, monitoring, secure data transfer, encryption, hashing/salting of passwords, firewalls, software updates, virus scanning, penetration testing, use of mobile devices, and more.

    These measures extend to all our system development work, not just the work overseen by our IT Support team and is it be done in compliance with out Information Security and Acceptable Use Policy.

19. **Systems to accommodate data subject rights:** The functionality to comply with each data protection principle and action each individual right, as assessed to be appropriate, must be built into every system's functionality that is used in Sustrans and the user guidance must give clear instructions to the system users as to how to comply with necessary actions. As such, only approved systems and software are to be used to process personal data on behalf of Sustrans.

Action time

20. **Responses to (suspected) breaches of personal data will be managed centrally within legal timeframes:** If Sustrans becomes aware that there has been a (possible) breach of personal data it will be logged, assessed with a focus on risk and impact to the individuals, contained and notification to the Information Commissioner's Office, third parties identified in relevant data sharing agreements, and the affected individuals will be determined within the legal timeframe of 72 hours, in compliance with our 'Data Breach Response Plan'.

21. **Individual rights requests will be managed within legal timeframes:** Requests by individuals to exercise their individual rights, received via any channels, must be recorded and escalated to the authorised point of action, and will normally be complied with within the legal period of one month. In clearly defined, exceptional circumstances we may take three months to respond. Managing individual rights requests, and assessing the complexity and therefore response timeframe, is done in compliance with our 'Data Subject Rights Response Plan'.

22. **Round the clock support is available:** Data protection support is provided on dataprotection@sustrans.org.uk which is monitored every day, or you can ring 01179 150 320 during office hours or the Out of Hours Emergency phone number is 08448 480226.

Auditing

23. **Regular data audits should be carried out**: To ensure that processing of personal data is compliant with relevant policies and procedures.

Breach, enforcement and compliance

Any suspicion of a breach of this policy must be reported immediately to the Data Protection Manager. All instances of suspected breaches of the policy shall be investigated and action taken as appropriate.

Non-compliance with this policy by permanent, temporary or contract employees, volunteers or any third parties, who have been granted access to our premises or information, may result in disciplinary proceedings or termination of their employment, agreement or contract.