Data Protection & Privacy Policy

Purpose:

The purpose of our Data Protection & Privacy Policy is to set out how Turtle CYP will ensure that personal data relating to our customers, staff and other data subjects is:-

a. processed lawfully, fairly and in a transparent manner in relation to individuals;
b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The above sets out Turtle CYP's main responsibilities under UK data protection law which is derived from the EU's General Data Protection Regulation (GDPR). Additionally, Turtle CYP is responsible for and must be able to demonstrate compliance with the principles relating to the processing of personal data.

VERSION CONTROL MATRIX			
Date:	**Version:**	**Effect:**	**Due for Review**
July 2019	V1	July 2019	July 2022
July 2022	V2	July 2022	July 2023
July 2023	V3	July 2023	July 2024
July 2024	V4	July 2024	July 2026
October 2024	V5	October 2024	October 2026

Scope of the policy:

The principles and terms within this policy apply to all information and documentation held by Turtle CYP which relates to personal data.

Personal data is defined as any information related to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person. It can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer IP address.

The GDPR's definition of personal data is more detailed than the Data Protection Act 1998 (DPA) and makes it clear that information such as an online identifier – e.g. an IP address – can be personal data. The more expansive definition provides for a wide range of personal identifiers to constitute personal data, reflecting changes in technology and the way organisations collect information about people.

Policy Statement & Principles:

Policy Statement

We are committed to an approach to personal data which is consistent with our values.

Our Values

- Discrimination always needs to be challenged
- We all have the right to reach out potential
- We all learn and develop through our life experience
- Everybody has the right to feel included and valued

Policy Principles

As part of our commitment to our values we adopt the following principles:

VERSION CONTROL MATRIX			
Date:	**Version:**	**Effect:**	**Due for Review**
July 2019	V1	July 2019	July 2022
July 2022	V2	July 2022	July 2023
July 2023	V3	July 2023	July 2024
July 2024	V4	July 2024	July 2026
October 2024	V5	October 2024	October 2026

We believe in privacy, and we embed privacy into design

We seek to deliver the maximum degree of privacy by ensuring that personal data is automatically protected in any given IT system or business practice. If an individual does nothing, their privacy remains intact. No action is required on the part of the individual to protect their privacy – it is built into the system, by default.

Privacy is embedded into the design and architecture of our IT systems and business practices. Privacy is an essential component of the core functionality being delivered. Privacy is integral to our systems processes and practices, without diminishing functionality.

Managers and staff must consult the data protection officer when a change to the way we use personal data could introduce new privacy risks in data processing activities. This is possible when new data processing processes, systems or technologies are introduced.

We believe in visibility and transparency, and we're committed to end-to-end security

Visibility and transparency are essential to establishing accountability and trust. We seek to assure all stakeholders that whatever the IT system or process or involved, it is in fact, operating according to stated promises and objectives, subject to independent verification.

Strong security measures are essential to privacy, from start to finish. This ensures that all data is securely retained, and then securely destroyed when no longer required in a timely fashion.

We are proactive not reactive; preventative not remedial. We won't trade off privacy against other objectives.

Our approach is characterised by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen. Our approach does not wait for privacy risks to materialise, and it aims to prevent data protection incidents from occurring.

We seek to accommodate all legitimate interests and objectives in a win-win manner. We avoid unnecessary trade-offs, such as privacy vs. security, demonstrating that it is possible, and far more desirable, to have both.

VERSION CONTROL MATRIX			
Date:	**Version:**	**Effect:**	**Due for Review**
July 2019	V1	July 2019	July 2022
July 2022	V2	July 2022	July 2023
July 2023	V3	July 2023	July 2024
July 2024	V4	July 2024	July 2026
October 2024	V5	October 2024	October 2026

We respect user privacy.

Above all we keep the interests of the individual uppermost by offering measures such as strong privacy defaults and respect for data subject's rights.

Turtle CYP has nominated a Data Protection Officer as described by the GDPR. The appointment of a Data Protection Officer is not mandatory, but Turtle CYP sees the role of the Data Protection Officer as important in delivering our approach and ensuring compliance with data protection law.

Responsibilities:

Turtle CYP is responsible for and must be able to demonstrate compliance with the principles relating to the processing of personal data.

The Trustees have overall responsibility for this policy.

The Director will maintain and monitor proper arrangements for data risk management, ensuring these are effectively developed, implemented, managed, monitored and embedded across Turtle CYP

The Manager is responsible for ensuring that all staff understand the policy statement and principles and the underlying procedures and guidance. Play Leaders must also encourage the reporting of data protection incidents as part of a commitment to continuously improving standards of data protection and privacy.

All Staff are required, by the Employees Code of Conduct to abide by procedures designed to protect the confidentiality of information held about residents, customers or other employees.

The Data Protection Officer is responsible for the following tasks:

- To inform and advise Turtle CYP and its employees about their obligations to comply with the GDPR and other data protection laws;
- To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advising on data protection impact assessments; train staff and conduct internal audits; and

VERSION CONTROL MATRIX			
Date:	**Version:**	**Effect:**	**Due for Review**
July 2019	V1	July 2019	July 2022
July 2022	V2	July 2022	July 2023
July 2023	V3	July 2023	July 2024
July 2024	V4	July 2024	July 2026
October 2024	V5	October 2024	October 2026

- To be the first point of contact for supervisory authorities (the Information Commissioner's Office) and for individuals whose data is processed (employees, customers etc.).

In particular, the Data Protection Officer is responsible for ensuring that appropriate procedures and guidance on our approach to data protection and privacy are available to Committee members, managers and staff.

Our data protection and privacy procedures will set out a specific way to carry out a specific duty or activity. These will include a clear desk procedure; procedures for carrying out data protection / privacy impact assessments and procedures for complying with data subject's rights under the GDPR.

Performance Standards / Measures of success:

The following performance standards and measures of success have been identified.

- All staff confirm that they have read and understood this policy;
- Data protection and privacy training is delivered to all staff
- Number of data protection incidents;
- Number of significant data protection incidents (defined as incidents that merit reporting to the Board) and data protection breaches (defined as incidents that merit reporting to the ICO);

Diversity, Equality and Inclusion:

This policy operates in tandem with our wider Equality and Diversity policy which prohibits discrimination on the grounds of disability, age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex and sexual orientation.

VERSION CONTROL MATRIX			
Date:	**Version:**	**Effect:**	**Due for Review**
July 2019	V1	July 2019	July 2022
July 2022	V2	July 2022	July 2023
July 2023	V3	July 2023	July 2024
July 2024	V4	July 2024	July 2026
October 2024	V5	October 2024	October 2026

Assurance Framework:

The Manager will be asked to ensure that this policy is communicated to all staff and a copy of the policy will be made available in each staff folder. Awareness of our Data Protection & Privacy Policy will be reinforced on a periodic basis via training and team talks.

The Director provides assurance to the Trustee's in discharging their responsibilities for ensuring the adequacy and effectiveness of data risk management across Turtle CYP.

Risks:

Adherence to this policy helps mitigate the following risk:

"Data is amended, disclosed or withheld inappropriately or without proper authorisation leading to breaches of data protection law".

VERSION CONTROL MATRIX			
Date:	**Version:**	**Effect:**	**Due for Review**
July 2019	V1	July 2019	July 2022
July 2022	V2	July 2022	July 2023
July 2023	V3	July 2023	July 2024
July 2024	V4	July 2024	July 2026
October 2024	V5	October 2024	October 2026