Treasure time Data Protection & Privacy Policy

V1 11.06.2025

Approved by: Sophia Giblin, Founder & CEO
Effective Date: 12th June 2025
Review Date: 11th June 2026
Distribution: Not confidential – may be shared internally or externally as appropriate

1. Introduction

Treasure Time ("we", "us", "our") is committed to safeguarding the privacy and protection of your personal data. This policy outlines our comprehensive approach to data protection in alignment with the UK General Data Protection Regulation (UK GDPR), Data Protection Act 2018, and ICO guidance. We aim to be transparent, ethical, and clear about the personal data we collect and how we use it.

2. Who we are

Treasure Time is a dedicated provider supporting parents and carers in enhancing family connections through play-based programmes. We are registered with the Information Commissioner's Office (ICO); our ICO registration number is ZB892507. For any questions or concerns about this policy or how your data is handled, please contact us at support@treasuretime.co.uk.

3. Definitions

Personal Data: Any information relating to an identified or identifiable living individual.

Special Categories: Sensitive data such as ethnicity, health, political beliefs, etc.

Data Controller: Treasure Time, responsible for deciding how personal data is processed.

Data Processor: Third parties processing data on our behalf.

Data Breach: Security incidents involving unauthorized access, loss, destruction, or disclosure of personal data.

Data Subject: The identified or identifiable individual whose personal data is held or processed.

4. Data protection principles

We adhere to principles ensuring data is:

- Processed lawfully, fairly, and transparently
- Collected for explicit and legitimate purposes
- Adequate, relevant, and limited to necessary purposes
- Accurate and up-to-date
- Stored no longer than necessary
- Secured against unauthorised access or loss

5. What data we collect and why

We collect the following categories of personal data:

- **Personal Details:** Names, emails, phones, addresses (logistical support).
- **Child Information:** First names, ages, specific needs (programme tailoring).
- **Session Reflections and Surveys:** Voluntary feedback to enhance programme quality.
- **Anonymised Session Transcripts:** Processed securely via ethical AI tools for improvement.

6. Lawful basis for data collection & processing

Our lawful bases include:

- **Consent:** Clearly obtained for participation and feedback.
- **Legitimate Interests:** Programme delivery, safeguarding, internal improvement.
- **Legal Obligation:** Safeguarding disclosures and mandatory reporting.

7. Information Sharing and Confidentiality

We maintain strict confidentiality. Data is shared externally only when legally required for safeguarding.

1:1 and group sessions are confidential, but safeguarding always overrides this.

Treasure Time is delivered as an employer-funded programme and a direct-to-consumer offer. Regardless of how access is provided, all participants engage with Treasure Time as individuals and safeguarding is managed independently from funding arrangements.

- Employers are not informed of safeguarding concerns or disclosures.
- Safeguarding concerns are only shared with appropriate statutory agencies—such as Local Authority Children's Services, the Police, or the NSPCC—never with employers or third parties.

Participants are informed that:

> **"Your employer will not be told about what you share with us. If we are worried about a child's safety, we may need to contact safeguarding services—but never your workplace."**

Information would only ever be shared with an employer in rare circumstances, such as:

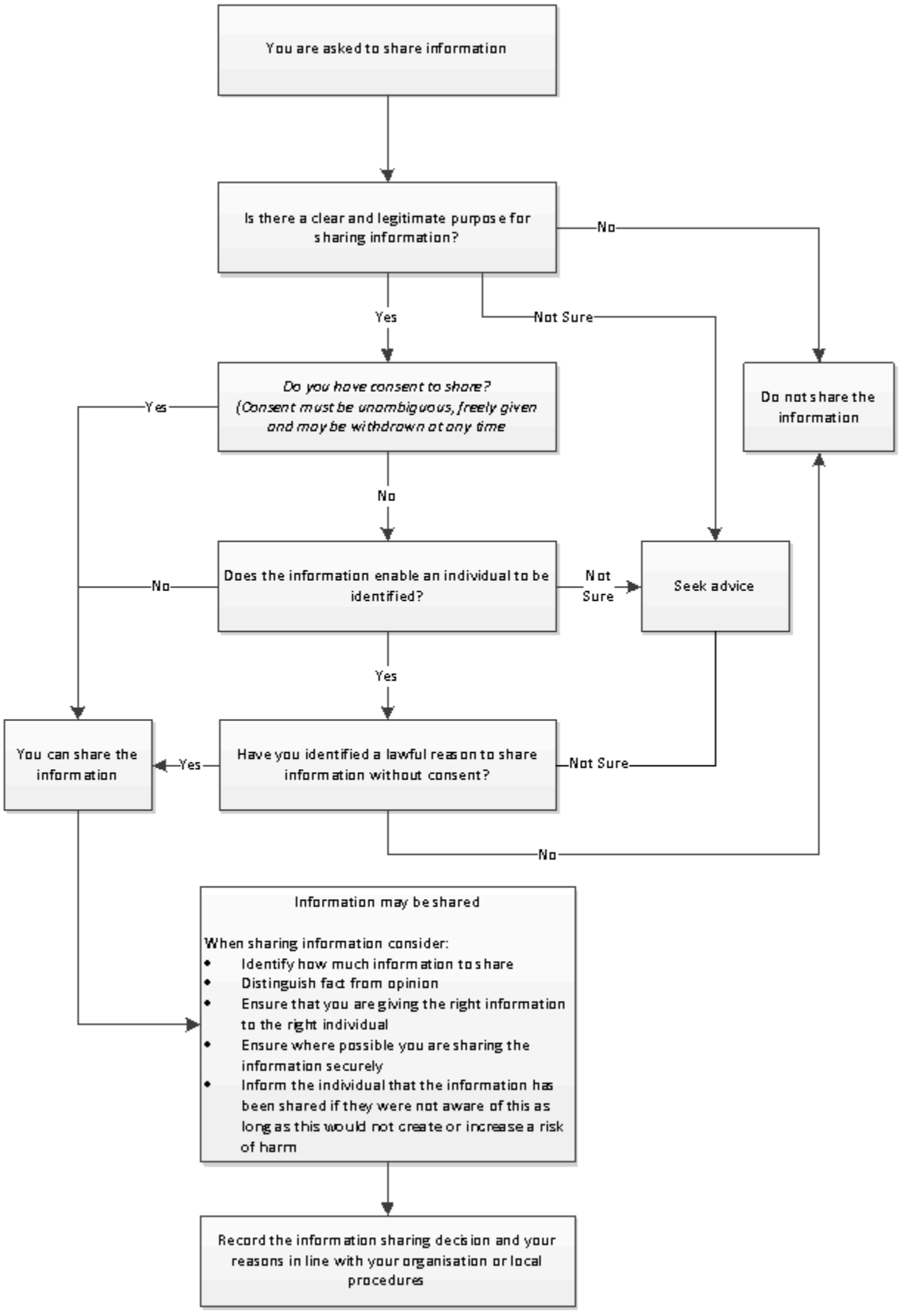
- Where the participant provides explicit, informed consent, or
- Where there is a legal safeguarding obligation involving regulated activity

If sharing is necessary:

- Determine whether there is a clear purpose
- Seek consent where it does not place the child at risk
- If consent cannot be gained and risk is high, share without consent in the child's best interest

All information shared must be:

- Necessary, proportionate, relevant, accurate, timely, secure


You are asked to share information
Is there a clear and legitimate purpose for sharing information?
No
Yes
Not Sure
Do you have consent to share? (Consent must be unambiguous, freely given and may be withdrawn at any time
Yes
Do not share the information
No
Does the information enable an individual to be identified?
No
Not Sure
Seek advice
Yes
You can share the information
Yes
Have you identified a lawful reason to share information without consent?
Not Sure
No
Information may be shared
When sharing information consider:
Identify how much information to share
Distinguish fact from opinion
Ensure that you are giving the right information to the right individual
Ensure where possible you are sharing the information securely
Inform the individual that the information has been shared if they were not aware of this as long as this would not create or increase a risk of harm
Record the information sharing decision and your reasons in line with your organisation or local procedures

8. Ethical use of AI tools

We use secure, ethical AI tools (e.g., OpenAI models) for the purpose of summarising anonymised session transcripts and reflecting on recurring themes. AI tools are not used to make decisions about participants, only to support human reflection and programme development. All data is anonymised before analysis. Participants may opt out of AI-supported analysis at any time.

9. Data protection by design & default

We embed privacy into our processes through:

- The use of secure platforms: Google Forms for onboarding, Circle for community access, and Google Workspace for all storage.
- Completion of Data Protection Impact Assessments (DPIAs) before introducing new tools that process personal or sensitive data.
- Minimal data collection: only data that is necessary for delivery, safeguarding, or evaluation is collected.
- Clear opt-out options for playbox logistics, surveys, and AI processing.
- Role-based access: data is only accessible to the small delivery team who require access, and access is reviewed periodically.

10. Third-party providers

We use reputable providers who comply with UK GDPR. These include:

- **Termly** for website policy management and cookie consent tools.
- **Circle** for our community platform. Circle stores all data in the Northeast United States via Amazon Web Services (AWS) and complies with both the GDPR and the California Consumer Privacy Act (CCPA). Circle meets the relevant compliance requirements, including transparency about how personal data is used, the right of users to access their personal data, and the right to request deletion. For more information, see their Privacy Policy, Terms, EU Notice, and Data Processing Agreement. A detailed Security Overview is also available.

- **Google Workspace** for email, collaboration, and secure cloud storage. Google Workspace holds the following certifications:
    - ISO/IEC 27001, 27017, 27018, 27701
    - SOC 1, SOC 2, SOC 3
    - FedRAMP High Authorization

      Google encrypts data at rest and in transit, offers data residency options (e.g., within the EU), and uses HTTPS and strong access controls.

We continue to review the data protection commitments of all third-party platforms used within our programme delivery.

11. Data security & storage procedures

All Treasure Time data is stored digitally using secure cloud-based tools, primarily Google Workspace. We do not hold any physical records. Our implemented practices include:

- Use of encrypted cloud storage through Google Workspace
- Password-protected accounts with restricted role-based access
- Multi-factor authentication (MFA) enabled for all user accounts
- Communication via Google Chat and Gmail, protected by HTTPS encryption
- Periodic review of account access logs for suspicious activity
- Access to cloud data only from encrypted devices with biometric/passcode protection

These measures ensure data is secure, access is controlled, and visibility over account activity is maintained, in line with ICO recommendations for small organisations.

12. Data retention & deletion

We retain personal data only as long as necessary for the purpose for which it was collected:

- Playbox delivery details: deleted within 3 months of programme completion.
- Survey responses and reflections: retained up to 12 months post-programme.
- Safeguarding records: retained according to statutory guidance.
- Anonymised data used for research or improvement is retained without identifiers.

Data is deleted securely via Google Workspace's built-in deletion and retention tools, and only by designated users with permission to manage files.

13. Subject Access Requests (SARs)

Participants have the right to request access to their personal data. We respond within one month, verifying identities, and detailing data purposes, recipients, and retention periods. Children over 12 are generally assumed to have sufficient understanding to make a request unless assessed otherwise.

14. Your rights under GDPR

Participants have the right to:

- Access, rectify, or erase data
- Restrict or object to processing
- Withdraw consent
- Data portability
- Complain to ICO

Requests can be directed to support@treasuretime.co.uk.

15. Personal data breach procedure

We have established procedures for managing data breaches:

- Immediate reporting to support@treasuretime.co.uk
- ICO notification within 72 hours
- Transparent communication with affected individuals
- Thorough documentation and review of breaches

16. Training & staff responsibilities

Staff receive onboarding and periodic training on data protection. Responsibilities include:

- Complying with this policy and safeguarding responsibilities
- Reporting any data breach, near miss, or concern immediately
- Only accessing data necessary for their work

17. Photography & videos

Explicit consent is obtained before capturing images for promotional purposes. Participants can withdraw consent at any time. Images are never published with identifying information without explicit permission.

18. Accountability & compliance monitoring

We maintain an internal record of processing activities, conduct DPIAs for AI tools and any new platform we introduce, and restrict access through permissions managed in Google Workspace and Circle. A log is maintained of access, reviews, and deletion activity.

19. Complaints

Participants may contact support@treasuretime.co.uk with any concerns about how their data is used. If unresolved, individuals may contact the ICO at ico.org.uk.

20. Policy review & updates

This policy is reviewed annually or following regulatory changes. Updates are transparently communicated.

For further details, please contact us at support@treasuretime.co.uk.