Nested Learning Information Governance Policy

Last updated 21 August 2026

Organisation: Nested Learning Ltd
Version: 1.0
Publication date: August 2026

Review: At least annually, and sooner following a material change in law, technology, services, information risk or organisational structure.

1. Purpose
   Information is a core business asset of Nested Learning.
   We depend on accurate, secure and appropriately governed information to provide educational technology, support learners and customers, manage our organisation, meet contractual obligations and improve our services.
   This policy sets out how Nested Learning creates, collects, uses, stores, shares, secures, retains and disposes of information.
   It applies to personal data and to other information that requires protection because it is confidential, commercially sensitive, operationally important or entrusted to us by another organisation.
   Our objective is straightforward: information should be lawful, accurate, necessary, appropriately accessible, secure and retained only for as long as there is a legitimate reason to keep it.
2. Scope
   This policy applies to:
   employees, directors, workers, contractors and consultants;
   people acting on behalf of Nested Learning;
   information held in Nested Learning systems, devices, cloud services and records;
   information provided by learners, customers, partners, suppliers and other third parties;
   personal data processed by Nested Learning as a controller or processor;
   learner conversations, transcripts, learning analytics and associated metadata;

business, financial, contractual and governance records;
source documents and materials supplied for use within Nested Learning services;
information generated by AI-assisted systems; and
paper records where these are used.
The policy applies whether information is held permanently or temporarily.

3. Related Nested Learning documents
This policy is the overarching information-governance policy for Nested Learning.
It should be read alongside:
the Nested Learning Privacy Policy, which explains how Nested Learning collects, uses, shares and retains personal data and how individuals can exercise their information rights;
the Nested Learning Security Statement, which describes our current technical and organisational security approach in plain language; and
any applicable customer contract, data-processing agreement, pilot agreement, retention schedule, privacy notice, information-sharing agreement or security schedule.
These documents have different purposes.
The Privacy Policy provides public-facing transparency about personal-data processing. The Security Statement describes the current security position without disclosing sensitive technical details. This Information Governance Policy sets the organisation-wide principles and responsibilities within which both operate.
Where a service-specific agreement lawfully imposes a more specific or higher standard, that requirement will be followed for the relevant service.

4. Information governance principles
Nested Learning will seek to ensure that information is:
used lawfully, fairly and transparently;
collected for clear and legitimate purposes;
limited to what is reasonably necessary;
accurate and kept up to date where necessary;
retained for no longer than required;
protected against unauthorised access, loss, alteration or disclosure;
available to authorised people when legitimately required;
managed through its complete lifecycle, from creation or collection to secure deletion or preservation;
shared only where there is a lawful and appropriate reason; and
governed in a way that can be evidenced and reviewed.
These principles apply to system design as well as day-to-day working practices.

5. Legal framework
Nested Learning operates within the UK information-governance and data-protection framework.

The principal legislation includes:
the UK General Data Protection Regulation (UK GDPR);
the Data Protection Act 2018;
the Data (Use and Access) Act 2025, which amended UK data-protection and privacy law;
the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR), as amended;
the Computer Misuse Act 1990;
the Copyright, Designs and Patents Act 1988; and
other legislation applying to particular records, activities, contracts or sectors.
The data-protection provisions of the Data (Use and Access) Act 2025 are in force. Nested Learning will therefore apply the UK GDPR and Data Protection Act 2018 as amended by that Act, rather than relying on older pre-reform wording.
Where Nested Learning processes information on behalf of a university, college, training provider, employer, local authority or other customer, additional statutory, regulatory or contractual requirements may apply.
Nested Learning seeks to work within the confines of this policy wherever reasonable and legally necessary.
This does not make legal compliance optional. Where legislation imposes a duty, that duty takes precedence. Where the law applies a test of reasonableness, necessity or proportionality, Nested Learning will apply that test to the circumstances.

6. Public-sector information duties
   Nested Learning is a private company.
   The Freedom of Information Act 2000 and Environmental Information Regulations 2004 do not automatically apply to Nested Learning merely because we work with universities, colleges, local authorities or other public bodies.
   Information held by a public-sector customer may nevertheless be subject to that organisation's access-to-information obligations.
   Where a customer requires reasonable assistance in locating, reviewing or supplying information within its control, Nested Learning will co-operate in accordance with the applicable contract and law.
   Nothing in this policy represents Nested Learning as a public authority where it is not one.
7. Accountability and responsibilities
   Information governance is a management responsibility.
   Senior leadership is responsible for ensuring that:
   material information risks are identified and managed;
   appropriate technical and organisational controls are in place;
   responsibilities are assigned clearly;
   data-protection and security considerations are included in material business

decisions;
incidents, requests and complaints are handled properly;
suppliers processing important or sensitive information are appropriately governed; and
evidence of compliance is maintained where required.
Everyone working for or on behalf of Nested Learning is responsible for handling information appropriately within their role.
No individual should access, use, copy, disclose or retain information simply because technical access is available.
Access must have a legitimate business purpose.

8. Controller and processor responsibilities
   Nested Learning may act as either a data controller or a data processor, depending on the service and processing activity.
   For general website, enquiry, marketing, customer-management and direct commercial administration purposes, Nested Learning will normally act as a controller.
   In institutional AI Tutor and learning-analytics deployments, the customer organisation will often act as controller for learner activity and institutional reporting while Nested Learning acts as processor.
   The exact roles must be determined by the facts and not merely by labels in a contract.
   Where Nested Learning acts as processor, we will:
   process personal data only on documented instructions, unless law requires otherwise;
   apply appropriate security;
   ensure people authorised to process the data are subject to confidentiality obligations;
   assist the controller with relevant data-protection duties where required;
   govern subprocessors appropriately;
   return or delete personal data as agreed at the end of the service, subject to lawful retention requirements; and
   provide information reasonably necessary to demonstrate compliance with processor obligations.
   The public description of this model is set out in the Nested Learning Privacy Policy.
9. Data minimisation and pseudonymisation
   Nested Learning will seek to collect and expose as little personal information as reasonably necessary.
   Our AI Tutor services are designed, where possible, to operate using pseudonymous session or user identifiers rather than learner names or email addresses.
   Institutional systems should retain formal learner identity and core student records

where there is no need for those identifiers to enter the Nested Learning service.
Pseudonymised information remains personal data where it can be linked back to an identifiable person through additional information. It must therefore continue to be protected appropriately.
Users should not enter unnecessary personal, confidential, financial, health, immigration or other sensitive information into AI systems or free-text fields unless it is genuinely required for the service.

10. Lawful and fair processing
    Personal data will be processed only where a valid lawful basis applies.
    Depending on the activity, this may include:
    performance of a contract or steps requested before entering a contract;
    consent;
    compliance with a legal obligation;
    legitimate interests, subject to the appropriate balancing of interests and individual rights;
    recognised legitimate interests where that statutory basis is available and appropriate; or
    another lawful basis available under data-protection law.
    Where special-category personal data or criminal-offence data is processed, an additional legal condition will be identified where required.
    Consent will not be used merely because it appears convenient. Where processing is necessary for a contract, legal obligation or another more appropriate basis, that basis should be used instead.
    The relevant public-facing explanations are set out in the Nested Learning Privacy Policy.
11. Privacy by design and by default
    Privacy and information governance should be considered when a system or process is designed, not added after deployment.
    Nested Learning will seek to:
    minimise unnecessary personal data;
    limit default access;
    use pseudonymous identifiers where practical;
    separate customer or organisation data appropriately;
    define retention and deletion arrangements;
    assess suppliers and data flows;
    consider information rights;
    identify security requirements; and
    document significant decisions where appropriate.
    This reflects Nested Learning's existing commitment to privacy by design in its Privacy Policy and security-conscious design in its Security Statement.

12. Data Protection Impact Assessments

    A Data Protection Impact Assessment (DPIA) will be completed where data-protection law requires one, particularly where proposed processing is likely to result in a high risk to people's rights and freedoms.

    A DPIA may also be used voluntarily where it provides a useful governance record for material new processing.

    Potential triggers can include:

    new uses of AI involving personal data;

    large-scale or systematic monitoring;

    new processing of sensitive data;

    significant profiling or automated decision-making;

    processing involving children or other potentially vulnerable groups;

    linking datasets in a way that materially changes privacy risk; or

    introducing technology that creates a materially different level of surveillance, access or inference.

    A DPIA should identify the purpose of processing, necessity and proportionality, risks to people, and measures used to reduce those risks.

    If a high residual risk cannot be adequately reduced, the legal requirement to consult the Information Commissioner's Office will be considered before processing begins.

13. Artificial intelligence and learning analytics

    Nested Learning's work includes AI-assisted learning, generated feedback, session analysis and learning analytics.

    Information produced by an AI system can itself become an organisational record and, where it relates to an identifiable person, may be personal data.

    AI-generated information should therefore be governed according to its content and use, not treated as exempt merely because a machine produced it.

    Nested Learning will seek to ensure that:

    AI systems process only information reasonably required for the relevant service;

    institutional learner identity is separated from AI Tutor processing where practical;

    outputs are not automatically treated as verified facts;

    inferred learning indicators are clearly understood as analytical outputs rather than formal academic records unless expressly agreed otherwise;

    significant decisions are not delegated to AI without an appropriate lawful basis, safeguards and human oversight;

    prompts, responses, transcripts, summaries and analytics are given appropriate retention and access controls;

    third-party AI providers are governed as suppliers or processors where applicable; and

    uses of AI remain consistent with the Nested Learning Privacy Policy and other applicable policies.

Nested Learning's Privacy Policy states that its AI-assisted learning tools are not used to make solely automated decisions that have legal or similarly significant effects on users. This Information Governance Policy adopts the same position.

14. Information classification

    Information should be handled according to its sensitivity and the consequences of inappropriate disclosure or loss.

    Nested Learning uses the following practical classification approach:

    Public

    Information approved for public release.

    Examples include published website content, public policies, published marketing material and public product information.

    Internal

    Routine operational information not intended for unrestricted publication but unlikely to cause significant harm if disclosed.

    Examples may include ordinary internal procedures, routine meeting notes and non-sensitive working documents.

    Confidential

    Information where unauthorised disclosure could harm an individual, customer, partner or Nested Learning.

    Examples may include customer information, contracts, learner records, non-public analytics, financial information, staff information and commercially sensitive material.

    Restricted

    Highly sensitive information requiring tightly controlled access.

    Examples may include authentication secrets, security credentials, encryption keys, particularly sensitive personal data, safeguarding records, incident evidence or material whose exposure could create a serious security risk.

    The classification should influence access, storage, transmission, sharing and disposal.

    Technical secrets and credentials must never be treated as ordinary documents merely because they are stored electronically.

15. Access control

    Access to information will be based on legitimate need.

    Nested Learning will seek to use:

    authenticated access;

    role-appropriate permissions;

    limited administrative access;

    short-lived or scoped credentials where appropriate;

    separation between ordinary user and administrative functions;

    organisation-level or tenant-level separation where supported;

secure management of secrets; and
prompt removal or adjustment of access when it is no longer required.
These principles reflect the current controls described in the Nested Learning Security Statement.
People with privileged or administrative access must use it only for authorised purposes.

16. Information security
    Nested Learning will apply technical and organisational measures appropriate to the nature of the information and the risk.
    Controls may include:
    encryption in transit;
    access controls;
    secure authentication;
    pseudonymisation;
    server-side protection of secrets;
    organisation-level data separation;
    secure hosting;
    monitoring and logging;
    restricted administrative and diagnostic functions;
    controlled file and document handling;
    dependency management;
    secure development practices;
    backup and recovery arrangements;
    malware and abuse prevention;
    supplier controls; and
    regular review and testing where appropriate.
    The detailed public description of the current position is maintained in the Nested Learning Security Statement.
    That statement is intentionally transparent about the present assurance position.
    Nested Learning will not claim Cyber Essentials, ISO 27001, SOC 2 or another external certification unless and until that certification has actually been obtained.
17. Records management
    Records should be sufficient to demonstrate what happened, support legitimate business activity and meet legal or contractual requirements.
    Records should be:
    understandable;
    accurate so far as reasonably possible;
    attributable where necessary;
    stored in an appropriate location;
    protected according to sensitivity;

capable of being found when legitimately required; and
retained or disposed of according to an appropriate retention decision.
Material business decisions should not depend solely on information kept in uncontrolled personal accounts, informal messaging threads or other locations that cannot reasonably form part of the organisational record.
Duplicate and superseded information should not be retained indefinitely without reason.

18. Data quality
    Information used to make important decisions should be sufficiently accurate, complete and current for the purpose.
    Where Nested Learning becomes aware that personal data is materially inaccurate, reasonable steps will be taken to correct or qualify it.
    AI-generated summaries, classifications or analytics must not automatically be assumed to be factually correct.
    Where their use could materially affect a learner, customer, worker or other person, appropriate human judgement and source evidence should be considered.
19. Retention and disposal
    Information should not be kept indefinitely merely because storage is technically cheap.
    Retention will be determined by factors including:
    the purpose for which the information is held;
    applicable law;
    contractual requirements;
    customer instructions where Nested Learning acts as processor;
    accounting and tax requirements;
    limitation and dispute periods;
    security and fraud-prevention needs;
    safeguarding requirements; and
    legitimate evidential or operational requirements.
    The Nested Learning Privacy Policy sets out public-facing examples of current retention arrangements, including enquiry records, customer records, learning-service records, AI interaction data, telemetry, diagnostic information and accounting records.
    Institutional AI Tutor retention may be defined by the relevant customer agreement, service configuration or data-processing agreement.
    When information is no longer required, it should be securely deleted, destroyed or irreversibly anonymised as appropriate.
    A deletion process should take account of backups, replicas and third-party processors where relevant.

20. Information sharing

    Information may be shared internally or externally only where there is a legitimate purpose and an appropriate legal and governance basis.

    Before material sharing, Nested Learning should consider:

    what information is actually required;

    why it is being shared;

    whether personal data is involved;

    the lawful basis;

    whether special-category or criminal-offence data is involved;

    whether the recipient is a controller, processor or other party;

    contractual requirements;

    security in transit and at the destination;

    retention after sharing; and

    whether the individual has been given appropriate privacy information.

    Only the minimum information reasonably necessary should normally be shared.

    Safeguarding, fraud prevention, legal obligations and serious security incidents may justify information sharing where the law permits or requires it.

    Data-protection law should not be incorrectly used as a reason to prevent lawful and necessary safeguarding action.

21. Suppliers, subprocessors and third parties

    Third-party systems can create information-governance risk even where Nested Learning does not directly host the underlying infrastructure.

    Suppliers that process personal, confidential or operationally significant information should be reviewed proportionately.

    Depending on the risk, this may include considering:

    the service being provided;

    the categories of information processed;

    processing locations;

    security controls;

    contractual data-protection terms;

    subprocessor arrangements;

    incident notification;

    deletion and return of data;

    service continuity;

    international transfers; and

    relevant assurance or certification.

    Where a supplier acts as a processor for Nested Learning, an appropriate written processing arrangement will be maintained as required by law.

    The use of third-party AI providers is addressed publicly in the Nested Learning Privacy Policy.

22. International transfers

    Where personal data is transferred outside the United Kingdom in a way that constitutes a restricted transfer, Nested Learning will use an appropriate lawful mechanism.

    Depending on the circumstances, this may include:

    UK adequacy regulations;

    the UK International Data Transfer Agreement;

    the UK Addendum to the EU Standard Contractual Clauses; or

    another lawful transfer mechanism.

    A transfer risk or data-protection test and additional safeguards will be used where required.

    The existence of a global cloud or AI service does not, by itself, remove Nested Learning's responsibility to consider where and how personal data is processed.

23. Individual information rights

    Individuals may have rights under UK data-protection law, including rights relating to:

    being informed;

    access to personal data;

    correction of inaccurate information;

    erasure;

    restriction of processing;

    data portability;

    objection;

    direct marketing;

    withdrawal of consent; and

    automated decision-making.

    Rights are not absolute in every circumstance.

    Requests will be handled according to the law applying to the request. Where the law permits reasonable and proportionate searches in response to an information-rights request, Nested Learning will apply that standard fairly rather than requiring disproportionate searches.

    Where Nested Learning acts only as processor, it may need to refer a request to or assist the relevant controller rather than respond independently.

    Privacy and information-rights enquiries may be sent to:

    info@nestedlearning.uk

    Further information is provided in the Nested Learning Privacy Policy.

24. Data-protection complaints

    Nested Learning maintains a process for complaints concerning its processing of personal data.

    This reflects the requirements introduced by the Data (Use and Access) Act 2025, including the data-protection complaints provisions in force from 19 June 2026.

A person who believes Nested Learning has handled their personal data improperly may complain to:

info@nestedlearning.uk

Nested Learning will:

acknowledge the complaint within 30 days;

take appropriate steps to investigate it;

keep the complainant informed where an investigation is ongoing;

provide an outcome without undue delay;

explain relevant findings and action where appropriate; and

maintain an appropriate record of the complaint and its handling.

A complainant may also have the right to complain to the Information Commissioner's Office (ICO).

Where another organisation is the controller for the processing complained about, Nested Learning may refer the complainant to that organisation or work with it to resolve the matter.

25. Personal data breaches and information incidents

    An information incident may include:

    loss or theft of information or a device;

    disclosure to the wrong person;

    unauthorised system access;

    accidental deletion or alteration;

    malware or account compromise;

    inappropriate publication;

    loss of availability;

    incorrect customer or tenant access;

    exposure of credentials or secrets; or

    any other event affecting the confidentiality, integrity or availability of information.

    Suspected incidents must be reported internally as soon as reasonably possible.

    Nested Learning will assess:

    what happened;

    what information is affected;

    whose information is involved;

    whether the incident is continuing;

    the likely consequences;

    immediate containment;

    recovery and remediation;

    contractual notification requirements;

    whether notification to the ICO is required; and

    whether affected individuals must be informed.

    Where a reportable personal data breach occurs, Nested Learning will meet the

applicable statutory notification timeframe.
Where Nested Learning acts as processor, it will notify the relevant controller without undue delay in accordance with law and the applicable agreement.

26. Logging, monitoring and diagnostics
    Operational logs and diagnostics are necessary for security, reliability, troubleshooting and service improvement.
    They should nevertheless be designed to avoid unnecessary exposure of learner or customer information.
    Where practical, operational telemetry should focus on information such as:
    timestamps;
    service status;
    errors;
    access events;
    model or system use;
    latency;
    token or resource use; and
    other technical indicators.
    Full content should not be copied into logs merely because it is technically possible.
    The Nested Learning Security Statement describes the current approach to monitoring, logging and protected diagnostics.
27. Backups, resilience and continuity
    Information governance includes availability as well as confidentiality.
    Nested Learning will maintain backup, recovery and continuity arrangements proportionate to the service and risk.
    Important information should not depend on a single fragile copy or an individual person's device where loss would create an unacceptable business, contractual or customer risk.
    Recovery arrangements should be reviewed as systems and institutional deployments develop.
    Backups do not justify indefinite retention of information that should otherwise be deleted. Retention and restoration arrangements should be designed to reconcile resilience with lawful deletion requirements.
28. Confidentiality and secure working
    People working for or on behalf of Nested Learning must protect confidential information encountered through their role.
    They should:
    use approved systems where reasonably available;
    verify recipients before sending sensitive information;
    avoid sharing accounts or credentials;
    protect devices from unauthorised access;

avoid storing restricted information in uncontrolled locations;
use secure methods for sensitive transfers;
lock or close systems when unattended;
report suspected compromise promptly; and
return or delete information when their legitimate need for it ends.
Working remotely does not reduce these responsibilities.

29. Intellectual property and third-party information
    Information governance includes respecting rights in information owned by others.
    Copyright material, customer documents, course materials, rulebooks, research, software and other protected works must be used only where Nested Learning has a lawful basis to do so.
    Access to information is not the same as permission to reproduce, publish, train on, distribute or commercially exploit it.
    Documents supplied by customers for AI Tutor or related services should be processed only for the agreed purpose and according to the applicable contract or licence.
30. Children, safeguarding and sensitive information
    Information concerning children, adults at risk, safeguarding, health or other sensitive matters requires particular care.
    Nested Learning will seek to minimise unnecessary collection and restrict access according to need.
    Where safeguarding information needs to be shared to protect a person, lawful and necessary safeguarding action should not be obstructed by an incorrect assumption that data-protection law prohibits sharing.
    Safeguarding information will also be handled in accordance with the Nested Learning Safeguarding Policy.
31. Training and awareness
    People whose roles involve material access to personal, confidential or restricted information must receive information-governance guidance appropriate to their responsibilities.
    This should include, where relevant:
    confidentiality;
    data protection;
    phishing and account security;
    secure sharing;
    incident reporting;
    data minimisation;
    information classification;
    records management;
    AI and data handling;

safeguarding information; and
responsibilities when leaving or changing roles.
Training and awareness will be proportionate to the size, structure and risks of the organisation.

32. Assurance, monitoring and improvement
    Nested Learning will review information governance as the organisation, technology and customer base develop.
    Assurance may include:
    review of incidents and near misses;
    access reviews;
    supplier review;
    testing of security controls;
    data-protection impact assessments;
    review of processing activities;
    policy review;
    customer due diligence;
    retention review;
    technical testing;
    audit evidence; and
    progress towards appropriate external assurance.
    Nested Learning's Security Statement explains that formal Cyber Essentials, ISO 27001, SOC 2 or equivalent certification is a future assurance objective rather than a current certification claim.
    The absence of a particular certification does not remove the obligation to maintain proportionate security and governance controls.
33. Relationship with customer requirements
    Nested Learning works with organisations whose own information-governance obligations may be extensive.
    Universities, colleges, local authorities, employers and training providers may impose requirements concerning:
    security;
    retention;
    information sharing;
    audit;
    data location;
    access control;
    deletion;
    records management;
    data-subject rights;
    incident reporting;

safeguarding; and
supplier assurance.
Nested Learning will seek to work within those requirements where they are reasonable, agreed and legally necessary.
Where a customer requirement conflicts with law, the law takes precedence.
Where a customer requires a control that is not currently part of Nested Learning's standard service, it should be assessed explicitly rather than assumed to exist.

34. Breaches of this policy
    A breach of this policy may create risk to individuals, customers and Nested Learning.
    Suspected breaches should be reported promptly.
    Depending on the circumstances, a breach may lead to:
    remedial action;
    removal or restriction of access;
    contractual action;
    disciplinary action where applicable;
    customer notification;
    regulatory notification;
    safeguarding action; or
    referral to law-enforcement or another competent authority.
    The response should be proportionate to the seriousness and circumstances of the breach.

35. Review
    This policy will be reviewed at least annually and sooner where there is:
    a material change in data-protection or information law;
    a serious information-security or personal-data incident;
    a significant change to Nested Learning's AI or learning-analytics services;
    a new category of sensitive processing;
    a material change in hosting, suppliers or international transfers;
    a significant customer or regulatory requirement; or
    evidence that existing governance arrangements are no longer adequate.
    The Privacy Policy, Security Statement and supporting operational documentation should be reviewed alongside this policy where changes affect their content.