

Data Protection Policy





DATA PROTECTION POLICY

Thrive Lincs Ltd

Policy owner	Mark Haggis, Director
Data Protection Officer	Philippa Miller
Version	2.0
Original issue date	20 August 2023
Current approval date	15 August 2026
Next review date	15 August 2027

Contact: Data protection enquiries, rights requests and complaints should be directed to Philippa Miller through Thrive Lincs Ltd's published office contact details. Staff must report suspected personal data breaches immediately through the internal breach-reporting route.

1. Policy statement

Thrive Lincs Ltd is committed to protecting the personal data of learners, parents and carers, employees, workers, applicants, contractors, commissioners, partner professionals and other people who come into contact with its services. Data protection is an essential part of safe practice, safeguarding, governance and public trust.

Thrive will process personal data in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, the Data (Use and Access) Act 2025 and other applicable law and guidance. Personal data will be used only where necessary for clear, lawful purposes and will be protected throughout its lifecycle.

2. Scope

This policy applies to all employees, workers, tutors, mentors, volunteers, agency staff and contractors working for or on behalf of Thrive Lincs Ltd. It applies to personal data in any format, including paper files, electronic records, email, messages, cloud systems, photographs, video, audio and information held on approved devices.

It covers learner and family records, education and attendance information, safeguarding and welfare information, medical and special educational needs information, staff and recruitment records, payroll and financial information, commissioner and professional contacts, and any other information from which a living person can be identified directly or indirectly.



3. Legal framework

- UK General Data Protection Regulation;
- Data Protection Act 2018;
- Data (Use and Access) Act 2025;
- Privacy and Electronic Communications Regulations 2003, where applicable;
- Human Rights Act 1998;
- common-law duty of confidentiality; and
- relevant statutory safeguarding and information-sharing guidance.

4. Data protection principles

Thrive Lincs Ltd will ensure that personal data is:

- processed lawfully, fairly and transparently;
- collected for specified, explicit and legitimate purposes;
- adequate, relevant and limited to what is necessary;
- accurate and, where necessary, kept up to date;
- retained for no longer than necessary;
- processed securely, with protection against unauthorised or unlawful processing and accidental loss, destruction or damage; and
- managed in a way that enables Thrive to demonstrate compliance with these principles.

5. Data controller and processor roles

Thrive Lincs Ltd is the data controller where it determines why and how personal data is processed. In some commissioned arrangements, Thrive may act as a processor or joint controller. The role and responsibilities of each party will be established before processing begins and recorded in an appropriate contract or data-sharing agreement.

Where Thrive acts as a processor, it will process personal data only on the controller's documented instructions unless the law requires otherwise. Where Thrive acts as a controller, it remains responsible for demonstrating compliance and responding to individuals' rights.

6. Responsibilities

6.1 Director – Mark Haggis

- holds overall organisational accountability for compliance;
- ensures that adequate resources, systems, training and governance arrangements are available;
- supports the independence of the Data Protection Officer;
- ensures significant risks and breaches receive appropriate senior oversight; and



- approves this policy and monitors implementation.

6.2 Data Protection Officer – Philippa Miller

- informs and advises Thrive and its staff about their data-protection obligations;
- monitors compliance, training, audits and the allocation of responsibilities;
- advises on Data Protection Impact Assessments and monitors their completion;
- oversees data-rights requests, complaints and personal data breach assessments;
- acts as the contact point for individuals and the Information Commissioner's Office (ICO); and
- reports directly to the Director on data-protection matters.

The DPO must be involved promptly in matters relating to personal data, provided with appropriate time, access and resources, and permitted to perform the role independently. The DPO must not be instructed about the conclusions to reach, dismissed or penalised for performing DPO duties, or assigned duties that create a conflict of interest. Any actual or potential conflict must be declared and resolved.

6.3 Managers and administrators

- implement this policy within their areas;
- ensure records are accurate, secure and accessible only to authorised people;
- refer rights requests, complaints and breaches to the DPO immediately;
- complete required checks, records and actions; and
- ensure access is removed promptly when a person changes role or leaves.

6.4 All staff, workers and contractors

- use personal data only for authorised work purposes and only to the extent necessary for their role;
- follow privacy, confidentiality, security and record-keeping procedures;
- use approved systems and devices;
- check recipients and attachments before sending information;
- keep passwords and access credentials confidential;
- complete required training; and
- report loss, unauthorised access, misdirected communications or any suspected breach immediately.

7. Information held

7.1 Learners and families

- identity, address, date of birth and contact details;



- parental responsibility and emergency contacts;
- attendance, engagement, education, progress and support records;
- special educational needs, disability, health, medication and accessibility information;
- behaviour, wellbeing, safeguarding and risk information;
- communications with learners, families, commissioners and professionals; and
- photographs, video or audio where there is a defined lawful purpose.

7.2 Staff, applicants and contractors

- identity, contact, right-to-work and recruitment information;
- employment, contract, payroll, pension and absence information;
- qualifications, training, supervision and performance records;
- health and reasonable-adjustment information; and
- DBS and safer-recruitment information.

7.3 Commissioners and professionals

- names, roles and professional contact details;
- placement, referral, review and contractual information; and
- professional correspondence and meeting records.

8. Lawful processing

Before processing begins, Thrive will identify and record an appropriate Article 6 UK GDPR lawful basis for each purpose. Depending on the circumstances, this may be legal obligation, contract, vital interests, public task, legitimate interests or consent. Thrive will not treat these bases as interchangeable. Public task will be used only where the task has an appropriate basis in law. Where legitimate interests are used, Thrive will document the purpose, necessity and balancing assessment. Consent will be used only where it is freely given, specific, informed and unambiguous and can be withdrawn without detriment. Consent will not normally be used for routine safeguarding, employment or commissioned-service processing where another basis is more appropriate.

The applicable purposes, lawful bases and retention arrangements will be recorded in Thrive's Record of Processing Activities and relevant privacy notices.

9. Special category data

Thrive processes information requiring additional protection, including health, disability, racial or ethnic origin, religious or philosophical beliefs and, where relevant, sexual orientation or other special-category data. For each purpose, Thrive will identify an Article 6 lawful basis and an Article 9 condition. Where



required, it will also identify the relevant Schedule 1 condition under the Data Protection Act 2018 and maintain an Appropriate Policy Document. Special-category data will be collected only where necessary, subject to heightened security and accessed only by people who need it for an authorised purpose.

10. Criminal offence and DBS data

Criminal-offence data will be processed only under official authority or where authorised by UK law and supported by an appropriate Schedule 1 condition. Thrive will maintain an Appropriate Policy Document where required and restrict access to authorised staff.

DBS certificate information will be handled in accordance with the DBS Code of Practice. Certificates will not normally be copied or retained unnecessarily. Where lawful, Thrive may record the certificate number, date, level, workforce, barred-list information and recruitment decision. Information will be securely destroyed when no longer required.

11. Privacy information and children

Thrive will provide clear privacy information when it collects personal data or, where information is obtained from another source, within the period required by law. Privacy notices will explain purposes, lawful bases, data categories, recipients, retention, rights, complaints and any international transfers. Separate or layered notices may be used for learners and families, staff and applicants, contractors and website users.

Children's data receives particular protection. Information addressed to children will be concise, transparent and written in age-appropriate language. Personal data about a child belongs to the child. Where a child is competent to understand and exercise their rights, Thrive will normally respond to the child. A parent or carer may act where authorised or where appropriate having regard to the child's age, understanding, best interests and circumstances.

12. Individual rights

Depending on the circumstances and lawful basis, individuals may have the right to:

- be informed about the use of their data;
- access their personal data;
- have inaccurate data corrected;
- request erasure;
- request restriction of processing;
- receive or transfer certain data in a portable format;
- object to processing;
- withdraw consent where consent is relied upon; and
- receive safeguards relating to solely automated decisions and profiling.



Requests do not need to mention data-protection law or identify a particular right. Anyone receiving a request must forward it to the DPO immediately. Thrive will respond without undue delay and within the applicable statutory period. If a request is refused or restricted, Thrive will explain the lawful reason and the right to complain to the ICO.

13. Subject access requests

A subject access request may be made verbally or in writing, including through social media or to any member of staff. Requests will be logged promptly. Thrive will clarify the scope where reasonably necessary and conduct reasonable and proportionate searches of relevant paper records, systems, email and approved communications.

Thrive will respond without undue delay and normally within one month. Where legally permitted because a request is complex or several requests have been made, the period may be extended by up to two further months. The requester will be told within the initial month of the extension and reasons.

Thrive may request information reasonably necessary to confirm identity where there are reasonable doubts. Only proportionate identification will be requested. Responses are normally free of charge, but a reasonable fee may be charged or a request refused where the law permits, including where it is manifestly unfounded or excessive.

Before disclosure, Thrive will consider third-party information, confidentiality, safeguarding risks and applicable exemptions. Information will be redacted or withheld only where lawful, and responses will be provided securely.

14. Accuracy and record quality

Staff must take reasonable steps to ensure personal data is accurate and up to date. Factual information should be distinguished from professional opinion where appropriate. Challenges to accuracy will be considered promptly, and corrections or supplementary statements recorded where required. Relevant recipients will be informed of corrections where the law requires.

15. Information sharing

Personal data will be shared only where lawful, necessary and proportionate. Before sharing, staff must confirm the recipient's identity and authority, share the minimum necessary information, use an approved secure method and record significant decisions. Routine sharing will be supported by appropriate contracts, information-sharing protocols or data-sharing agreements. Information may be shared with local authorities, schools, commissioners, safeguarding partners, health professionals, police, courts, regulators and other relevant bodies where a lawful basis applies. Consent is not required where another lawful basis applies. Necessary safeguarding sharing must not be delayed solely because consent has not been obtained, but individuals



should normally be informed unless this would be unsafe, unlawful or prejudice an investigation.

16. Information security

- access will be role based and limited to the minimum necessary;
- multi-factor authentication will be used where available and appropriate;
- devices and accounts will use secure passwords, screen locking, updates, malware protection and encryption where proportionate;
- confidential information will be sent only through approved secure systems, with recipients and attachments checked before sending;
- personal data must not be stored in personal email, personal cloud storage or unapproved applications;
- use of personal devices must be specifically authorised and subject to Thrive's security requirements;
- paper records will be secured when unattended and transported only where necessary;
- backups will be protected and tested in accordance with business-continuity arrangements;
- access permissions will be reviewed and removed promptly when no longer required; and
- staff will receive induction and refresher training appropriate to their role.

17. Suppliers, processors and cloud services

Before appointing a processor, Thrive will complete proportionate due diligence covering security, confidentiality, data location, resilience, deletion and sub-processing. A written contract meeting Article 28 UK GDPR requirements will be in place. Processor compliance and continued suitability will be reviewed periodically.

18. International transfers

Personal data will not be transferred outside the UK unless the transfer is lawful and appropriate safeguards are in place. These may include UK adequacy regulations, the UK International Data Transfer Agreement, the UK Addendum to the EU Standard Contractual Clauses or another permitted mechanism. A transfer-risk assessment will be completed where required.

19. Data protection by design and DPIAs

Privacy and security will be considered from the earliest stage of new projects, systems, contracts and working practices. Default settings will limit collection, access, use and retention to what is necessary.



A Data Protection Impact Assessment (DPIA) will be completed before processing likely to result in a high risk to individuals. This may include new technology, systematic monitoring, profiling, large-scale special-category processing or significant processing involving vulnerable learners. The DPO will advise on and monitor the DPIA. High residual risk will be referred to the ICO before processing where the law requires.

20. Photographs, video and audio

Images and recordings will be created and used only for a defined, lawful and communicated purpose. Internal educational use, safeguarding evidence and external publication will be considered separately. Where consent is relied upon, it must be specific and capable of withdrawal. Withdrawal will not make earlier lawful processing unlawful.

Staff must not use personal devices to photograph or record learners unless expressly authorised under a documented arrangement. Recordings must be transferred promptly to an approved system and deleted from the source device when required. Publication must follow Thrive's safeguarding, consent and communications controls.

21. Retention and secure disposal

Thrive will maintain a Data Retention Schedule specifying a retention period or review criterion for each category of record. Decisions will take account of statutory and contractual requirements, safeguarding needs, commissioner requirements, limitation periods and the need to establish, exercise or defend legal claims.

When information is no longer required, paper records will be securely destroyed and electronic information securely deleted or placed beyond normal operational use. Backup copies will be overwritten or deleted through the normal secure backup cycle. Disposal will be suspended where information is subject to a rights request, complaint, investigation, legal hold or ongoing safeguarding need.

22. Personal data breaches

A personal data breach includes accidental or unlawful loss, destruction, alteration, unauthorised disclosure of, or access to personal data. Examples include information sent to the wrong recipient, lost devices or papers, inappropriate access, compromised accounts and unavailable or corrupted records.

Any suspected breach must be reported immediately to Philippa Miller, DPO, using the internal breach-reporting route. Staff must preserve evidence, follow containment instructions and must not conceal, investigate independently or contact affected people unless authorised.

The DPO will coordinate an assessment of the nature, scope, affected people, likely consequences and containment measures. All breaches will be documented, including the facts, effects, decisions and remedial action.



Where a breach is likely to risk people's rights and freedoms, Thrive will notify the ICO without undue delay and, where feasible, within 72 hours of awareness. Where the risk is high, affected individuals will be informed without undue delay. Initial notification may be supplemented as further facts become available.

23. Complaints

Data-protection complaints may be made verbally or in writing to Philippa Miller, DPO. Thrive will acknowledge a complaint within 30 days, take appropriate steps to investigate it without undue delay, keep the complainant appropriately informed and communicate the outcome. Complaints will be recorded and used to identify improvements.

Individuals may complain to the Information Commissioner's Office if dissatisfied. Thrive will provide the ICO's contact details and cooperate with any enquiry. No person will be disadvantaged for raising a genuine concern in good faith.

24. Training, monitoring and audit

All staff will receive data-protection and confidentiality training at induction and appropriate refresher training. Additional training will be provided for people handling safeguarding, special-category, criminal-offence, recruitment, payroll or rights-request information.

The DPO will monitor compliance through training records, audits, breach and complaint trends, rights-request handling, access reviews, retention checks, processor reviews and DPIAs. Findings and required actions will be reported to the Director and tracked to completion.

25. Records and related documents

- Record of Processing Activities;
- privacy notices for learners and families, staff and applicants, and website users;
- Data Retention Schedule;
- Appropriate Policy Document;
- information-sharing agreements and processor contracts;
- Data Protection Impact Assessments;
- Legitimate Interests Assessments;
- personal data breach log and response procedure;
- Subject Access Request and Individual Rights Procedure;
- Information Security and Acceptable Use Policy;
- Safeguarding and Child Protection Policy; and
- staff confidentiality and training records.



26. Review

This policy will be reviewed at least annually and sooner following material legal or regulatory change, a serious breach, a significant complaint, introduction of high-risk processing, a major system or contractual change, or evidence that arrangements are ineffective. The latest approved version will be made available to staff and superseded versions archived.



27. Approval

This policy is approved on behalf of Thrive Lincs Ltd and takes effect from the approval date shown below.

Name	Mark Haggis
Position	Director
Signature	
Date	15 August 2026