General Data Protection Policy

Introduction
The object of Slow The Flow is to advance the education of the public in Natural Flood Management, Sustainable Drainage Systems and other renewable methods of managing the environment, including the exploration of alternative practices which safeguard the natural environment and its resources in a manner which best fits the specifics of a local geography.

SLOW THE FLOW'S OBLIGATIONS

CORE PRINCIPLES:
The UK General Data Protection Regulations (GDPR) and Data Protection Act 2018 regulate how Slow The Flow manages the data that it is entrusted with, in relation to those who administer, work and volunteer on site, and to those who visit us.

The core data protection principles are:

1. **Lawfulness, fairness, and transparency** – There has to be a legal basis for collecting, processing and storing personal data. This may include fulfilling the legitimate objectives of Slow The Flow, or to meet any other regulatory obligations. No-one should ever be surprised by the use to which we put their data;
2. **Purpose limitation** – Data will **ONLY** be obtained, processed and used for specific reasons which must be stated at the time of collection;
3. **Data minimisation** – Only the amount of data necessary for Slow The Flow to fulfil its purpose will be collected, used and retained;
4. **Accuracy** – Data accuracy is paramount and any individual has the right to request a correction of their data. All such requests will be taken seriously. Any data or data sets acquired via a third party must be as accurate as possible. All necessary measures, including regular audits, will be taken to ensure that the highest standards of accuracy are maintained;
5. **Storage limitation** – As soon as data is no longer needed, or any other legal time limits have expired, unnecessary data will be deleted from our computer records, and paper records securely disposed of;
6. **Integrity and confidentiality of data** – Data may **ONLY** be accessed by those with a legitimate right to do so. Systems of storage will be sufficiently secure.
7. **Accountability** – Slow The Flow must be able to demonstrate compliance with the previous 6 principles, to ensure that all data is secure. Systems, including audit trails are in place and regularly reviewed.

WHAT INFORMATION DO WE STORE?
Information including personal data is obtained and retained on the following types of people, and in the circumstances described:

Trustees

Information	Names, addresses, telephone numbers, mobile numbers, e-mail addresses, images, DBS certificates and documentation relating to trustee applications.

Reason	Information for regulatory purposes, for public awareness and for internal communications between trustees.
Where stored	Personal details kept on the Slow The Flow Google Drive & password protected. All trustees have access. Internal communications via WhatsApp groups are restricted to trustee members only. Emails may occur between trustees (via a designated @slowtheflow.net email address) and third parties. Local copies may exist on trustees' personal devices.
How long retained	For the duration of the role. When a Trustee ceases to hold the role, details are then deleted, except as required for regulatory purposes. Former trustees are removed from WhatsApp groups and emails, although their previous messages may be retained for historic reasons.

Volunteers

Information	Names, contact numbers, e-mail addresses, emergency contact details, **health**, employment skills, permission to use images (including on social media accounts).
Reason	Safety and welfare of volunteers whilst engaging in their role with Slow The Flow. Permitted use of images in external communications to raise awareness of Slow The Flow's work.
Where stored	Details on Slow The Flow Google Drive & password protected. Images and contact information may temporarily be held on trustees' personal devices during and immediately following an event.
How long stored	3 years from last confirmation of details/session attendance, unless early deletion is requested. Data will be deleted from personal devices as soon as possible following an event.

Third parties and the wider NFM community

Information	E-mail addresses and business contact details.
Reason	Engagement with local, national, and international NFM community**.** Correspondence around funding applications. Regulatory and professional support contacts.
Where stored	Details on Mail Chimp software, login required. Third party contacts may also be retained on Slow The Flow email system. Local copies may exist on trustees' personal devices.
How long stored	3 years from last confirmation of details or contact, unless early deletion is requested.

Accident Book

Information	Names, addresses, contact numbers and e-mail addresses of anyone who has had an accident on site (staff and visitors). Detail of accident or injury as required for compliance (**health**). Consent will be obtained wherever possible, but HSE compliance is paramount.
Reason	Regulatory compliance with HSE.
How long stored	5 years.
Where stored	STF Google Drive & password protected.

Digital copies on local devices

Where a photograph or scanned copy is taken on any type of device for the purposes of creating a digital image (such as from a paper file of a sign-in sheet or other document which records personal details), that photo or scanned copy must be permanently deleted from the device - including from the device's Deleted folder - once the image has been uploaded to the password protected Google Drive. This is to be done as soon as reasonably possible.

MAINTENANCE OF DATA SECURITY AT STORAGE SITES:

This is facilitated by the designated Trustee from Slow The Flow who will ensure that:

1. **Annual checks** are completed to ensure that all data stored by Slow The Flow as outlined above, is accurate.

2. **Storage limitation** – Data we no longer need, or which is no longer required to fulfil legal obligations such as HMRC, PAYE or HSE, is securely disposed of and that expired contact details are **ALWAYS** deleted from the computer system after a year (to allow for the option of renewal).
3. All **marketing e-mails** to contacts contain a form of consent to use the data for marketing, and to give the recipient the option of unsubscribing, as per GDPR guidelines.
4. Prompt, effective, and proportionate action is taken in the event of a **breach** in full compliance with GDPR. This includes the maintenance of an effective system for logging breaches and ensuring that the Information Commissioner's Office (ICO) and the owner/s of the data are notified where appropriate.
5. Ensuring that the **security systems for data storage** are always maintained to the highest standards possible and that any breaches are reported to the DPO / Trustees and appropriate action is immediately taken.
6. Slow The Flow will provide enough **training** and regular updates to enable full compliance with GDPR. This particularly applies to emphasising the necessity of immediately reporting any data breaches in order that appropriate action can be initiated, and identifying Subject Access Requests.
7. All **Subject Access Requests** are dealt with promptly and effectively, and within one calendar month as required.

DATA BREACH NOTIFICATION

Under GDPR and data protection, there is an obligation on controllers (ie the organisations who process personal data - Slow The Flow is a data controller) to inform the ICO and (potentially) the individuals affected in the event of certain data breaches. The term ***data breach*** has a broad definition that includes data loss, as well as unauthorised access and alteration (such as a hacking attack).

- If there is any ***breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data*** it must be notified (reported) to the ICO. The exemption is if a breach is unlikely to cause any risk to individuals. In this case the details must still be documented.
- Staff processing the information breach **MUST** inform our DPO swiftly, once aware of the incident. e.g. A staff member must report to DPO / Trustees as soon as any breach is discovered.
- Reporting to the ICO has to be done promptly and usually within 72 hours of becoming aware of the incident. Our nominated Data Protection Officer (DPO) must also update the individual(s) involved unless:
    - The breach is unlikely to affect their rights and freedoms.
    - The DPO had taken measures to protect the information e.g. encryption;
    - Notification would involve disproportionate effort. If so, a public communication, such as a notice in a newspaper or website announcement is acceptable.

DATA AMENDMENT / BREACH – REPORTING DOCUMENTS

All requests for personal data access, amendment of personal details, and data breaches **MUST** immediately be reported to the Slow The Flow Trustees and passed to the Data Protection Officer to deal with. A **detailed** description of the nature of the request is needed to ensure we are able to comply with it as fully and promptly as possible. Responses to requests may be time limited.

DATA AMENDMENT FORM

Request for Access, Rectification, Erasure, Restriction of information *Please use only one form per individual request*				
Date	**Person(s) to whom request made and method of doing so.**	**Person requesting access, rectification, erasure or rectification of information.** **Please record the nature of the request in as much detail as possible.** **Include full name, address, contact number(s) and e- mail address (if applicable).**	**Action Taken** **Please record all action(s) taken in as much detail as possible.**	**Revisions made and applicant updated** **DPO to endorse and date when complete.**

DATA BREACH FORM

Date	Details of Data Breach - piease give as much detail as possible.	Person(s) affected Include full name, address, contact number(s) and e-mail address (if applicable).	Action Taken by DPO Please record all action(s) taken in as much detail as possible.	ICO Informed Y/N	DPO's Signature and date

Change Record

Date of Change:	Changed By:	Comments:
5/8/2020		Approved by Trustees via Trello
24/4/22	TD	Document reviewed and no changes required
21.07.2023	TB	Reviewed – updated references to One Drive to Google Drive & updated references to EU to UK and EU.
30.11.2023	TB	Reviewed – updated in relation to the deletion of photos/scans of documents which record personal details.