Data Protection Regulation Policy

Document Title	General Data Protection Regulation Policy
Author	Joanne Vertannes
Reviewed by	The Board of Directors
Approved by	
Date of issue	23 September 2025
Version and Date revised	Version 1.0
Revisions made	N/A

Contents

1. Scope

This policy applies to:

- All staff, volunteers, and contractors of The Hub @ Toothill.
- All service users and survey respondents whose personal data we collect.
- All personal data held digitally or in paper records, including data processed by third-party providers on our behalf.

2. Definitions

General Data Protection Regulation (GDPR)
An EU regulation governing data protection and privacy for individuals within the EU and EEA, including the export of personal data outside these areas.

Controller
The person or organisation determining the purposes and means of processing personal data. Controllers remain responsible for GDPR compliance, even when using processors.

Processor
A person or organisation that processes personal data on behalf of a controller. Processors have legal obligations under GDPR, including maintaining records of processing activities.

Personal Data
Information relating to an identifiable individual, directly or indirectly, via identifiers such as name, ID number, location data, or online identifiers. This includes both automated and structured manual data.

Sensitive Personal Data (Special Categories)
Includes, but is not limited to:

- Racial or ethnic origin
- Political opinions
- Religious beliefs or similar
- Trade union membership
- Health information
- Sexual orientation

Data relating to criminal convictions requires similar safeguards.

“Necessary” Processing
Processing must be targeted and proportionate to achieve its purpose. It need not be essential, but must be the least intrusive method available.

3. Roles and Responsibilities

- **Data Protection Lead:** Joanne Vertannes. Oversees GDPR compliance, staff training, and incident management.
- **Staff and Volunteers:** Responsible for handling personal data in line with this policy.

- **Third-Party Processors:** Must comply with contractual and GDPR obligations, including safeguards for data transferred outside the UK/EU.

4. GDPR Principles

Personal data must be:

- Processed lawfully, fairly, and transparently.
- Collected for specified, explicit, and legitimate purposes.
- Adequate, relevant, and limited to what is necessary.
- Accurate and kept up to date; regularly reviewed and corrected where necessary.
- Retained only as long as necessary, or longer for archiving, research, or statistics with safeguards.
- Secured against unauthorised access, loss, destruction, or damage.
- Demonstrably compliant with GDPR principles.

5. Lawful Bases for Processing

We only process personal data if one or more of the following apply:

- **Consent** – explicit permission given by the individual.
- **Contract** – necessary for contractual obligations or pre-contractual steps.
- **Legal Obligation** – required by law (e.g., DBS checks).
- **Legitimate Interests** – processing necessary for organisational interests unless overridden by individual rights.
- **Public Task** – necessary for tasks with a legal basis.
- **Vital Interests** – necessary to protect life.

Note: The Hub @ Toothill is unlikely to rely on Public Task or Vital Interests.

6. Individual Rights

Individuals have the right to:

- Be informed about data collection and use.
- Access their personal data (“Subject Access”).
- Rectify inaccurate or incomplete data.
- Request erasure (“right to be forgotten”), subject to legal limits.
- Restrict processing temporarily.

- Receive their data for portability purposes.
- Object to certain processing, including direct marketing.
- Challenge automated decisions (not currently used by the Hub).

Lawful Basis vs Rights:

Lawful Basis	Erasure	Portability	Object
Consent	Yes	Yes	No (can withdraw consent)
Contract	Yes	Yes	No
Legal Obligation	No	No	No
Legitimate Interests	Yes	No	Yes
Public Task	No	No	Yes
Vital Interests	Yes	No	No

Requests must be logged and responded to within **28 days**.

7. Information We Collect

Service Users:

- Name / Organisation name
- Contact information (email & phone)
- Billing address

Survey Respondents:

- Sex / Gender
- Age or age group
- Other relevant personal or demographic information

Purpose:

- Provide services and support
- Communicate updates
- Improve services through surveys and feedback
- Manage billing and compliance

Note: Sensitive data is stored securely and used only for stated purposes.

8. Who We Share Information With

We only share personal information when it is necessary to deliver our services, comply with the law, or support community activities. This includes:

- **Safeguarding and child protection**: Information may be shared with **Swindon Borough Council** or other statutory safeguarding bodies to ensure the safety and welfare of children and vulnerable adults.
- **Community engagement and surveys**: Aggregate or anonymised information may be shared with **community organisers or partner organisations** who help us carry out surveys, research, or community projects.
- **Service delivery**: Data may be shared with trusted contractors or suppliers when necessary to provide services or manage payments.

We do **not sell or share your personal information for marketing purposes**. All sharing is limited to what is necessary, secure, and compliant with **GDPR**.

9. How We Store and Protect Your Information

All personal information is stored securely, with access restricted to authorised personnel only. Digital data is held on encrypted and trusted platforms including **Microsoft 365**, **G-Suite**, our **Wix website**, and **Capsule CRM**. Paper records are kept in locked storage and shredded when no longer needed. Regular backups and security protocols prevent unauthorised access, loss, or breaches.

This storage and security approach ensures compliance with **GDPR**, supporting your rights to access, erasure, and portability wherever applicable. Sensitive information, such as safeguarding or health & safety data, is stored securely and retained as required by law.

8. Data Retention Schedule

Data Type	Purpose	Retention Period	Notes
Service User Name & Contact Info	Communication and service provision	6 years after last contact	Aligns with accounting/contract retention
Billing Information / Invoices	Financial records	7 years	HMRC compliance

Survey Responses (non-identifiable)	Service improvement / research	5 years	Anonymised where possible
Survey Responses (identifiable)	Service improvement / reporting	3 years	Stored securely
Staff / Volunteer Records	HR, payroll, legal compliance	6 years after leaving	Includes DBS checks, references
Health / Sensitive Data	Service-specific needs	Duration of service + 3 years	Stored securely
Legal / Regulatory Records	Compliance	As required by law	Reviewed periodically
Email / Internal Communications	Operational purposes	2 years	Can be archived or deleted sooner
Marketing / Mailing Lists	Promotional communications	Until consent withdrawn	Consent records retained

Data beyond retention periods will be securely deleted or anonymised.

9. Security

We implement physical, electronic, and managerial measures to protect personal data from unauthorised access, disclosure, loss, or damage.

10. Data Sharing

Personal data may be shared with third parties only when:

- Legally required
- Necessary for service delivery
- Covered by a data processing agreement

All data transfers outside the UK/EU will be subject to appropriate safeguards.

11. Data Breach Management

- Any suspected breach must be reported immediately to the Data Protection Lead.
- Breaches will be investigated, contained, and, if required, reported to the ICO within 72 hours.

- Affected individuals will be informed if there is a risk to their rights or freedoms.

12. Staff Training & Compliance

- All staff and volunteers handling personal data receive GDPR awareness training.
- Failure to follow this policy may result in disciplinary action.

13. Children's Data

- Any personal data collected from children under 13 (or local equivalent) will only be collected with parental or guardian consent.

14. Cookies / Online Data

- Personal data collected online (forms, newsletters, surveys) is processed in line with this policy.

15. Controlling Your Personal Information

- Individuals can request removal from communications or deletion of personal data.
- Full removal may not always be possible due to legal or contractual obligations; this will be communicated.
- Personal information is not sold or leased without consent or legal requirement.
- Individuals may also complain to the **ICO** if they believe their data has been mishandled.
- Contact: **contact@toothillhub.co.uk** for queries or data requests.

16. Policy Review

- This policy will be reviewed at least annually or when there are significant changes in data processing or legislation.

Appendix

A) Lawful Basis Checklist Template

What is your purpose – what are you trying to achieve?	
Can you reasonably achieve it in a different way?	
Do you have a choice over whether or not to process the data?	

Consent	Has the individual given clear consent?	
Contract	Is it necessary for a contract?	
Legal Obligation	Is it necessary in order to comply with the law?	
Legitimate Interests	Is it necessary for our legitimate interests?	
Public Task	Is it necessary to perform an official task/our official function?	N/A
Vital Interests	Is it necessary to protect someone's life?	N/A

B) GDPR Checklist

We have reviewed the purposes of our processing activities and selected the most appropriate lawful basis (or bases) for each activity.	
We have checked that the processing is necessary for the relevant purpose and are satisfied that there is no other reasonable way to achieve that purpose.	
We have documented our decision on which lawful basis applies to help us demonstrate compliance.	
We have included information about both the purposes of the processing and the lawful basis for the processing in our privacy notice.	
Where we process special category data, we have also identified a condition for processing special category data and have documented this.	
Where we process criminal offence data, we have also identified a condition for processing this data and have documented this.	