



LIGHTHOUSE

LEARNING PROVISION

— BELONG • GROW • ACHIEVE • THRIVE —

— PRACTICAL LEARNING. EMOTIONAL GROWTH. PREPARATION FOR ADULTHOOD. —

OPERATIONAL AND PUBLIC POLICY

Data Protection Policy and Privacy Notice

Belong • Grow • Achieve • Thrive

Organisation	Lighthouse Learning Provision Ltd
Policy owner	Board of Directors / Data Protection Lead
Data Protection Lead	Rachel Waldron - Director
Safeguarding information lead	Adam Waldron - Director and Designated Safeguarding Lead
Approved / published	July 2026 Version 2.0
Review	July 2027, or sooner following relevant legal, safeguarding, technological, operational or commissioning change

Children's information receives enhanced protection. Confidentiality is important, but it must never delay necessary and proportionate information sharing to safeguard a child.

Policy at a glance

Lighthouse handles personal information lawfully, fairly, transparently and securely. We collect only what is needed, explain how it is used, restrict access, respond to rights and complaints, record information-sharing decisions and act immediately when information is lost, misdirected or accessed without authority.

Contents

1. Purpose and aims
2. Scope, status and legal framework
3. Definitions and data-protection principles
4. Governance, accountability and named responsibilities
5. Data Protection Officer assessment
6. Information inventory, records of processing and ownership
7. Data protection by design, default and impact assessment
8. Lawful bases and purpose limitation
9. Special-category and criminal-offence information
10. Children's information and best interests
11. Privacy information and transparency
12. Consent and optional processing
13. Referral, placement, education and safeguarding records
14. Working with schools, Local Authorities and other commissioners
15. Workforce, recruitment, DBS and contractor information
16. Information sharing and disclosure decisions
17. Accuracy, minimisation and access control
18. Email, devices, remote working and physical records
19. Photography, video, audio and learner work
20. Website, cookies, social media and direct communications
21. Suppliers, processors, contracts and international transfers
22. Retention, archiving and secure disposal
23. Individual rights and subject access requests
24. Children, parents, carers and access requests
25. Data-protection complaints and external escalation
26. Personal-data breaches and cyber incidents
27. CCTV, access systems and new monitoring technology
28. Training, audit, assurance and policy review
29. Reference framework
- Appendices A-K

1. Purpose and aims

1.1 This policy establishes how Lighthouse Learning Provision Ltd collects, uses, shares, stores, protects, reviews and disposes of personal information relating to learners, families, employees, self-employed practitioners, directors, applicants, commissioners, visitors, suppliers and other people connected with the provision.

1.2 It is designed to ensure that personal information is used in a way that supports safe and effective education, safeguarding, health and safety, lawful business operation and fair treatment of individuals.

1.3 Lighthouse will:

- build privacy and security into referral, placement, staffing, technology and service decisions;
- give children and adults clear, accessible information about how their information is used;
- identify a lawful basis and, where required, an additional condition before processing sensitive information;
- share information promptly where necessary to safeguard a child or another person;
- keep accurate records of significant processing, decisions, disclosures, requests, complaints and breaches;
- use suppliers and systems only after proportionate privacy and security checks; and
- support people to exercise their rights without fear of disadvantage.

2. Scope, status and legal framework

2.1 This policy applies to information in any form, including paper records, email, cloud systems, laptops, phones, photographs, video, audio, website forms, learning platforms, referral documents, safeguarding records, finance records and information communicated verbally.

2.2 It applies to directors, employees, self-employed practitioners, contractors, agency workers, volunteers and any other person using information for or on behalf of Lighthouse. Contractual or employment status does not reduce confidentiality, security or reporting responsibilities.

2.3 Lighthouse is a private limited company and an independent non-school alternative provision provider. It is normally a data controller for information used for its own safeguarding, staffing, health and safety, legal, contractual and operational purposes. For some commissioned activities, the parties may each be independent controllers, joint controllers or controller and processor. The actual arrangement must be documented rather than assumed from labels in a contract.

2.4 The principal legal framework is the UK General Data Protection Regulation, the Data Protection Act 2018 as amended, the Data (Use and Access) Act 2025, the Privacy and Electronic Communications Regulations where applicable, and relevant safeguarding, employment, equality, health and safety, company and financial law.

2.5 The Data (Use and Access) Act 2025 has amended parts of UK data-protection law. Lighthouse will use current ICO guidance, including the requirements now in force for data-protection complaints, reasonable and proportionate searches for subject access requests and child-specific considerations where an online service is likely to be used by children.

3. Definitions and data-protection principles

Term	Meaning
Personal information / personal data	Information relating to an identified or identifiable living person.
Special-category information	Information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic or biometric identification data, health, sex life or sexual orientation.
Criminal-offence information	Information about alleged or proven offences, convictions, cautions, allegations, proceedings, security measures or related risks.
Processing	Anything done with information, including collecting, viewing, recording, sharing, altering, storing, deleting or destroying it.
Controller	The organisation that determines why and how personal information is used.
Processor	An organisation that processes personal information only on documented instructions from a controller.
Data subject	The living person the information is about.
Personal-data breach	A security incident leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal information.

3.2 Lighthouse follows the principles of lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; and accountability. We must be able to show how these principles are applied in practice.

4. Governance, accountability and named responsibilities

4.1 Board of Directors

The Board is accountable for data-protection governance and will ensure that:

- the organisation has sufficient resources, competence and authority to manage privacy and information security;
- significant new systems, suppliers, sharing arrangements and monitoring technologies receive appropriate review;
- records of processing, retention, suppliers, incidents, rights requests and complaints are maintained;
- staff and contractors receive induction, role-specific guidance and refresher training;
- serious breaches, repeated errors, overdue actions and high-risk processing are reviewed;
- ICO registration and fee obligations are assessed and evidence is retained; and
- this policy and associated notices are approved and reviewed.

4.2 Data Protection Lead - Rachel Waldron

The Data Protection Lead coordinates day-to-day compliance and will maintain or oversee privacy notices, the data inventory and record of processing, retention arrangements, processor contracts, data-sharing records, DPIAs, rights requests, complaints, breach logs, training records and assurance reporting. She is the first internal point of contact for data-protection questions and ICO correspondence.

4.3 Safeguarding information lead - Adam Waldron

As Director and DSL, Adam Waldron leads safeguarding information decisions and works with the Data Protection Lead where safeguarding, confidentiality, rights requests or disclosures overlap. Urgent safeguarding action does not wait for routine data-protection approval.

4.4 All adults

- use only approved systems, accounts, devices and storage;
- access only information needed for their role;
- verify recipients before sending or sharing information;
- protect passwords, devices, keys and paper records;
- report loss, misdirection, unauthorised access or suspected breach immediately;
- avoid discussing confidential matters where they may be overheard;
- keep information accurate and return or securely delete it when instructed; and
- seek advice before introducing a new tool, recording method, app, form or sharing arrangement.

5. Data Protection Officer assessment

5.1 Lighthouse has appointed a Data Protection Lead. This title does not automatically mean that the statutory Data Protection Officer requirements apply.

5.2 A formal DPO is required where an organisation is a public authority or body, or its core activities involve large-scale regular and systematic monitoring, or large-scale processing of special-category or criminal-offence information. Lighthouse will document its assessment at least annually and whenever its scale, technology or services change.

5.3 On the current planned operating model, Lighthouse is unlikely to meet the mandatory DPO thresholds. The Board will keep this under review. If it voluntarily appoints a person using the protected title Data Protection Officer, it will ensure that the role has the independence, resources, expertise and absence of conflict required by law.

Governance safeguard

The Data Protection Lead may seek external specialist or legal advice where a decision is complex, high risk, disputed or involves a possible ICO notification. Directors remain accountable for the organisation's decisions.

6. Information inventory, records of processing and ownership

6.1 Lighthouse will maintain a data map and record of processing activities proportionate to its size and risks. The record will identify the information, people affected, purpose, lawful basis, special-category or criminal-offence condition, source, recipients, systems, processor, transfer arrangements, retention period, security controls and responsible owner.

6.2 Each core record set will have an information owner responsible for accuracy, access, retention and review. Safeguarding records are controlled by the DSL; workforce and governance records by the Directors; finance records by the responsible Director or accountant; and operational learner records by the Provision Lead under agreed access controls.

6.3 Data flows will be reviewed before a placement starts and when a new commissioner, supplier, website feature, device, learning platform or activity is introduced.

7. Data protection by design, default and impact assessment

7.1 Privacy and security must be considered at the earliest stage of a project, not added after information has already been collected.

7.2 A Data Protection Impact Assessment screening will be completed for new or materially changed processing. A full DPIA is required where processing is likely to result in high risk, including certain uses of children's information, extensive sensitive records, systematic monitoring, innovative technology, profiling, biometric systems, large-scale data matching or processing that could significantly affect a person.

7.3 A DPIA will describe the purpose and information flows, assess necessity and proportionality, identify risks to people, record measures to reduce those risks, consult relevant people where appropriate and be approved before processing begins. Unmitigated high risk may require consultation with the ICO.

7.4 Default settings will minimise information, access, visibility and retention. Optional sharing or publication will be off by default unless a clear reason requires otherwise.

8. Lawful bases and purpose limitation

8.1 Lighthouse will identify and record a lawful basis before using personal information. The appropriate basis depends on the specific purpose and relationship.

Lawful basis	Typical Lighthouse use
Contract	Managing agreements with commissioners, suppliers, employees or contractors where the processing is objectively necessary for the contract.
Legal obligation	Tax, company, employment, health and safety, safeguarding referral, insurance or other duties imposed by law.
Vital interests	Urgent use needed to protect life or prevent serious harm where another basis is not reasonably available.
Legitimate interests	Necessary and proportionate business, educational, safety, security or relationship management interests after balancing the effect on the person, particularly a child.
Public task	Only where Lighthouse is carrying out a specific task in the public interest or exercising official authority under a clear legal basis or documented arrangement that supports this basis.
Consent	Genuinely optional processing where refusal or withdrawal does not cause unfair detriment, such as some promotional photography or optional communications.

8.2 Public task is not assumed merely because a placement is publicly funded. Contract is not used where processing is not objectively necessary to perform the contract. Consent is not used as a convenient substitute where the person has no real choice.

8.3 Information collected for one purpose will not be used incompatibly for another without assessing compatibility, identifying a lawful basis, updating privacy information and completing a DPIA where needed.

9. Special-category and criminal-offence information

9.1 Lighthouse routinely expects to handle health, disability, SEND and safeguarding information and may handle information about religion, ethnicity, sexual orientation, allegations, convictions or restrictions. This information requires greater care.

9.2 In addition to an Article 6 lawful basis, Lighthouse will identify an Article 9 condition for special-category information and an appropriate legal condition for criminal-offence information. Depending on purpose, conditions may include safeguarding of children and individuals at risk, health or social care, employment and social-security obligations, substantial public interest, legal claims or explicit consent.

9.3 Where required by Schedule 1 of the Data Protection Act 2018, Lighthouse will maintain an Appropriate Policy Document explaining compliance, retention and deletion arrangements. The document will be reviewed and made available to the ICO on request.

9.4 Access to these records will be role-based and limited. Sensitive labels must not be placed in email subject lines, diary titles or shared folders where they reveal more than necessary.

10. Children's information and best interests

10.1 Children have their own data-protection rights and merit specific protection because they may be less aware of risks, consequences and safeguards.

10.2 Lighthouse will consider the child's best interests, age, maturity, communication needs, disability, understanding, family circumstances and the potential impact of processing. Explanations will be concise, clear and available in accessible or child-friendly form.

10.3 The child's voice will be sought where appropriate, but a child cannot require Lighthouse to withhold information where sharing is necessary to protect them or another person.

10.4 If Lighthouse introduces an online service likely to be accessed by children, it will expressly consider children's needs in its design and use of personal information and assess whether the Age Appropriate Design Code applies.

11. Privacy information and transparency

11.1 Privacy information will be provided at or before collection where reasonably possible, or as soon as practicable where information is received indirectly. Notices will identify the controller, contact route, information collected, purposes, lawful bases, sensitive-data conditions, recipients, transfers, retention, rights and complaint route.

11.2 Lighthouse will use layered notices where this improves understanding, including a concise learner/family notice, fuller policy, workforce notice, website notice and task-specific wording on forms.

11.3 Where providing information would seriously prejudice safeguarding, crime prevention or another legal purpose, Lighthouse will consider the relevant exemption and record its decision. Exemptions are applied case by case, not as blanket rules.

12. Consent and optional processing

12.1 Consent must be freely given, specific, informed, unambiguous and evidenced. It must be as easy to withdraw as to give. Withdrawal affects future optional use but does not make earlier lawful processing unlawful.

12.2 Lighthouse will not seek one general consent to cover all referral, safeguarding, medical, contractual, staffing and business processing. Those activities usually rely on another lawful basis.

12.3 Separate choices will be used for genuinely optional activities, such as identifiable promotional images, testimonials or direct marketing. A child's views will be considered alongside parental responsibility and capacity. Refusal will not affect access to core education or safeguarding support.

13. Referral, placement, education and safeguarding records

13.1 Referral and placement information may include identity, family and professional contacts, education history, attendance, EHCP and SEND information, health, medication, behaviour, risk, safeguarding, social-care, transport, progress and accreditation records.

13.2 Lighthouse will collect only information necessary to assess whether it can safely meet need, plan and deliver the placement, safeguard the child, communicate with responsible organisations and evidence contractual delivery.

13.3 Safeguarding records will be factual, attributable, secure and separated from ordinary learning records where appropriate. Access is restricted to the DSL, Deputy DSL and others with a genuine need to know.

13.4 At the end of placement, safeguarding and education records will be securely transferred to the responsible school, Local Authority or next setting as agreed. Receipt will be recorded. Lighthouse will retain only the information necessary to evidence its actions, comply with law and manage foreseeable claims or enquiries.

14. Working with schools, Local Authorities and other commissioners

14.1 Before a placement begins, the parties will agree in writing what information will be shared, for what purpose, the lawful basis, each party's role, security method, retention, correction route, breach reporting and end-of-placement transfer.

14.2 Where both organisations decide their own purposes and means, they are normally independent controllers and require a data-sharing agreement rather than a processor contract. Where Lighthouse acts only on documented

instructions, an Article 28-compliant processor contract is required. Joint-controller arrangements require a transparent allocation of responsibilities.

14.3 Contractual wording cannot prevent or delay a lawful safeguarding disclosure. Information will be shared through verified professional routes and significant disclosures will be recorded.

15. Workforce, recruitment, DBS and contractor information

15.1 Workforce information includes identity, contact, application, employment history, references, qualifications, DBS and barred-list status, right-to-work evidence, training, supervision, performance, attendance, health adjustments, payment, insurance, allegations and conduct records where relevant.

15.2 Recruitment and vetting information will be used only for lawful suitability, safeguarding, contract, employment and compliance purposes. Criminal-offence information will be restricted to authorised decision-makers.

15.3 Lighthouse will normally retain only the DBS certificate number, level, issue date, identity-check date, decision and checker on the Single Central Record. A certificate copy will not normally be retained for longer than six months after the decision unless a specific documented lawful reason applies.

15.4 Applicants and workers will receive separate privacy information. Health questions before offer are limited to lawful purposes such as reasonable adjustments or intrinsic role requirements.

16. Information sharing and disclosure decisions

16.1 Lighthouse may share information with commissioning schools and Local Authorities, families and authorised representatives, police, children's social care, health services, safeguarding partnerships, LADO, awarding bodies, insurers, professional advisers, IT providers, regulators, courts and other bodies where lawful and necessary.

16.2 Before a non-routine disclosure, the decision-maker should consider:

- what purpose is being achieved and whether sharing is necessary;
- the lawful basis and any sensitive-data condition;
- whether the information is relevant, accurate and limited;
- the child's best interests and any risk of informing or not informing the family;
- whether the recipient and contact route have been verified;
- the safest transfer method and any restrictions on onward use; and
- what decision, rationale, information and recipient must be recorded.

16.3 Data-protection law is not a barrier to safeguarding. Information may be shared without consent where necessary and proportionate to protect a child or another person. Urgent action must not be delayed while seeking routine approval.

16.4 Adults must not obtain evidence unlawfully, access records out of curiosity or disclose information to friends, family or unauthorised colleagues.

17. Accuracy, minimisation and access control

17.1 Records should distinguish fact, observation, opinion and information received from another source. Material inaccuracies will be corrected or clearly annotated without improperly rewriting historic safeguarding or decision records.

17.2 Forms and systems will avoid unnecessary free-text collection. Mandatory fields must be justified. Duplicate records will be reduced and outdated copies removed or archived securely.

17.3 Access will follow least-privilege principles. User accounts must be individual, permissions reviewed, access removed promptly when roles change and shared passwords prohibited.

18. Email, devices, remote working and physical records

18.1 Sensitive emails must be sent from approved professional accounts. Recipients and attachments must be checked before sending. Full child names and sensitive details should be avoided in subject lines where a secure reference can be used.

18.2 Bulk external emails must use BCC or an approved mailing system unless recipients need to see one another. Auto-complete should be used cautiously and delayed-send or confirmation controls used where available.

18.3 Devices must use strong authentication, automatic locking, supported software, malware protection and encryption where appropriate. Information must not be stored in unapproved personal cloud accounts, consumer messaging apps or removable media.

18.4 Where an authorised personal device is exceptionally used for a photograph or recording under another policy, automatic cloud backup must be disabled, the material transferred promptly to approved storage and permanently deleted from the device and recently deleted folder. Personal use, messaging or social-media upload is prohibited.

18.5 Paper records must be locked when unattended. Information taken off site requires authorisation, minimum necessary content, secure transport and a record where appropriate. Confidential discussions must not take place where they may be overheard.

19. Photography, video, audio and learner work

19.1 Images and recordings are personal information where a person is identifiable. Lighthouse will identify the purpose, lawful basis, storage, access, retention and publication arrangements before creating them.

19.2 Images used for internal learning evidence, safeguarding, accident recording or contractual reporting may rely on a basis other than consent where necessary and lawful. Promotional publication will normally use separate informed consent and will respect the child's views.

19.3 Names, locations, routines or other identifying details will not be combined with public images unless specifically justified and authorised. Consent records and withdrawal action will be maintained.

19.4 Sexual images of children must never be copied, forwarded, printed or saved during safeguarding handling unless police or an authorised specialist process expressly directs otherwise.

20. Website, cookies, social media and direct communications

20.1 The website privacy notice will explain enquiry forms, hosting, security logs, essential cookies, analytics and embedded services. Non-essential cookies or similar technologies will be used only with the consent required by PECR and data-protection law.

20.2 Website forms will collect the minimum information required and use secure transmission and storage. Sensitive referral information should use an approved secure referral route rather than a general website contact form.

20.3 Lighthouse will not use children's information for direct marketing or sell personal information. Business communications to schools and professionals will be lawful, targeted, relevant and provide an appropriate opt-out where required.

20.4 Social-media posting will follow the communications and photography procedures. Personal accounts must not be used to communicate privately with learners or publish identifiable learner information.

21. Suppliers, processors, contracts and international transfers

21.1 Before using a supplier that handles personal information, Lighthouse will assess security, privacy, reliability, data location, sub-processors, breach history, deletion arrangements and ability to support rights requests.

21.2 Processor contracts must include the requirements of Article 28, including documented instructions, confidentiality, security, sub-processing, assistance, deletion or return, audit and breach notification. Suppliers may not repurpose Lighthouse information for their own unrelated product development, advertising or profiling without a separate lawful controller arrangement.

21.3 International transfers will be identified and documented. Where information is transferred outside the UK, Lighthouse will use an adequacy regulation or approved safeguard, assess transfer risk where required and explain the transfer in privacy information.

21.4 Free or consumer tools will not be used for sensitive learner information merely because they are convenient. Procurement approval is required before introducing AI, transcription, translation, analytics or generative systems that process personal information.

22. Retention, archiving and secure disposal

22.1 Lighthouse will maintain a retention schedule linked to purpose, legal duties, safeguarding need, contractual requirements and foreseeable claims. Information will not be kept indefinitely "just in case".

22.2 Disposal may be paused where records are needed for an active safeguarding matter, complaint, investigation, litigation hold, insurance claim, statutory enquiry or unresolved rights request.

22.3 Paper will be cross-cut shredded or securely destroyed. Digital information will be securely deleted from live systems and, where technically possible and proportionate, backups in line with the system's deletion cycle. Devices and media will be securely wiped or physically destroyed before disposal or reuse.

22.4 Anonymisation must be effective and irreversible before information is treated as non-personal. Pseudonymised information remains personal information where re-identification is possible.

23. Individual rights and subject access requests

23.1 Depending on the circumstances, individuals may have rights to be informed, access their information, correct inaccuracies, request erasure or restriction, object, receive portable information and receive safeguards in relation to automated decision-making.

23.2 A request does not need to mention data protection or use a form. Any adult receiving a possible request must forward it immediately to the Data Protection Lead.

23.3 Lighthouse will:

- record the request and confirm identity or authority proportionately;
- clarify the request where genuinely needed and explain any effect on the time limit;
- make reasonable and proportionate searches across relevant systems and people;
- respond without undue delay and normally within one month;
- extend by up to two further months only where the request is complex or numerous and notify the person within the first month;
- review third-party, safeguarding, legal, social-work, health and other exempt information carefully;
- provide information securely, clearly and in an accessible commonly used format; and
- explain any refusal, restriction, fee or exemption and the complaint route.

23.4 The response period begins when Lighthouse has the request and any reasonably required identity evidence or permitted fee. Where lawful clarification is requested, the clock may pause until clarification is received. Searches must be defensible as reasonable and proportionate.

23.5 Requests are normally free. A reasonable administrative fee may be charged only where permitted, including manifestly unfounded or excessive requests or further copies. Refusal is exceptional and must be approved and documented.

24. Children, parents, carers and access requests

24.1 Personal information about a child belongs to the child for data-protection purposes. Whether a parent or carer may exercise a right on the child's behalf depends on the child's understanding, best interests, authority and the circumstances, not a fixed age rule.

24.2 Lighthouse will consider the child's maturity and communication needs, the nature of the information, parental responsibility, any conflict of interest, safeguarding risk and the child's wishes. A competent child may exercise rights directly.

24.3 The separate statutory right of parents to access a child's educational record applies to certain schools under education legislation. Lighthouse is a non-school provider and will not assume that this separate school-specific right applies directly. It will cooperate with the responsible school or Local Authority and respond under UK GDPR rights and contractual arrangements as appropriate.

24.4 Safeguarding, third-party and social-work information may require redaction or exemption where disclosure could cause harm, identify another person or prejudice protective work. Decisions will be recorded and specialist advice obtained where necessary.

25. Data-protection complaints and external escalation

25.1 Any person may complain about how Lighthouse has collected, used, shared, secured, retained or responded to a request concerning personal information. Complaints can be made verbally, by email, through an electronic form where provided or in writing. Reasonable adjustments and child-friendly support are available.

25.2 Under the Data (Use and Access) Act 2025 requirements in force from 19 June 2026, Lighthouse will provide a clear complaint route, acknowledge receipt within 30 days, take appropriate steps to investigate without undue delay, keep the complainant informed and communicate the outcome without undue delay.

25.3 Lighthouse operational targets are to acknowledge within five working days and provide an outcome within twenty working days where reasonably possible. Complex cases may take longer, but progress and a revised date will be provided.

25.4 The review will be undertaken by a person with sufficient independence and competence. The outcome will explain the issue considered, enquiries made, findings, action, rights and how to complain to the Information Commissioner's Office.

25.5 A person may complain to the ICO. Lighthouse encourages internal resolution where safe and appropriate but will not obstruct or penalise external complaint or lawful disclosure.

ICO Registration reference: ZC192625

Lighthouse Learning Provision Ltd is registered with the Information Commissioner's Office as a data controller.

26. Personal-data breaches and cyber incidents?

Immediate rule

Report every suspected loss, misdirection, unauthorised disclosure, access, deletion, cyberattack, stolen device or insecure record to the Data Protection Lead immediately. Do not wait to establish whether harm occurred.

26.1 Lighthouse will contain the incident, preserve evidence, recover or recall information where safe, change access credentials where necessary, assess risk to people and record the decision.

26.2 A notifiable personal-data breach must be reported to the ICO without undue delay and, where feasible, within 72 hours of Lighthouse becoming aware of it. If risk to individuals is high, affected people must also be informed without undue delay unless an exception applies.

26.3 The risk assessment will consider the nature, sensitivity and volume of information; whether it was encrypted; ease of identification; people affected; likely consequences; safeguarding implications; recipient action; containment and the vulnerability of children or adults involved.

26.4 The breach log will record all incidents, including those not notified, the facts, effects, decision, rationale, notifications, actions and lessons. Suppliers must notify Lighthouse promptly enough to meet the controller's legal deadlines.

26.5 Staff must not conceal, privately resolve or delete evidence of an incident. Good-faith reporting is supported; deliberate concealment or reckless disregard may be addressed under conduct procedures.

27. CCTV, access systems and new monitoring technology

27.1 CCTV, door-access logs, biometric systems, location tracking, monitoring software or similar technology will not be introduced without a documented purpose, necessity and proportionality assessment, DPIA screening, signage or privacy information, access rules, retention period and security controls.

27.2 Audio recording will not be used routinely because of its greater intrusiveness. Covert monitoring is exceptional and requires specific lawful authority and specialist advice.

27.3 Monitoring will never be used in toilets, changing areas or other spaces where there is a high expectation of privacy, except where an emergency legal authority requires otherwise.

28. Training, audit, assurance and policy review

28.1 All adults will receive data-protection and information-security induction before handling sensitive information. Refresher updates will cover safeguarding sharing, email errors, phishing, passwords, devices, rights requests, complaints and breach reporting.

28.2 The Data Protection Lead will monitor the processing inventory, overdue retention actions, processor reviews, access permissions, DPIAs, requests, complaints, breaches, training and implementation actions. Themes and significant risks will be reported to the Board without unnecessary personal detail.

28.3 This policy will be reviewed at least annually and after a serious breach, ICO or commissioner action, new technology, major system or site change, change in scale, new online service, new high-risk processing or relevant legal change.

29. Related policies and reference framework

Core external framework

- UK General Data Protection Regulation
- Data Protection Act 2018
- Data (Use and Access) Act 2025 and commencement regulations
- Privacy and Electronic Communications Regulations 2003, as amended
- ICO guidance on children and the UK GDPR
- ICO guidance on data sharing to safeguard children
- ICO guidance on subject access requests and reasonable and proportionate searches
- ICO guidance on data-protection complaints
- ICO guidance on personal-data breaches and the 72-hour reporting period
- ICO guidance on Data Protection Officers and DPIAs
- Information sharing advice for safeguarding practitioners

External sources checked July 2026. Current legislation, ICO guidance and safeguarding requirements take precedence where a source changes.

Appendix A - Record of processing activities and data inventory

Complete one row for each material processing activity or record set. Use a linked information-asset record where more detail is required.

Field	Record
Processing activity / record set	
Information owner	
People affected	
Categories of information	
Special-category / criminal-offence information	
Purpose	
Article 6 lawful basis	
Article 9 / DPA condition and APD reference	
Source of information	
Recipients / sharing partners	
Controller / processor status	
System / physical location	
International transfer / safeguard	
Retention and disposal	
Security and access controls	
DPIA reference / review date	
Privacy notice location	
Last reviewed / reviewer	

Appendix B - Lawful basis and sensitive-data decision record

Activity / purpose	
Information and people affected	
Why the processing is necessary	
Article 6 lawful basis and rationale	
Alternative less intrusive options considered	
Special-category data present?	☐ No ☐ Yes - categories:
Article 9 condition and rationale	
DPA 2018 Schedule 1 condition, if required	
Appropriate Policy Document required / reference	
Criminal-offence information and condition	
Children's best-interests assessment	
Legitimate Interests Assessment reference, if used	
Privacy information provided	
DPIA screening / DPIA reference	
Approved by / date / review date	

Appendix C - Data Protection Impact Assessment screening

Complete before introducing or materially changing a system, supplier, data flow, monitoring method or activity.

Screening question	Yes / No / detail
Does the activity use children's personal information in a new or significant way?	
Does it involve sensitive or criminal-offence information?	
Does it involve systematic monitoring, tracking, profiling or scoring?	
Will decisions significantly affect a person?	
Does it use innovative technology, AI, biometric or location data?	
Does it combine information from different sources or match datasets?	
Is information shared widely, published or transferred internationally?	
Could a breach lead to physical, emotional, financial, discriminatory or safeguarding harm?	
Would people reasonably find the processing unexpected or intrusive?	
Could the activity prevent someone exercising a right or accessing a service?	

Screening outcome	☐ Full DPIA required ☐ Not required
Reason and risk summary	
Consultation required	
Approved by and date	
Review trigger / date	

Full DPIA prompts

- Describe the processing, purpose, context, systems, people and information flows.
- Explain necessity, proportionality and the lawful basis.
- Record consultation with children, families, staff, commissioner or specialist where appropriate.
- Identify risks to rights, freedoms, safety, dignity, equality, autonomy and safeguarding.
- Score likelihood and severity before and after controls.
- Record controls, owner, deadline, residual risk and approval.
- Consult the ICO before processing if high risk cannot be reduced sufficiently.

Appendix D - Information-sharing decision record

Person / child concerned	
Date and time	
Requesting / receiving organisation and verified contact	
Purpose of sharing	
Information requested / shared	
Lawful basis and sensitive-data condition	
Consent sought? Outcome / reason not sought	
Necessity and proportionality	
Child's best interests / wishes and feelings	
Risks of sharing / not sharing	
Security method and restrictions	
Decision and rationale	
Commissioner / DSL / Data Protection Lead consulted	
Follow-up and outcome	
Decision-maker / signature / date	

Appendix E - Personal-data breach and 72-hour assessment log

Incident reference	
Date/time occurred, if known	
Date/time Lighthouse became aware	
Reported by / contact	
Systems, records and locations affected	
People and approximate number affected	
Information categories and sensitivity	
What happened	
Immediate containment and evidence preservation	
Safeguarding or physical-safety action	
Encryption / access protection	
Likely consequences for people	
Risk level and rationale	
ICO notification required? Decision and deadline	
Individuals informed? Decision and wording	
Commissioner / insurer / police / supplier notification	
Root cause and corrective actions	
Decision-maker / date	
Final review and closure	

72-hour timing

The clock normally starts when Lighthouse has a reasonable degree of certainty that a security incident has compromised personal information. Start the log immediately and do not wait for every fact before escalating or making a phased notification.

Appendix F - Individual rights and subject access request log

Field	Details
Request reference	
Requester and person represented	
Date received / channel	
Right requested	
Identity / authority evidence and date received	
Clarification requested / received	
Statutory due date	
Systems, custodians and search terms	
Searches completed and proportionality rationale	
Third-party / safeguarding / exemption review	
Information supplied and secure method	
Extension, fee, refusal or restriction and reason	
Date completed	
Complaint / review follow-up	

Appendix G - Data-protection complaint form and investigation record

Complainant / representative / contact	
Person whose information is concerned	
Date and method received	
Complaint issue and outcome sought	
Identity / authority evidence	
Acknowledgement date - within 30 days	
Investigator and conflict check	
Information, systems and people reviewed	
Enquiries made and evidence	
Interim updates provided	
Findings	
Outcome and remedy	
Systemic improvement actions	
Outcome communicated date	
ICO complaint route explained	
Review / closure date	

Appendix H - Operational retention schedule

These are operational baselines. A legal hold, safeguarding need, commissioner requirement or active dispute may require longer retention. Shorter retention should be used where the purpose no longer exists.

Record category	Baseline retention / action
General website enquiry not leading to referral	Review and normally delete within 12 months after final response.
Unsuccessful referral or placement enquiry	Normally six years from final decision where needed to evidence assessment or contractual discussions; minimise earlier where risk is low.
Core learner placement, attendance, progress and contract records	Normally six years from the end of placement or contract, subject to commissioner agreement, safeguarding requirements and legal claims.
Safeguarding records	Transfer securely to the responsible school, Local Authority or next setting. Retain only necessary decision, transfer and case-management evidence for the agreed and legally justified period; review at least annually.
Medical and medication records	Follow the healthcare, accident and commissioner retention requirements; retain only while necessary for safety, accountability and claims.
Accident and incident records	At least the applicable statutory period and longer where a child's age or foreseeable claim requires it; coordinate with Health and Safety policy.
Complaints and investigation records	Normally six years after closure, longer where safeguarding, legal or regulatory action remains possible.
Recruitment - unsuccessful applicants	Normally six months after the final decision, longer only with documented consent or a specific legal reason.
Workforce personnel and contract records	Normally six years after the relationship ends, with selected safeguarding or pension records retained longer where required.
DBS certificate copies	Normally no longer than six months after the recruitment or suitability decision; retain check metadata and decision on the SCR.
Financial, tax and company records	Usually six years after the relevant financial year or transaction, subject to accountant and statutory advice.
Visitor and access logs	Normally three years, shorter where no safety or safeguarding purpose remains.
CCTV, if introduced	A short documented period, normally around 31 days, unless footage is required for an incident, safeguarding matter, complaint or legal process.
Consent records	For as long as the related processing continues and long enough afterwards to evidence the consent and any withdrawal.
Breach, rights-request, complaint and DPIA logs	Normally six years after closure or supersession, subject to risk and legal advice.

Appendix I - Privacy notice for learners, parents, carers and commissioners

Who we are

Lighthouse Learning Provision Ltd, Company No. 17244395, is the organisation responsible for personal information it uses for its own purposes. Our Data Protection Lead is Rachel Waldron. Contact: info@lighthouselearningprovision.co.uk | 07436 177831 | www.lighthouselearningprovision.co.uk.

ICO Registration reference: ZC192625. Lighthouse Learning Provision Ltd is registered with the Information Commissioner's Office as a data controller.

What we collect

We may collect identity and contact details; education, EHCP, SEND and attendance information; health, medication and allergy details; safeguarding, behaviour, risk and social-care information; family and professional contacts; transport and activity information; learning work, progress, accreditation, photographs or recordings where appropriate; and communication, complaint or incident records.

Why we use it

We use information to consider and manage referrals, assess whether we can safely meet need, deliver personalised learning, safeguard children, manage health and safety, communicate with families and professionals, evidence attendance and progress, fulfil commissioner contracts, meet legal duties and improve quality.

Our legal reasons

Depending on the purpose, we rely on contract, legal obligation, vital interests, legitimate interests, public task where the legal conditions are met, or consent for genuinely optional activities. Sensitive information also requires an additional legal condition, which may include safeguarding, health or social care, employment obligations, substantial public interest or explicit consent.

Who we share with

We may share relevant information with commissioning schools and Local Authorities, parents and authorised representatives, safeguarding partners, police, health and social care, Virtual Schools, awarding organisations, insurers, professional advisers, secure IT and record providers, regulators and courts. We do not sell personal information or use children's information for direct marketing.

How long we keep it

Retention depends on the record, safeguarding need, commissioner agreement, legal duty and foreseeable claim. Safeguarding and education records are transferred securely when required. Information is deleted, destroyed or anonymised when no longer needed.

Your rights and complaints

You may have rights to access information, correct it, request erasure or restriction in some circumstances, object and receive safeguards around automated decisions. Children have their own rights. Contact the Data Protection Lead. You may also raise a data-protection complaint with Lighthouse and complain to the Information Commissioner's Office.

Safeguarding

We may share information without consent where necessary to protect a child or another person. Data-protection law does not prevent appropriate safeguarding information sharing.

Appendix J - Workforce, applicant and contractor privacy notice

Lighthouse uses workforce information to recruit suitable people, verify identity and qualifications, complete lawful safeguarding and DBS checks, manage employment or contracts, pay people, provide training and supervision, ensure health and safety, respond to concerns, meet legal and insurance obligations and maintain service quality.

Information may include contact and identity details, application and employment history, references, interview records, qualifications, right-to-work evidence, DBS and barred-list status, training, performance, attendance, health adjustments, payment, insurance, complaints, allegations and conduct information where relevant.

Depending on purpose, Lighthouse relies on contract, steps before contract, legal obligation, legitimate interests, vital interests and consent for limited optional uses. Sensitive and criminal-offence information requires an additional legal condition.

Information may be shared with authorised directors and managers, payroll and accounting services, DBS and recruitment providers, commissioners requiring safeguarding assurance, insurers, professional advisers, occupational health, regulators, police, LADO or safeguarding agencies where lawful and necessary.

Unsuccessful recruitment records are normally retained for around six months. Personnel and contractual records are normally retained for six years after the relationship ends, with selected records retained longer where law, safeguarding or claims require it. DBS certificate copies are not normally retained beyond six months after the decision.

Applicants and workers may exercise applicable data-protection rights and raise a complaint through the Data Protection Lead or the ICO. Information about another person, safeguarding enquiries and confidential references may be subject to legal restrictions or exemptions.

Appendix K - Staff quick guide: protect, check, share and report

Do	Do not
Use approved accounts, systems and secure storage.	Do not store learner information in personal email, cloud drives or messaging apps.
Check recipients, attachments and permissions before sending.	Do not rely on email auto-complete without verifying the address.
Use BCC for external group emails unless recipients must see each other.	Do not expose parent, school or professional email addresses unnecessarily.
Lock screens, protect passwords and keep paper records secure.	Do not share accounts, passwords, keys or leave information unattended.
Record facts accurately and distinguish opinion and source.	Do not alter historic records to hide an error; correct or annotate transparently.
Share necessary information to safeguard a child and record the decision.	Do not use data protection as a reason to delay urgent safeguarding action.
Forward any rights request or data complaint immediately to Rachel Waldron.	Do not ignore an informal verbal request because it does not use legal wording.
Report every suspected breach immediately.	Do not conceal, privately fix or delete evidence of an information incident.
Seek approval before using a new app, AI tool, platform or supplier.	Do not upload personal information to free or unapproved services.

Internal contacts

Data Protection Lead: Rachel Waldron | Safeguarding / DSL: Adam Waldron | Main contact: info@lighthouselearningprovision.co.uk | 07436 177831. Immediate danger: 999. Report suspected data loss or disclosure immediately, even if you think it has been corrected.