Thallo
ALTERNATIVE PROVISION

Data Protection and Confidentiality Policy

Thallo Education Ltd.

VERSION: 1.0
DATE: 25th September 2026
AUTHOR: May MacKay-Morris

Data Controller	Thallo Education Ltd
Data Protection Lead	May MacKay-Morris Provision Lead / Director
Data Protection Contact	may@thalloeducation.co.uk / 07811143355
ICO Registration Number	00015671299
Approved by	May MacKay-Morris Provision Lead / Director
Approval Date	25th September 2026
Review Date	September 2027, or sooner, following relevant change.

1. Purpose and scope

Thallo Alternative Provision is committed to protecting personal information and respecting the privacy and confidentiality of children and young people, parents and carers, staff, volunteers, contractors, commissioners and other people whose information we process.

This policy explains the principles and arrangements Thallo uses to collect, record, use, store, share, retain and dispose of personal information. It applies to all staff, volunteers, contractors and other people processing personal information on behalf of Thallo.

2. Legal framework and accountability

Thallo will process personal information in accordance with applicable data protection legislation, including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 as amended, including relevant changes made by the Data (Use and Access) Act 2025, together with current guidance issued by the Information Commissioner's Office (ICO).

Thallo will identify and document the purpose and appropriate lawful basis for each significant processing activity before processing begins. Where special category data is processed, Thallo will also identify and document an applicable Article 9 condition and any relevant condition under the Data Protection Act 2018. Where criminal offence data is processed, the additional legal requirements for that information will be considered.

Thallo will comply with the data-processing arrangements agreed for commissioned services. Thallo will fulfil its own controller responsibilities and comply with the agreed Data Processing Schedule.

3. Data protection principles

Thallo will ensure personal information is:

- processed lawfully, fairly and transparently;
- collected for specified, explicit and legitimate purposes and not used incompatibly with those purposes;
- adequate, relevant and limited to what is necessary;
- accurate and, where necessary, kept up to date;
- kept in identifiable form only for as long as necessary;
- processed securely using appropriate technical and organisational measures;
- managed in a way that enables Thallo to demonstrate accountability and compliance.

4. Information Thallo may process

Depending on the relationship and purpose, Thallo may process information including:

- names, dates of birth, addresses, contact details and other identifiers;
- parent/carer and emergency contact information;
- referral, commissioning and placement information;
- attendance, engagement, progress, learning, assessment and outcome information;
- SEND information, EHCP information and communication or accessibility needs;
- health, medical, allergy, dietary and medication information;
- safeguarding, child protection, social care and professional involvement information;
- equality and demographic information where required or appropriate;

- risk assessments, incident and accident records;
- staff, volunteer and contractor recruitment, vetting, qualification, training, payroll and employment information;
- complaints, correspondence and records necessary for contract management, safeguarding or legal compliance.

Thallo will not collect personal information simply because it might be useful. The information collected will be limited to what is reasonably necessary for an identified purpose.

5. Why we process information

Personal information may be processed in order to:

- assess referrals and suitability and arrange commissioned placements;
- deliver safe, appropriate and individually responsive education and support;
- understand a young person's needs, risks, reasonable adjustments and agreed outcomes;
- record and report attendance, engagement, progress and outcomes;
- safeguard children and respond to welfare concerns;
- communicate with young people, parents/carers, commissioners and relevant professionals;
- meet contractual, safeguarding, health and safety, employment, financial and other legal obligations;
- manage staff, volunteers and contractors and maintain safer-recruitment records;
- respond to complaints, requests, incidents and legal claims;
- monitor and improve the quality, safety and effectiveness of Thallo's services.

6. Lawful bases and special category information

Thallo may rely on different lawful bases for different processing purposes. These may include legal obligation, legitimate interests, performance of a contract where the legal requirements for that basis are met, vital interests, consent, and public task only where Thallo can demonstrate that the particular task or function has the necessary basis in law.

Consent will not be used as a blanket lawful basis for core educational, safeguarding or contractual processing where another basis is more appropriate. Where consent is relied upon, it will be specific, informed, freely given where required, recorded and capable of withdrawal.

Information about health, disability, ethnicity, religion and certain other matters may constitute special category data. An Article 6 lawful basis alone is not sufficient for this information. Thallo will identify an applicable Article 9 condition and, where required, a Data Protection Act 2018 Schedule 1 condition and appropriate policy documentation before processing.

7. Collecting information and privacy information

Thallo may receive personal information directly from a young person, parent/carer, member of staff or contractor, and from third parties such as Suffolk County Council, a commissioning school or setting, social care, health professionals, other education providers or relevant agencies.

At or around the time information is collected, Thallo will provide appropriate privacy information explaining who we are, what information we use, why we use it, the lawful basis, who it may be shared with, how long it is kept and the rights available to the individual. Privacy

information for children will be written or explained in a form appropriate to their age and understanding.

8. Confidentiality and access

Personal information is confidential and will only be accessed by people who need it for an authorised purpose. Staff must not discuss confidential information where it may be overheard or disclose it to friends, family members or unauthorised colleagues.

Safeguarding information will be handled in accordance with Thallo's Safeguarding and Child Protection Policy. Confidentiality does not prevent information being shared where this is lawful and necessary to protect a child or another person from harm.

9. Information sharing

Thallo may share relevant personal information with Suffolk County Council, commissioning schools or settings, education providers, children's social care, health services, police, safeguarding bodies, awarding organisations and other agencies where there is an appropriate lawful basis and the sharing is necessary and proportionate.

Before routine or significant sharing, staff will consider the purpose, lawful basis, necessity, proportionality, accuracy and security of the information. Only information necessary for the purpose will be shared. Where appropriate, the individual will be informed about the sharing unless doing so would be unsafe, unlawful or prejudice a safeguarding or other investigation.

Sensitive information will be transferred through secure methods appropriate to the risk. This may include approved secure portals, encrypted systems, password-protected files with passwords communicated separately, or other approved secure transfer arrangements. Physical records will be transferred securely and tracked where appropriate.

10. Storage and information security

Thallo uses Google Workspace for organisational email, document storage and collaboration, and MosaicEd as its management information system for learner and provision records. Access to these systems is restricted to authorised users according to role and operational need. Thallo documents its electronic storage, hosting, access, security, back-up and secure-transfer arrangements in its data map / Record of Processing Activities and in relevant commissioner Data Processing Schedules.

Thallo will use appropriate technical and organisational measures to protect personal information against unauthorised or unlawful access, accidental loss, destruction, alteration or disclosure.

- access to electronic records will be restricted according to role and need;
- organisational accounts and devices will use appropriate passwords and security controls, including multi-factor authentication where enabled for the relevant system;
- all staff computers used for Thallo work must have encrypted hard drives and be kept updated and appropriately secured;
- Thallo information will be accessed and stored only through approved organisational systems and devices; personal email accounts and unapproved personal devices must not be used for learner or commissioner records;
- paper records containing sensitive information will be minimised and, where required, stored securely with controlled access;

- safeguarding records will be kept securely with access restricted to those with a professional need to know;
- staff will use approved secure methods for sharing personal and special category information;
- confidential material will be disposed of securely;
- staff computers and other Thallo devices must be locked in a secure, lockable storage cupboard when not in use.

11. Retention and disposal

Thallo will maintain a retention schedule setting out how long categories of information are retained. Retention periods will be based on the purpose for which information is held, applicable legal or contractual requirements, safeguarding considerations and recognised sector guidance. Information will not be retained indefinitely simply because storage is available.

At the end of the retention period, information will be securely deleted, destroyed or anonymised unless there is a lawful reason to retain it for longer. On the end or termination of a commissioned arrangement, Thallo will also comply with any applicable requirements concerning return, transfer or deletion of commissioner information.

12. Data subject rights

Individuals have rights under data protection law which may include the rights to be informed, access personal information, have inaccurate information rectified, request erasure or restriction in certain circumstances, object to certain processing, data portability in certain circumstances, and rights relating to automated decision-making.

These rights are not absolute and whether a right applies depends on the nature and lawful basis of the processing. Requests should be sent to Thallo's Data Protection Lead. Thallo will verify identity where appropriate, record the request and respond within the applicable statutory timescale.

Thallo has not appointed a statutory Data Protection Officer (DPO). At its current scale, Thallo has appointed a Data Protection Lead as the operational contact for data protection matters. The need for a statutory DPO will be kept under review as the organisation and its processing activities develop.

Where a parent or carer asks to access information relating to a child, Thallo will consider the child's own data protection rights, age, competence, circumstances and any safeguarding implications before disclosure.

13. Children's information

Children merit particular protection when their personal information is processed. Thallo will design its information-handling arrangements with children's interests in mind and will explain privacy and information sharing in accessible language wherever appropriate.

Where Thallo relies on consent for an optional processing activity involving a child, it will consider whether the child can provide valid consent and whether parental authorisation is required. Consent will not be assumed merely because a parent/carer has made a referral.

14. Photographs, video and recordings

Images, video and audio recordings are personal information and will only be created, used, stored or shared for an identified purpose and lawful basis. Consent will be obtained where consent is the appropriate basis, for example for optional promotional use. Safeguarding or evidential images will be handled according to the applicable safeguarding and legal basis rather than relying automatically on consent.

Staff must not retain images of young people on personal devices or personal cloud accounts. Any authorised images will be stored and deleted in accordance with Thallo's approved systems and retention arrangements.

15. Data processors, suppliers and sub-processors

Where an external organisation processes personal information on Thallo's behalf, including providers of cloud, management information and other technology services, Thallo will carry out appropriate due diligence and ensure that appropriate contractual and data-processing terms are in place. Thallo uses Google Workspace and MosaicEd and will keep the data-protection and security arrangements for these services under review.

Where Suffolk County Council's Data Processing Schedule requires prior notification or written consent before a sub-processor is used for information connected with the contract, Thallo will obtain that approval before the processing begins.

16. Data protection impact assessments

Thallo will consider whether a Data Protection Impact Assessment (DPIA) is required before introducing processing that is likely to result in a high risk to individuals' rights and freedoms. This may be particularly relevant when introducing new technologies, extensive sensitive-data processing, systematic monitoring or materially new ways of using children's information.

Thallo will provide reasonable assistance to Suffolk County Council with DPIAs relating to commissioned processing where required by the contract.

17. Personal data breaches

A personal data breach includes accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal information. Examples may include sending information to the wrong recipient, loss of an unencrypted device, unauthorised access to a record, accidental publication or loss of paper files.

Any suspected or actual personal data breach must be reported immediately to the Data Protection Lead. Thallo will contain and investigate the incident, assess the risk to individuals, record the breach and take corrective action.

Where required, Thallo will notify the ICO without undue delay and, where feasible, within 72 hours of becoming aware of a reportable breach. Where the breach is likely to result in a high risk to individuals, affected people will also be informed where required. For data breaches connected with the Suffolk CD1397 contract, Thallo will notify Suffolk County Council in accordance with the Data Processing Schedule, including the Provider Services Team and CYP Business & Information Team within 48 hours of discovery, or any replacement contacts/timescale notified by the Council. Other commissioner-specific notification requirements will also be followed.

18. Requests, complaints and the ICO

Questions, requests or concerns about Thallo's use of personal information should be directed to the Data Protection Lead using the contact details at the beginning of this policy. The Data Protection Lead is May MacKay-Morris, Provision Lead / Director. Thallo will investigate concerns and respond appropriately.

Individuals also have the right to raise a data protection concern with the Information Commissioner's Office. Thallo will cooperate with the ICO and with Suffolk County Council in relation to relevant data protection enquiries, complaints, audits or requests.

19. Staff training and compliance

All staff, volunteers and contractors who handle personal information will receive appropriate data-protection and confidentiality information or training as part of induction and thereafter at intervals appropriate to their role. Additional guidance will be provided where roles involve safeguarding records, special category information, information sharing or data-system administration.

Failure to follow this policy may result in restriction of access to information or systems and, where applicable, disciplinary, contractual or safeguarding action.

20. Monitoring and review

The Data Protection Lead will monitor compliance through review of information-handling practices, data subject requests, breaches and near misses, training, retention arrangements, processor agreements and any relevant commissioner or ICO feedback.

This policy will be reviewed at least annually and sooner following a significant data incident, material change to Thallo's processing, changes to the CD1397 Data Processing Schedule, or relevant changes in legislation or ICO guidance.

21. Related documents and information-governance records

- Privacy Notice for Young People and Parents/Carers
- Workforce Privacy Notice
- Data Retention Schedule
- Record of Processing Activities / data map
- Data Breach Procedure and Breach Log
- Subject Access / Data Rights Procedure
- Suffolk Provider Services Data Processing Schedule
- Safeguarding and Child Protection Policy