DATA PROTECTION & GDPR POLICY

for

THE HABBIT FACTORY

Version 1.0 | Date: March 2026

Lead: Andy Bennett (Data Protection Officer)

Approved by: Andrew Bennett

Policy Owner: Lee Giles

This Privacy Policy describes Our policies and procedures on the collection, use and disclosure of Your information when You use the Service and tells You about

Your privacy rights and how the law protects You. We use Your Personal data to provide and improve the Service. By using the Service, You agree to the collection and use of information in accordance with this Privacy Policy.

1. Purpose

The Habbit Factory (THF) is committed to respecting and protecting the privacy of all children, young people, adults, volunteers, parents/carers, staff, and donors. This policy outlines how THF collects, stores, processes, and disposes of personal data in compliance with the UK GDPR and Data Protection Act 2018.

2. Scope

This policy applies to all personal data processed by The Habbit Factory, in any format:

- Children, young people, vulnerable adults, parents/carers
- Staff and volunteers
- Donors, funders, partners, and schools
- Third-party contractors and suppliers

All staff, volunteers, and trustees must adhere to this policy.

3. Data Protection Principles (Article 5 GDPR)

THF complies with the following principles:

- Lawfulness, fairness, and transparency – Personal data is processed lawfully, fairly, and transparently.
- Purpose limitation – Data is collected only for specific, legitimate purposes.
- Data minimisation – Only necessary data is collected and processed.
- Accuracy – Data is kept accurate and up to date.

- Storage limitation – Data is retained only for as long as necessary (see Section 8).
- Integrity and confidentiality – Data is stored securely and protected from unauthorised access.
- Accountability – THF demonstrates compliance with GDPR through this policy, training, and record-keeping.

4. Roles and Responsibilities

Data Protection Officer (DPO): Andy Bennett

- Oversees GDPR compliance, liaises with ICO, manages subject access requests, and monitors training.

CEO/Artistic Director (Lee Giles)

- Ensures operational implementation of GDPR and policy adherence.

Staff

- Responsible for following GDPR procedures, completing training, and reporting incidents.

5. Consent and Data Collection

- Consent is obtained via online sign-up forms (membership, volunteers, staff recruitment) linked directly to THF's CRM
- For children, parental/guardian consent is collected via digital signature.
- Consent is recorded and can be withdrawn at any time; however, withdrawing consent may affect THF's ability to provide services or employment.

6. Information We Hold

Data Type	**Examples**	**Lawful Basis**	**Retention**	**Disposal Method**
Children/young people registration	Name, DOB, parent details, emergency contacts, group attendance, SEND/SEMH needs	Contract with parent	1 year post-show (fitness forms) / 3 years for incidents	Secure deletion/shredding

Fitness/performance forms	Child/parent name, signature, phone, group, date signed	Contract with parent	1 year post-show	Secure deletion
First aid / Accident forms	Injuries, treatment, witnesses	Legal obligation, safeguarding	3 years	Secure deletion/shredding
Staff payroll & HR	Name, contact, NI, salary, health info	Legal obligation	6 years	Secure deletion/shredding
Emails with personal data	All correspondence	Legitimate interest / legal	3 years (unless legal)	Secure deletion
Volunteer information	Name, contact, DBS checks	Contract / legal obligation	3 years post-volunteer role	Secure deletion
Gift Aid forms	Name, address, donation amount, declaration	Legal obligation (HMRC)	5 years post-claim	Secure deletion
Funders, partners, schools	Contact details, contracts, agreements	Legitimate interest / contractual	3 years after relationship ends	Secure deletion

Retention of Your Personal Data

The Habbit Factory will retain Your Personal Data only for as long as is necessary for the purposes set above.. We will retain and use Your Personal Data to the extent necessary to comply with our legal obligations (for example, if we are required to retain your data to comply with applicable laws), resolve disputes, and enforce our legal agreements and policies. The Habbit Factory will also retain Usage Data for internal analysis purposes. Usage Data is generally retained for a shorter period of time, except when this data is used to strengthen the

security or to improve the functionality of Our Service, or We are legally obligated to retain this data for longer time periods.

Note: All data is stored securely, with 2 factor authentication on devices, Office 365 encryption, and antivirus protection (Avast). No trustee or volunteer has direct access to personal data.

7. Third-Party Processors

- THF uses third-party services such as CRM and Accountancy Services to process data.
- The Habbit factory ensures all contracts comply with GDPR and UK data protection law, and processors implement appropriate security measures.

8. Access and Confidentiality

- Personal data is only accessible to staff and Trustees with a legitimate need.
- Confidentiality is maintained for children, parents, staff, volunteers, and donors.
- Staff, volunteers, and students are trained on confidentiality during induction and receive annual GDPR refresher training.

9. Data Subject Rights

Individuals may request:

- Access to personal data (Subject Access Requests)
- Correction of inaccurate data
- Deletion of data (where legal obligations do not prevent it)
- Restriction or objection to processing
- Withdrawal of consent

Requests will be responded to within 1 month. Complaints can be escalated to the ICO if unresolved.

10. Use of Your Personal Data

The Habbit Factory may use Personal Data for the following purposes:

- To provide and maintain our Service, including to monitor the usage of our Service.
- To manage your Account: to manage Your registration as a user of the Service. The Personal Data You provide can give You access to different functionalities of the Service that are available to You as a registered user.
- For the performance of a contract: the development, compliance and undertaking of the purchase contract for the products, items or services You have purchased or of any other contract with Us through the Service.
- To contact You: To contact You by email, telephone calls, SMS, or other equivalent forms of electronic communication, such as a mobile

application's push notifications regarding updates or informative communications related to the functionalities, products or contracted services, including the security updates, when necessary or reasonable for their implementation.

- To provide You with news, special offers and general information about other goods, services and events which we offer that are similar to those that you have already purchased or enquired about unless You have opted not to receive such information.
- To manage Your requests: To attend and manage Your requests to Us.
- For Business transfers: We may use Your information to evaluate or conduct a merger, divestiture, restructuring, reorganisation, dissolution, or other transfer of some or all of Our assets, whether as a going concern or as part of bankruptcy, liquidation, or similar proceeding, in which Personal Data held by Us about our Service users is among the assets transferred.
- For other purposes: We may use Your information for other purposes, such as data analysis, identifying usage trends, determining the effectiveness of our promotional campaigns and to evaluate and improve our Service, products, services, marketing and your experience. We may share Your personal information in the following situations:
- With Affiliates: We may share Your information with Our affiliates, in which case we will require those affiliates to honour this Privacy Policy. Affiliates include joint venture partners or funders
- With other users: when You share personal information or otherwise interact in the public areas with other users, such information may be viewed by all users and may be publicly distributed outside.
- With Your consent: We may disclose Your personal information for any other purpose with Your consent.

11. Data Breach Reporting & Response

- Who reports breaches: Any staff member, volunteer, or trustee who identifies a potential breach must report to DPO Andy Bennett or CEO immediately.
- Recording breaches: Complete the Data Breach Reporting Form (Section 1-3) and submit to DPO.
- Notification timeframe: The ICO must be notified within 72 hours for breaches likely to result in a high risk to individuals. Affected individuals must also be notified without undue delay if high risk.

Breach Response Steps:

1. Identification & initial assessment
2. Containment & recovery
3. Risk assessment
4. Notification to ICO, affected individuals, and relevant parties
5. Evaluation & response to prevent recurrence

All breaches and actions are logged in THF's GDPR Framework.

12. Storage & Security

- All digital data is stored on Office 365 with 2FA.
- Paper records are stored securely in locked storage unit with limited access.
- Devices are protected by antivirus software and passwords.
- Only authorised staff may access personal data.

13. Staff & Volunteer Training

- GDPR training is included in induction.
- Annual refresher training for all staff, volunteers, and trustees.
- Training covers data handling, breach reporting, and confidentiality.

14. Policy Review & Version Control

Version	Date	Author	Approved By	Notes
1.0	13th April 2022	Lee Giles	Trustees	
2.0	March 2026	Lee Giles	Andrew Bennett	Comprehensive update, DPO Andy Bennett, online forms, retention schedule

Policy to be reviewed annually or sooner if legislation or operational changes require.

Signed:

Lee Giles – CEO/Artistic Director

Andrew Bennett – Data Protection Officer