# Confidentiality and Data Protection Policy

| | | | |
|---|---|---|---|
| **Organisation** | Thrive Holistic Education CIC | **Version** | 2026–27 |
| **Approved by** | Directors | **Date approved** | August 2026 |
| **Policy owner** | Directors / Data Controller | **Review date** | August 2027 |
| **Applies to** | Staff, volunteers, facilitators and relevant visitors | **Earlier review** | After a significant incident or relevant change in guidance |

## 1. Purpose

Thrive Holistic Education CIC respects the privacy of children, parents/carers, staff, volunteers and other people whose information we hold. This policy explains how personal information will be collected, used, stored, shared, retained and disposed of securely and lawfully.

Thrive Holistic Education CIC is the data controller for personal data it determines the purposes and means of processing.

## 2. Legal framework and principles

Thrive will process personal data in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and other applicable data-protection law.

- Lawfulness, fairness and transparency.
- Purpose limitation – data is collected for specified and legitimate purposes.
- Data minimisation – only information that is adequate, relevant and necessary is collected.
- Accuracy – information is kept accurate and updated where necessary.
- Storage limitation – information is kept only for as long as needed or legally required.
- Integrity and confidentiality – appropriate security is used to protect information.
- Accountability – Thrive will be able to demonstrate reasonable compliance with these principles.

## 3. Types of information we may hold

- Names, dates of birth, contact details and emergency contacts.
- Attendance and booking information.
- Health, allergy, medication, additional-needs and accessibility information where required to provide safe support.
- Accident, incident, behaviour and safeguarding records.
- Parent/carer communications and consent records.

- Photographs or video where relevant and appropriately managed.
- Staff, volunteer and recruitment information.
- Financial, invoicing, grant and accounting information.

# 4. Lawful bases

Before using personal data, Thrive will identify an appropriate lawful basis. Depending on the activity, this may include performance of a contract, compliance with a legal obligation, legitimate interests, vital interests or consent. Consent will only be relied upon where it is appropriate and can genuinely be withdrawn.

Where special category data is processed, such as health information, Thrive will also identify an appropriate additional condition for processing and apply additional safeguards.

# 5. Privacy information

People whose data is collected by Thrive will be provided with appropriate privacy information explaining what is collected, why it is needed, how it is used, who it may be shared with, how long it is kept and what rights they have.

# 6. Access and security

- Access to personal information will be limited to people who need it for their role.
- Digital devices and accounts containing personal information will be protected by appropriate passwords and security settings.
- Sensitive information must not be left where it can be accessed by unauthorised people.
- Paper records containing confidential information will be stored securely.
- Personal information must not be routinely transferred to personal devices or accounts unless an approved, secure method is in place.
- Confidential discussions about a child, family or member of staff should take place privately and only with those who need the information.

# 7. Sharing information

Personal information will not be shared merely because another person or organisation requests it. Before sharing, Thrive will consider the purpose, lawful basis, necessity and proportionality of the disclosure.

Information may be shared with parents/carers, statutory agencies, emergency services, professional advisers, service providers or other bodies where there is a lawful and necessary reason. Safeguarding information may be shared without consent where necessary to protect a child or another person.

# 8. Individual rights and Subject Access Requests

Individuals have rights under data-protection law, which may include rights to be informed, access their personal data, correct inaccurate data, request erasure in certain circumstances, restrict processing, object to processing, and data portability where applicable.

- A Subject Access Request (SAR) may be made verbally or in writing.
- Staff who receive a request must pass it promptly to a Director.

- Thrive will normally respond without undue delay and within one month of receipt, subject to lawful extensions in appropriate cases.
- Identity may be verified where reasonably necessary.
- Information about other individuals will be protected where required.
- A parent/carer request concerning a child will be considered in light of the child's rights, capacity and the circumstances of the request.

# 9. Photographs, video and social media

- Thrive will obtain and record appropriate consent/permission for uses that rely on consent.
- A child will not be pressured to take part in photographs or recordings.
- Images used publicly will avoid unnecessary identifying information.
- Staff must not post identifiable images or confidential information about Thrive children on personal social media accounts.
- Withdrawal of consent will apply to future use where reasonably practicable; it may not always be possible to remove material already lawfully published or distributed.

# 10. Personal data breaches

A personal data breach includes accidental or unlawful loss, destruction, alteration, unauthorised disclosure of, or access to personal data.

1. Any suspected breach must be reported to a Director immediately.
2. The incident will be contained where possible and recorded in a breach log.
3. Thrive will assess the likely risk to people's rights and freedoms.
4. Where the legal reporting threshold is met, Thrive will notify the Information Commissioner's Office without undue delay and, where feasible, within 72 hours of becoming aware of the breach.
5. Where a breach is likely to result in a high risk to affected individuals, they will be informed without undue delay where required.
6. Actions and learning arising from the breach will be recorded.

# 11. Retention and disposal

Thrive will not keep personal data indefinitely simply because it may be useful. Records will be retained for a period appropriate to their purpose and any legal, safeguarding, insurance, contractual or financial requirements. Retention periods will be reviewed periodically.

| Record type | General approach | Notes |
|---|---|---|
| Child registration/contact records | Keep while the child attends, then retain only as long as there is a justified operational/legal need. | Review at end of attendance. |
| Attendance registers | Retain for an appropriate period for safeguarding, operational and insurance purposes. | Apply a documented retention period. |
| Safeguarding records | Retain securely in accordance with safeguarding, limitation and professional guidance. | Do not destroy simply because a child leaves. |
| Accident/incident records | Retain in line with applicable limitation, insurance and statutory requirements. | Longer periods may apply where a child is involved. |
| Medical/medication information | Keep while required for safe provision; archive only where there is a justified legal or safeguarding reason. | Avoid retaining obsolete health information. |

| | | |
|---|---|---|
| Photograph/video consent | Keep while the relevant images/use remain active and for a reasonable audit period. | Record withdrawal where applicable. |
| Staff/recruitment/personnel records | Retain according to employment, safeguarding, DBS and limitation requirements. | Do not retain unnecessary DBS certificate copies. |
| Accounting/tax/grant records | Retain for the period required by company, tax, grant and funding obligations. | Follow current HMRC/Companies House/funder rules. |
| Complaints and significant correspondence | Retain according to seriousness, safeguarding implications and potential legal/insurance need. | Link to associated incident records where relevant. |

The table above is an operational framework rather than a substitute for checking any statutory retention period that applies to a particular record.

# 12. Secure disposal

- Paper records containing personal information will be shredded or securely destroyed.
- Electronic records will be securely deleted, including from routinely accessible backups where practicable and appropriate.
- Storage devices will be securely erased or physically destroyed before disposal where they contain confidential information.

# 13. Breaches of confidentiality

Unauthorised access, use or disclosure of confidential information may be treated as a serious matter and may result in disciplinary action or other appropriate steps. Safeguarding concerns arising from misuse of information will also be considered under the Safeguarding Policy.

# 14. Relevant guidance

- UK General Data Protection Regulation (UK GDPR).
- Data Protection Act 2018.
- Information Commissioner's Office (ICO) guidance, including guidance on lawful processing, subject access and personal data breaches.

# Policy review and approval

This policy will be reviewed at least annually and earlier where there is a significant incident, a material change to Thrive's provision, or a relevant change in legislation or official guidance.

| | |
|---|---|
| **Approved by** | Directors of Thrive Holistic Education CIC |
| **Date** | August 2026 |
| **Signed** | _____ |
| **Next scheduled review** | August 2027 |