



Lighthouse
Outreach Service

AI, Online Safety, Data Protection & Cybersecurity Policy

Lighthouse Outreach Service places the highest importance on the mental health and well-being of every individual in our community.

Our policies are grounded in the core values of respect, inclusion, and mutual support across all aspects of life. We aim to create a safe and empowering environment where collaboration helps each person to thrive, celebrate their strengths, and honour the unique differences of others.

Resilience, Perseverance, Independence

September 2026

AI, ONLINE SAFETY, DATA PROTECTION & CYBERSECURITY POLICY

Lighthouse Outreach Service

Policy Review

This policy will be reviewed in full by the Data controller annually.

The policy was last reviewed and agreed by Trevor Adams, Lighthouse Outreach Service on 02/09/2026.

It is due for review 02/09/2027, or sooner if legislation, guidance, technology or business arrangements change

Director Signature: *T. Adams* Date: 02/09/26

Statement of Intent

Lighthouse Outreach Service is committed to safeguarding and promoting the welfare of all children. We recognise that safeguarding is everyone's responsibility and that all staff have a duty to act in the best interests of the child at all times.

This policy reflects statutory guidance issued by the Department for Education, including Keeping Children Safe in Education (KCSIE) and Working Together to Safeguard Children.

We adopt a **child-centred approach** and maintain a culture of vigilance where concerns are identified early and acted upon promptly.

Resilience, Perseverance, Independence

September 2026

1. Purpose

This policy sets out how Lighthouse Outreach Service ("Lighthouse Outreach Service", "the Business", "I", "me" or "my") will use technology, artificial intelligence (AI), online services and digital information safely and responsibly.

The purpose of this policy is to:

- protect children, young people, adults, parents/carers and professionals who engage with Lighthouse Outreach Service;
- protect personal, confidential and safeguarding information;
- reduce the risk of cyber attacks, data breaches, loss or theft of information;
- establish clear rules for the safe use of artificial intelligence;
- ensure that AI is not used inappropriately to make decisions about children or adults;
- support compliance with applicable data protection and safeguarding requirements;
- provide schools and other commissioning organisations with confidence that Lighthouse Outreach Service takes information security seriously;
- establish a clear process for responding to suspected cyber incidents, data breaches or inappropriate use of technology.

This policy is intended to operate alongside the policies and procedures of schools, local authorities and other organisations with which Lighthouse Outreach Service works.

2. Scope

This policy applies to all work carried out by Lighthouse Outreach Service and covers:

- mentoring;
- training;
- educational programmes;
- interventions;
- work with children and young people;
- work with adults aged 18 and over;
- work with parents and carers;
- information received from schools or local authorities;
- pupil and participant information;
- safeguarding information;
- SEND information;
- photographs of pupils' work;
- business and financial information;

Resilience, Perseverance, Independence

September 2026

- use of laptops, tablets and mobile phones;
- local and external storage;
- email and messaging;
- internet and Wi-Fi;
- cloud and online services;
- generative AI and other AI technologies;
- social media and online communication;
- cybersecurity and incident management.
- remote working;
- accessing school guest networks or guest accounts.

As a director, I am personally responsible for implementing this policy and maintaining appropriate safeguards.

3. Legal and Regulatory Framework

Lighthouse Outreach Service will take account of applicable UK requirements and guidance, including, where relevant:

- UK GDPR;
- Data Protection Act 2018;
- Children's safeguarding requirements;
- Keeping Children Safe in Education (KCSIE), where relevant to work undertaken in education settings;
- Department for Education guidance on data protection in schools;
- Department for Education guidance concerning generative AI and data protection;
- Information Commissioner's Office (ICO) guidance;
- National Cyber Security Centre (NCSC) guidance;
- contractual requirements imposed by schools, colleges, local authorities and other commissioning organisations.

This policy does not replace the safeguarding, acceptable-use, data-protection or IT-security policies of an individual school.

Where Lighthouse Outreach Service works within a school, the school's policies and instructions will be followed.

Where there is uncertainty about how information should be handled, Lighthouse Outreach Service will seek clarification from the relevant school, commissioning organisation or other responsible organisation before proceeding.

4. Relationship with Schools and Other Organisations

When working within or on behalf of a school, academy, college, local authority or other organisation, Lighthouse Outreach Service will comply with the relevant policies and instructions of that organisation.

These may include:

- safeguarding and child protection procedures;
- acceptable use policies;
- data protection policies;
- information security policies;
- online safety policies;
- photography and image policies;
- IT and device policies;
- filtering and monitoring arrangements;
- confidentiality requirements;
- incident-reporting procedures.

Depending on the circumstances, Lighthouse Outreach Service may act as:

- a data processor;
- a data controller;
- a joint controller in limited circumstances; or
- another party with responsibilities defined by contract or other lawful arrangements.

Where a school's requirements are stricter than this policy, the school's requirements will normally be followed while working within that setting.

If I am uncertain whether an action is permitted, I will seek clarification from the relevant school contact, Designated Safeguarding Lead (DSL), Data Protection Officer (DPO), IT lead or other appropriate person before proceeding.

5. Safeguarding

Safeguarding remains the highest priority when working with children and young people.

Lighthouse Outreach Service recognises that online activity, technology, AI-generated content and digital communications can create safeguarding risks.

These may include:

- cyberbullying;
- online harassment;
- grooming;
- exploitation;
- inappropriate communication;
- harmful or illegal online content;
- misinformation and disinformation;
- AI-generated harmful content;
- deepfakes;
- manipulated images;
- self-generated intimate images;
- impersonation;
- online scams;
- inappropriate use of AI by children or adults.

I will follow the safeguarding procedures of the school or organisation in which I am working.

I will know who the Designated Safeguarding Lead (DSL) is before beginning work with pupils where this information is available.

Any safeguarding concern will be reported promptly through the appropriate school or organisation safeguarding procedure.

I will not attempt to investigate safeguarding concerns beyond my role unless specifically instructed to do so by the appropriate safeguarding professional.

Where a child or young person makes a disclosure, I will follow the school's safeguarding procedures and record or communicate information appropriately.

Data protection will not be treated as a reason to prevent necessary safeguarding information from being shared with an appropriate person where safeguarding procedures require or permit it.

KCSIE 2026 makes clear that safeguarding concerns should be acted on immediately and reported to the DSL or deputy, and that this applies to contractors as well as other people working in education settings.

6. Professional Boundaries

Lighthouse Outreach Service will maintain appropriate professional boundaries when communicating with children and young people.

I will:

- use communication methods approved by the school or commissioning organisation;
- avoid unnecessary private communication with pupils;
- avoid using personal social media accounts to communicate with pupils;
- not accept inappropriate social-media connections from pupils;
- not exchange personal photographs with pupils;
- not request unnecessary personal information;
- not use AI to create inappropriate or personal communications with pupils;
- report concerns about online contact or communications through appropriate safeguarding procedures.

Where digital communication with a child or young person is required, it should normally take place through an approved school or organisational system.

7. Artificial Intelligence Policy

7.1 General principle

AI tools can support productivity, educational resource development and administrative work. However, AI can also create risks relating to:

- personal data;
- confidentiality;
- safeguarding;
- accuracy;
- bias;
- inappropriate content;
- copyright;
- misinformation;
- automated decision-making;
- children's privacy;
- security.

Lighthouse Outreach Service will therefore use AI cautiously and proportionately.

Lighthouse Outreach Service may use AI where it provides a genuine business, educational or administrative benefit and where its use can be carried out safely, lawfully and ethically.

AI will be treated as a tool to assist professional work, not as a replacement for professional judgement.

AI-generated information will not automatically be assumed to be accurate, appropriate, unbiased or suitable for children.

I remain responsible for anything I produce, send, publish or use, even where AI has assisted in creating it.

7.2 Permitted uses of AI

Examples of potentially acceptable uses include:

- generating generic activity ideas;
- brainstorming educational programme ideas;
- producing generic lesson or intervention structures;
- creating generic worksheets;
- improving the wording of non-confidential business documents;
- proofreading;
- generating generic training materials;
- creating generic quizzes;
- developing fictional scenarios;
- brainstorming marketing ideas;
- generating non-personal administrative content;
- helping structure reports where no identifiable personal information is entered;
- generating generic professional-development material.

8. Artificial Intelligence Policy

8.1 Purpose

AI tools can support productivity, educational resource development and administrative work. However, AI can also create risks relating to:

- personal data;
- confidentiality;
- safeguarding;
- accuracy;

- bias;
- inappropriate content;
- copyright;
- misinformation;
- automated decision-making;
- children's privacy;
- security.

Lighthouse Outreach Service will therefore use AI cautiously and proportionately.

8.2 Approved General Principle

AI may be used for low-risk purposes such as:

- generating generic ideas;
- brainstorming educational activities;
- creating draft lesson or intervention ideas;
- improving generic wording;
- creating fictional examples;
- generating non-personal educational resources;
- proofreading non-confidential documents;
- producing generic administrative templates;
- summarising public information where appropriate.

AI must not be used as a substitute for professional judgement.

Any AI-generated material used by Lighthouse Outreach Service will be reviewed by the director before being used with service users or provided to a school.

9. Information That Must Not Be Entered Into Public AI Tools

Lighthouse Outreach Service will not enter identifiable information relating to children, young people, parents/carers, adult service users or school staff into publicly available generative AI systems unless there is a specific, documented and authorised reason to do so and the relevant data-protection requirements have been satisfied.

This includes:

- pupil names;
- dates of birth;
- addresses;
- school identification numbers;

- photographs of pupils;
- pupil records;
- school reports;
- SEND information;
- medical information;
- safeguarding information;
- family information;
- behavioural records;
- intervention records;
- counselling or mentoring records;
- individual assessment information;
- contact details;
- passwords;
- usernames;
- access codes;
- school security information;
- confidential school documents;
- information that could identify a child or vulnerable adult.

This rule applies even where an AI service appears to be free or convenient.

10. AI Traffic-Light Guide

GREEN – Generally acceptable

Examples include:

- generic educational activity ideas;
- generic mentoring ideas;
- fictional scenarios;
- generic presentation ideas;
- public information;
- generic proofreading;
- brainstorming;
- generic training materials;
- creating a blank template;
- improving wording where no confidential information is included.

AMBER – Use caution

Examples include:

Resilience, Perseverance, Independence

September 2026

- anonymised case examples;
- information that has been heavily generalised;
- material derived from school circumstances;
- information that could potentially identify an individual when combined with other information;
- AI tools supplied by a school or education provider.

Before using such information, Lighthouse Outreach Service will consider whether the individual could realistically be identified and whether the school has authorised the processing.

RED – Do not enter into public AI systems

- pupil names;
- pupil records;
- SEND information;
- safeguarding information;
- medical information;
- personal addresses;
- contact details;
- school confidential information;
- passwords;
- security information;
- identifiable photographs;
- identifiable mentoring notes;
- identifiable intervention records;
- confidential communications.

11. AI and Children

Lighthouse Outreach Service will not require or encourage children or young people to provide personal information to AI systems for Lighthouse Outreach Service's benefit.

Where AI is used during an educational activity, the business will:

- follow the school's rules;
- check whether the school permits the relevant AI tool;
- consider the age restrictions and terms of the tool;
- avoid requiring pupils to create accounts unless authorised;
- avoid entering pupil personal data;
- provide appropriate adult oversight;
- consider whether the content produced is suitable for the age group;

Resilience, Perseverance, Independence

September 2026

- challenge inaccurate, harmful or inappropriate AI-generated content.

Lighthouse Outreach Service will not make decisions about a child's safeguarding, SEND provision, suitability, behaviour, progression or welfare solely on the basis of an AI-generated recommendation.

12. AI Accuracy and Human Oversight

AI-generated information may be inaccurate, incomplete, biased or misleading. Lighthouse Outreach Service will therefore:

- check AI-generated factual information before relying on it;
- use professional judgement;
- check educational materials for age appropriateness;
- check generated content for discriminatory or stereotypical material;
- ensure safeguarding decisions are made by people, not AI;
- avoid presenting AI-generated information as professional or authoritative advice unless it has been independently verified.

AI will not replace safeguarding judgement or professional responsibility.

13. AI, Copyright and Intellectual Property

AI-generated content will be reviewed before use.

Lighthouse Outreach Service will consider:

- copyright;
- licensing;
- ownership;
- school-specific intellectual property arrangements;
- confidentiality;
- whether generated material reproduces material belonging to another person or organisation.

Where a school provides resources to Lighthouse Outreach Service, those resources will not be uploaded into public AI systems unless the school has authorised this.

14. AI and Automated Decision-Making

Lighthouse Outreach Service will not use AI to make solely automated decisions that have legal or similarly significant effects on children, young people, parents, adult service users or staff.

In particular, AI will not independently determine:

- whether a child should receive an intervention;
- whether a child is at risk;
- whether a safeguarding concern is valid;
- whether a child has a particular condition;
- whether a child should be excluded;
- whether a child should receive a particular educational outcome;
- whether an individual is suitable for a service.

Any AI-assisted analysis must remain subject to meaningful human review.

15. AI Records and Review

Where AI is used for a significant business purpose, Lighthouse Outreach Service will consider recording:

- the AI tool used;
- the purpose;
- the type of information entered;
- whether personal data was involved;
- whether the use was authorised;
- the output produced;
- the human review undertaken.

AI tools will be reviewed periodically.

If a tool changes its privacy arrangements, terms, data retention practices or functionality in a way that creates additional risk, its use will be reconsidered.

16. Cybersecurity Policy

Lighthouse Outreach Service recognises that cybersecurity is essential because business devices may contain confidential information relating to children, young people, adults, parents/carers and schools.

Cybersecurity controls will be proportionate to the risks faced by a sole-trader education business.

17. Devices

The business uses:

- Windows laptop;
- iPad;
- mobile phone;
- external hard drive.

All devices used for business purposes will be protected with:

- a strong password, PIN, biometric authentication or equivalent;
- automatic screen locking;
- current operating-system updates;
- current security updates;
- appropriate anti-malware/security protection where available;
- encryption where available and appropriate.

Devices will not be left unattended while unlocked.

Business devices will not knowingly be lent to other people.

18. Device Loss or Theft

If a device containing or providing access to business information is lost or stolen, Lighthouse Outreach Service will act immediately.

Actions may include:

1. Attempting to locate or remotely secure the device where the relevant service supports this.
2. Changing passwords for accounts accessible from the device.
3. Revoking sessions or access tokens where possible.
4. Contacting the relevant school or organisation if their information may be affected.
5. Assessing whether a personal data breach has occurred.
6. Recording the incident.
7. Notifying the ICO where legally required.

8. Notifying affected individuals where legally required.

19. Passwords

Lighthouse Outreach Service will use:

- unique passwords for important accounts;
- strong passwords;
- a password manager where appropriate;
- multi-factor authentication (MFA) or two-step verification (2SV) wherever available.

Passwords will not be:

- shared with pupils;
- shared with parents;
- shared with schools unless specifically required by an authorised process;
- written in easily accessible locations;
- reused across critical accounts;
- stored in unsecured documents.

The National Cyber Security Centre (NCSC) recommends strong, unique passwords and 2SV/MFA for important accounts.

20. Email Security

Business email will be treated as a potentially sensitive communication channel.

Lighthouse Outreach Service will:

- check recipients before sending information;
- use care when sending attachments;
- avoid sending sensitive information to personal addresses unless authorised and necessary;
- verify unusual requests for information;
- be alert to phishing;
- avoid clicking suspicious links;
- avoid opening unexpected attachments;
- use MFA where available;
- report suspicious emails where appropriate.

Before sending pupil or safeguarding information, the recipient and destination will be checked carefully.

21. Phishing and Social Engineering

Lighthouse Outreach Service recognises that attackers may impersonate:

- schools;
- teachers;
- local authorities;
- parents;
- technology providers;
- banks;
- government organisations;
- suppliers;
- colleagues.

Requests involving passwords, money, personal information, unusual links or urgent action will be treated cautiously.

Where appropriate, Lighthouse Outreach Service will verify the request using a separate trusted communication method.

22. Wi-Fi and School Networks

Where a school provides guest Wi-Fi or another authorised network, Lighthouse Outreach Service will:

- use the network only for legitimate business activities;
- follow the school's acceptable-use requirements;
- never attempt to bypass security controls;
- never scan, probe or test the school's network without written authorisation;
- never attempt to access restricted systems;
- never share guest credentials;
- disconnect from the network when it is no longer required.

School Wi-Fi access will not be interpreted as permission to access school systems or information beyond what has been authorised.

23. School Guest Accounts

Where a school provides Lighthouse Outreach Service with a guest account, it will only be used for the agreed purpose.

The account will not be:

Resilience, Perseverance, Independence

September 2026

- shared;
- used by another person;
- used to access unrelated information;
- used after authorisation has ended.

Lighthouse Outreach Service will notify the school if it no longer requires access.

24. Storage of Information

Lighthouse Outreach Service currently stores some business information locally, including on:

- a Windows laptop;
- an external hard drive.

Where personal or confidential information is stored locally:

- access will be restricted;
- devices will be password protected;
- sensitive information will be encrypted where reasonably available;
- unnecessary copies will be deleted;
- external drives will be stored securely;
- external drives will not be left permanently connected where this creates unnecessary risk;
- information will not be retained longer than necessary.

The NCSC recommends maintaining backups and keeping removable backup devices securely stored and disconnected when not required. National Cyber Security Centre

25. Backups

Lighthouse Outreach Service will maintain appropriate backups of important business information.

Backups should be:

- performed regularly;
- protected from unauthorised access;
- separated from the main device where possible;
- tested periodically;
- updated when important information changes.

Where practical, the business should maintain more than one backup method, such as a secure cloud backup together with an external backup.

26. External Hard Drive

The external hard drive will be:

- stored securely;
- protected against unauthorised access;
- disconnected from the main computer when not being used for backup;
- checked periodically;
- replaced when necessary;
- securely erased or disposed of when no longer required.

If the external hard drive contains confidential school or pupil information, the information will be protected appropriately and securely deleted when retention is no longer required.

27. Photographs of Student Work

Lighthouse Outreach Service may occasionally photograph work completed by a student for the purpose of passing the work to the relevant school.

The following rules apply:

- photographs will only be taken where there is a legitimate and authorised reason;
- the student will be asked for permission before the photograph is taken;
- only the student's work will be photographed;
- pupils will not intentionally be included in the photograph;
- faces and other unnecessary identifying information will not be captured;
- pupil names will not be included unless genuinely necessary and authorised;
- photographs will not be posted on personal social media;
- photographs will not be uploaded to public AI tools;
- photographs will not be used for marketing without the appropriate separate permission/authorisation;
- the photograph will be transferred to the appropriate school/organisation securely where required;
- the photograph will then be deleted when it is no longer required.

The student's permission is an important part of respectful practice, but it does not by itself determine the legal basis for processing. Where the school is responsible for

the pupil's information, Lighthouse Outreach Service will follow the school's instructions and agreed data-protection arrangements.

28. Social Media

Lighthouse Outreach Service will maintain professional boundaries online. The business will not:

- post photographs of pupils without appropriate authorisation;
- identify pupils on social media;
- post confidential school information;
- post safeguarding information;
- discuss individual pupils publicly;
- share screenshots of school communications;
- publish identifiable case studies without appropriate authorisation;
- accept inappropriate personal social-media contact from children and young people where doing so would undermine professional boundaries.

Professional communication will use appropriate business or school-approved channels.

29. Online Mentoring and Communication

Where online communication is used:

- the platform should be appropriate and authorised;
- privacy settings will be configured appropriately;
- meeting links will not be unnecessarily shared publicly;
- recording will not take place unless expressly authorised;
- children and young people will not be asked to communicate through inappropriate personal channels;
- personal information will be minimised;
- professional boundaries will be maintained.

Lighthouse Outreach Service will follow any online meeting requirements established by the school.

30. Safeguarding and Online Safety

Cybersecurity and safeguarding are connected.

Lighthouse Outreach Service will take appropriate action where online activity raises concerns about:

Resilience, Perseverance, Independence

September 2026

- abuse;
- neglect;
- exploitation;
- grooming;
- bullying;
- cyberbullying;
- sexual exploitation;
- inappropriate sexual content;
- self-harm;
- radicalisation;
- criminal exploitation;
- harmful online behaviour;
- inappropriate contact with children.

Safeguarding concerns will be reported using the procedures of the school, local authority or commissioning organisation involved.

Lighthouse Outreach Service will not attempt to conduct its own safeguarding investigation unless specifically required and authorised to do so.

Where there is an immediate risk of harm, appropriate emergency or safeguarding services will be contacted.

31. Confidentiality

Information received through professional work will be treated confidentially.

Confidentiality may need to be broken where:

- there is a safeguarding concern;
- there is a serious risk of harm;
- disclosure is required by law;
- disclosure is necessary under contractual or professional arrangements;
- the relevant organisation has authorised disclosure.

Children and young people will not be promised absolute confidentiality where safeguarding responsibilities apply.

32. Data Minimisation

Lighthouse Outreach Service will aim to collect and retain only the information required to deliver its services.

Resilience, Perseverance, Independence

September 2026

For example, where a school only needs confirmation that an intervention took place, Lighthouse Outreach Service will not automatically retain unrelated pupil information.

Where detailed information is necessary, it will be handled securely and retained only for the appropriate period.

33. Data Retention

Lighthouse Outreach Service will maintain a proportionate retention approach. Information will be reviewed periodically and securely deleted when it is no longer required.

Particular attention will be given to:

- pupil records;
- safeguarding information;
- intervention notes;
- photographs;
- school documents;
- emails containing personal information;
- downloaded school files;
- temporary files;
- information held on external hard drives.

Where a school or local authority specifies a retention period, Lighthouse Outreach Service will follow the agreed requirement.

Where no retention period is specified, information will be retained only for as long as reasonably necessary for the purpose for which it was collected, contractual obligations, legal requirements and legitimate business record-keeping.

34. Secure Deletion

When information is no longer required, Lighthouse Outreach Service will delete it securely.

This includes:

- electronic files;
- photographs;
- downloaded school documents;
- temporary copies;
- duplicate records;
- external-drive copies.

Simply moving a file to a recycle bin will not necessarily be treated as sufficient where the information is particularly sensitive and more secure deletion is reasonably required.

35. Third-Party Services

Before using a new online service, AI tool, cloud platform or software application for business purposes, Lighthouse Outreach Service will consider:

- what information the service collects;
- whether personal data is involved;
- where the data is stored;
- whether data is transferred internationally;
- whether the provider uses information for training or other purposes;
- security measures;
- account controls;
- deletion arrangements;
- contractual terms;
- whether the school has approved the service.

A free service will not automatically be considered safe for confidential information.

36. Data Protection by Design

Privacy and security will be considered before introducing new technology, particularly where it involves:

- children;

Resilience, Perseverance, Independence

September 2026

- special category data;
- safeguarding information;
- AI;
- automated processing;
- photographs;
- online platforms;
- new cloud services.

Where processing is likely to result in a high risk to individuals, Lighthouse Outreach Service will consider whether a Data Protection Impact Assessment (DPIA) or other formal risk assessment is required.

The Information Commissioner's Office (ICO) specifically recommends a risk-based approach and data protection by design and default when AI involves personal data.

37. Data Breaches

A personal data breach may include:

- sending information to the wrong person;
- losing a laptop;
- losing an external hard drive;
- unauthorised access to an account;
- hacking;
- ransomware;
- accidentally publishing information;
- unauthorised disclosure;
- accidental deletion;
- theft of information;
- a compromised email account.

All suspected breaches must be taken seriously.

The business will not wait for complete certainty before taking protective action.

38. Breach Reporting

Where Lighthouse Outreach Service is acting as a processor, it will notify the relevant controller/school without undue delay in accordance with the contractual arrangement.

Where Lighthouse Outreach Service is the controller, it will assess whether the breach must be reported to the ICO.

A reportable personal data breach must generally be reported to the ICO without undue delay and, where feasible, within 72 hours of becoming aware of it. If the breach is likely to result in a high risk to individuals, those affected may also need to be informed without undue delay.

The ICO recommends documenting breach decisions and maintaining an appropriate breach log.

39. Cyber Incident Response

If Lighthouse Outreach Service suspects that a device or account has been compromised, the following approach will be used:

1. Stop the suspected activity where safe to do so.
2. Disconnect an affected device from networks if appropriate.
3. Do not knowingly destroy evidence.
4. Change compromised passwords from a safe device.
5. Enable or reset MFA where necessary.
6. Contact the relevant school/organisation if its information may be affected.
7. Assess whether personal data has been compromised.
8. Record what happened.
9. Consider whether the ICO must be notified.
10. Take steps to recover and prevent recurrence.

Where ransomware or malware is suspected, the affected device should not be reconnected to sensitive systems until it has been assessed and appropriately secured.

40. Cybersecurity Incident Examples

Incidents include:

- clicking a phishing link;

Resilience, Perseverance, Independence

September 2026

- entering a password into a fraudulent website;
- losing a phone;
- losing a laptop;
- losing an external hard drive;
- accidentally emailing a pupil record to the wrong person;
- discovering malware;
- an AI account containing personal information being compromised;
- a school login being used by someone else;
- sending confidential information through an insecure channel;
- discovering that confidential information has been uploaded to an unauthorised AI system.

All such incidents should be recorded and assessed.

41. Professional Boundaries

Lighthouse Outreach Service will maintain appropriate professional boundaries when working with children, young people and adults.

Digital communication will remain professional and relevant to the service.
The business will avoid:

- inappropriate private messaging;
- sharing personal or intimate information;
- inappropriate social-media relationships;
- using disappearing-message services for professional records where this conflicts with school requirements;
- storing pupil information in personal messaging applications unless specifically authorised.

42. Use of Personal Devices

Where a personal device is used for business purposes, the same security expectations apply.

The device should:

- have a secure passcode;
- use biometric security where appropriate;
- be kept updated;
- use appropriate security controls;
- be protected from unauthorised access;
- not be shared with children or service users;
- be capable of securely deleting business information when it is no longer required.

Where practical, business information should be separated from personal information.

43. Working Remotely

When working away from school premises, Lighthouse Outreach Service will:

- avoid discussing confidential information where others can overhear;
- avoid leaving documents visible in public places;
- avoid using unsecured public Wi-Fi where sensitive information is being accessed;
- secure devices when travelling;
- avoid leaving devices unattended in vehicles;
- use appropriate screen locking;
- ensure confidential documents are stored securely.

44. Physical Security

Paper records containing personal or confidential information, where used, will be:

- kept secure;
- transported only where necessary;
- not left unattended;
- disposed of securely.

Sensitive information should not be left visible in vehicles, classrooms or public areas.

45. Training and Awareness

As the business is operated by one person, the director is responsible for maintaining their own awareness of:

Resilience, Perseverance, Independence

September 2026

- safeguarding;
- data protection;
- AI risks;
- phishing;
- cybersecurity;
- school-specific requirements;
- changes to relevant guidance.

Relevant training will be undertaken periodically and particularly where the nature of the services or technology changes.

46. School-Specific Requirements

Before commencing work with a new school or organisation, Lighthouse Outreach Service will establish, where applicable:

- the school's safeguarding arrangements;
- the appropriate safeguarding contact;
- data-protection arrangements;
- whether a data-processing agreement is required;
- how pupil information will be shared;
- what information may be accessed;
- retention requirements;
- photography requirements;
- acceptable-use requirements;
- IT/network requirements;
- approved communication methods;
- incident-reporting arrangements.

47. Records of Processing

Lighthouse Outreach Service will maintain appropriate records of its processing activities where legally required or otherwise useful to demonstrate accountability. These may include:

- categories of people whose information is processed;
- types of information;
- purposes;
- recipients;
- retention arrangements;
- security measures;
- controller/processor status;

- relevant schools or organisations.

48. Risk Management

Lighthouse Outreach Service will periodically consider risks associated with:

- children and young people's information;
- safeguarding information;
- SEND information;
- devices;
- email;
- AI;
- cloud services;
- external hard drives;
- remote working;
- photographs;
- school network access.

Where a significant risk is identified, appropriate controls will be introduced.

49. Policy Review

This policy will be reviewed at least annually and sooner where:

- legislation changes;
- government guidance changes;
- ICO guidance changes;
- NCSC guidance changes;
- a significant cyber incident occurs;
- a data breach occurs;
- a new AI tool is introduced;
- services change;
- a school requires additional controls;
- new technology is introduced.

The policy owner will maintain the current version.

50. Declaration

Lighthouse Outreach Service recognises its responsibility to protect children, young people, adults and schools from unnecessary risks arising from the use of technology, AI and digital information.

Resilience, Perseverance, Independence

September 2026

The business is committed to responsible, proportionate and secure use of technology and to maintaining professional standards when working in education settings.

This policy should be read alongside relevant safeguarding, data-protection, confidentiality and school-specific requirements.

Policy owner: Lighthouse Outreach Service

Version: 1.0

Effective: 2 September 2026

Review: 2 September 2027

Signed: *T. Adams*

Name: Trevor Adams

Date: 02/03/2026

LIGHTHOUSE OUTREACH SERVICE

AI ACCEPTABLE USE – ONE-PAGE GUIDE

Lighthouse Outreach Service

Resilience, Perseverance, Independence

September 2026

Our commitment

Lighthouse Outreach Service may use artificial intelligence (AI) to support administrative work, educational resource development and creative thinking.

AI is used as an **assistive tool, not as a replacement for professional judgement.**

Because Lighthouse Outreach Service works directly with children and young people, particular care is taken with personal, sensitive and safeguarding information.

AI CAN BE USED FOR

- Generic educational ideas
- Mentoring activity ideas
- Training ideas
- Generic intervention resources
- Brainstorming
- Creating fictional scenarios
- Proofreading non-confidential text
- Generic templates
- Public information
- Creating age-appropriate resource ideas

USE CAUTION

Before entering information into an AI system, Lighthouse Outreach Service considers whether someone could be identified from the information.

Examples include:

- anonymised case studies;
- information derived from school circumstances;
- unusual or highly specific scenarios;
- information that has been altered but may still identify an individual.

Where there is uncertainty, the information is not entered.

NEVER ENTER INTO PUBLIC AI TOOLS

Lighthouse Outreach Service does not enter identifiable:

Resilience, Perseverance, Independence

September 2026

- pupil names;
- pupil records;
- SEND information;
- safeguarding information;
- medical information;
- addresses;
- contact details;
- intervention records;
- mentoring records;
- school confidential information;
- photographs of pupils;
- passwords;
- usernames;
- security information.

School documents are not uploaded to public AI systems unless the school has specifically authorised this and the appropriate data-protection requirements have been addressed.

OUR PRINCIPLE

If I would not put it in an email to an unauthorised person, I will not put it into a public AI tool.

When in doubt: DON'T UPLOAD IT.

Lighthouse Outreach Service – AI Acceptable Use Guide – Version 1.0

LIGHTHOUSE OUTREACH SERVICE

CYBERSECURITY INCIDENT RESPONSE PROCEDURE

Resilience, Perseverance, Independence

September 2026

Version: 1.0

Effective: 2 September 2026

1. Purpose

This procedure explains what Lighthouse Outreach Service will do if a device, account, system or information may have been compromised.

An incident should be treated seriously even if it is not yet clear whether personal data has been affected.

2. Examples of Incidents

Examples include:

- lost or stolen laptop;
- lost or stolen phone;
- lost external hard drive;
- phishing attack;
- compromised email account;
- malware or ransomware;
- suspicious login;
- stolen password;
- accidental disclosure of information;
- information sent to the wrong person;
- unauthorised access to school information;
- confidential information uploaded to an unauthorised AI system;
- suspicious software;
- accidental publication of confidential information.

3. Immediate Response

Step 1 – Stop

Stop the activity that may be causing the problem.

If appropriate, disconnect the affected device from Wi-Fi or other networks.

Do not continue using a potentially compromised system unnecessarily.

Step 2 – Protect

From a safe device where possible:

Resilience, Perseverance, Independence

September 2026

- change affected passwords;
- enable/reset MFA;
- sign out other sessions;
- contact the relevant service provider;
- secure important accounts.

Step 3 – Tell the Right Organisation

If the incident involves information supplied by a school or local authority, contact the appropriate school/organisation immediately in accordance with the agreed incident-reporting procedure.

Do not conceal an incident because it appears minor.

Step 4 – Assess

Determine:

- what happened;
- when it happened;
- what information may be affected;
- whose information may be affected;
- whether children or vulnerable people are involved;
- whether confidential school information is involved;
- whether access was unauthorised;
- whether the information has been disclosed;
- what immediate steps have been taken.

Step 5 – Record

Create an incident record containing:

Date/time discovered: _____

Date/time incident occurred (if known): _____

What happened: _____

Device/account involved: _____

Information involved: _____

People potentially affected: _____

School/organisation notified: _____

Immediate action taken: _____

Further action required: _____

4. Personal Data Breach

If personal data may have been lost, accessed, disclosed, destroyed or altered without authorisation, assess whether a personal data breach has occurred.

If Lighthouse Outreach Service is acting as a processor, the relevant controller/school must be informed without undue delay in accordance with the contractual arrangements.

If Lighthouse Outreach Service is acting as controller, it will assess whether notification to the ICO is required.

Where a reportable breach is required to be notified to the ICO, the normal deadline is without undue delay and, where feasible, within 72 hours of becoming aware of the breach.

5. High-Risk Breaches

Particular urgency applies where the incident involves:

- children;
- safeguarding information;
- SEND information;
- medical information;
- large amounts of personal information;
- passwords;
- financial information;
- identity information;
- unauthorised access;
- information that could cause significant harm.

The relevant school/organisation should be contacted immediately where its information is involved.

6. If Ransomware or Malware Is Suspected

- Disconnect the affected device from networks where appropriate.
- Do not knowingly spread or copy the affected files.
- Do not delete evidence unnecessarily.
- Do not reconnect the device until it has been appropriately assessed.
- Change important passwords using a safe device.
- Contact relevant organisations if their data may be affected.
- Consider professional technical assistance where necessary.
- Assess whether a personal data breach has occurred.

7. Lost or Stolen Device

If a device is lost or stolen:

1. Attempt remote location/locking if available.
2. Change important passwords.
3. Revoke access where possible.
4. Notify the relevant school if its information may be present.
5. Assess whether personal data is involved.
6. Record the incident.
7. Assess whether the ICO must be notified.
8. Consider whether affected individuals must be informed.

8. Phishing

If a phishing message has been opened:

- do not provide further information;
- close the suspicious page;
- disconnect if malware is suspected;
- change the relevant password from a safe device;
- enable MFA;
- monitor the account;
- report the incident.

If a password was entered into a fraudulent website, treat that password as compromised immediately.

9. After the Incident

Following an incident, Lighthouse Outreach Service will consider:

- what caused the incident;

Resilience, Perseverance, Independence

September 2026

- whether personal data was involved;
- whether safeguarding implications exist;
- whether security controls need strengthening;
- whether passwords need changing;
- whether training is required;
- whether this policy needs updating;
- whether similar incidents could be prevented.

Lessons learned will be recorded.

Emergency Principle

When in doubt, report the incident promptly rather than waiting for complete certainty.

Lighthouse Outreach Service will cooperate with schools, local authorities, the ICO, the NCSC, law enforcement or other relevant organisations where appropriate.

Policy owner: Lighthouse Outreach Service

Review date: 2 September 2027

LIGHTHOUSE OUTREACH SERVICE

PERSONAL DATA BREACH PROCEDURE & BREACH LOG

Resilience, Perseverance, Independence

September 2026

Version: 1.0

Effective: 2 September 2026

PART A – BREACH PROCEDURE

1. What Is a Personal Data Breach?

A personal data breach can involve:

- unauthorised access;
- unauthorised disclosure;
- accidental disclosure;
- loss;
- theft;
- destruction;
- alteration;
- hacking;
- malware;
- ransomware;
- sending information to the wrong recipient;
- loss of a device containing personal information.

2. First Response

As soon as a potential breach is discovered:

1. Contain

Take immediate steps to stop further access or disclosure.

2. Protect

Secure accounts, devices and information.

3. Notify

If the information belongs to a school or local authority, notify the appropriate organisation according to the agreed arrangements.

4. Assess

Determine:

- what happened;

Resilience, Perseverance, Independence

September 2026

- what information was involved;
- who may be affected;
- how many people may be affected;
- whether children are involved;
- whether special category or safeguarding information is involved;
- whether the information was encrypted;
- whether the information has been recovered;
- the likely consequences.

5. Record

Record the incident and the decisions made.

3. ICO Notification

Where Lighthouse Outreach Service is the controller and a breach is likely to result in a risk to individuals' rights and freedoms, the ICO should be notified without undue delay and, where feasible, within 72 hours of becoming aware of the breach.

If the risk is high, affected individuals may also need to be informed without undue delay.

Where Lighthouse Outreach Service is a processor, the relevant controller/school must be notified in accordance with the applicable contractual arrangements.

PART B – BREACH LOG

Incident Reference

Reference number: LOS-BR-_____

Date discovered: _____

Time discovered: _____

Date incident occurred: _____

Person discovering incident: Director

1. Description of Incident

What happened?

2. Type of Incident

Tick as appropriate:

- ☐ Lost device
- ☐ Stolen device
- ☐ Lost external hard drive
- ☐ Email sent to wrong recipient
- ☐ Unauthorised disclosure
- ☐ Unauthorised access
- ☐ Hacking
- ☐ Phishing
- ☐ Malware
- ☐ Ransomware
- ☐ Accidental deletion
- ☐ AI-related incident
- ☐ Photograph/data issue
- ☐ Other: _____

3. Information Involved

- ☐ Names
- ☐ Contact information
- ☐ Pupil information
- ☐ SEND information
- ☐ Safeguarding information
- ☐ Health information
- ☐ Mentoring information

- ☐ Intervention information
- ☐ School information
- ☐ Financial information
- ☐ Passwords/access information
- ☐ Photographs
- ☐ Other: _____

4. People Potentially Affected

Number of people:

Categories:

- ☐ Children
- ☐ Young people
- ☐ Adults
- ☐ Parents/carers
- ☐ School staff
- ☐ Other

5. Special Circumstances

Does the incident involve:

- ☐ Children
- ☐ Vulnerable people
- ☐ Safeguarding information
- ☐ SEND information
- ☐ Health information
- ☐ Large amounts of information
- ☐ Passwords
- ☐ Identity information

If yes, provide details:

6. Immediate Containment

What action was taken?

Date/time:

7. School/Organisation Notification

Was a school or commissioning organisation involved?

- ☐ Yes
- ☐ No

If yes:

Organisation: _____

Person contacted: _____

Date/time: _____

Method: _____

8. ICO Assessment

Is Lighthouse Outreach Service acting as:

- ☐ Controller
- ☐ Processor
- ☐ Other/unclear – advice required

Does the incident meet the threshold for ICO notification?

- ☐ Yes
- ☐ No
- ☐ Under assessment

Resilience, Perseverance, Independence

September 2026

Reason for decision:

9. ICO Notification

Date/time reported: _____

ICO reference: _____

If not reported, reason:

10. Individual Notification

Is notification to affected individuals required?

- ☐ Yes
- ☐ No
- ☐ Under assessment

Reason:

11. Outcome

12. Lessons Learned

What could prevent this happening again?

13. Actions

Resilience, Perseverance, Independence

September 2026

Action	Responsible person	Deadline Completed
--------	--------------------	--------------------

☐	Director	
☐	Business & Marketing Manager	

14. Closure

Incident closed: _____

Reviewed by: Director

Date: _____

Further review required: Yes / No