



PRIVACY NOTICES

FCA Authorised Consumer Credit Lender

Document owner	Chief Compliance and Operations Officer
Approved by	The Board
Version	1.0 — for adoption
Effective date	01 October 2026
Next review	01 October 2027
Classification	External Website — Compliance / Regulatory

Who we are

We are a community interest company limited by guarantee, registered in England under company number 04512225. Registered address: Heatherton Park Studios, Heatherton Park, Bradford-on-Tone, Somerset, TA4 1EU. ICO registration: Z8200608.

Lendology CIC is authorised and regulated by the Financial Conduct Authority under firm reference number 675263 for UK credit regulated activities.

We are the data controller for the purposes of our relationship with you.

Special category and vulnerability information

We use health, disability, accessibility and vulnerability information to adapt our service and support fair customer outcomes. Providing this type of data is normally voluntary. We restrict access and use it only where an Article 6 lawful basis and Article 9 condition apply. You may ask us to correct or remove information, although law or regulation may require us to retain some data; we will make this clear to you, if the circumstances arises.

Automated decision-making

Decision-support systems may assist administration and assessment. We do not currently make decisions producing legal or similarly significant effects solely by automated means. If this changes, we will explain the logic, significance, likely consequences and human review before processing begins.

How we protect information

We use proportionate technical and organisational measures, including:

- role-based access and least-privilege controls;
- multi-factor authentication where technically possible;
- encryption and secure document storage;
- security monitoring and audit logs;
- team member and Board member training;
- information security, records management and data protection policies;
- supplier checks and contractual controls; and
- personal data breach identification, reporting and response procedures.

International transfers and security

Some service providers may process information outside the United Kingdom. Before transferring information internationally, Lendology will identify a lawful transfer route and put appropriate safeguards in place. These may include UK adequacy regulations, the UK International Data Transfer Agreement, the UK Addendum to approved contractual clauses, and a transfer risk assessment where required.

You can ask us for more information about the safeguard that applies to a particular transfer.

Your rights

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

- be informed about how we use your information;
- ask for access to your personal information;
- ask us to correct inaccurate or incomplete information;
- ask us to erase information where the law applies;
- ask us to restrict how we use information;
- receive information you provided in a structured, commonly used and machine-readable format, where data portability applies;

- object to processing based on legitimate interests and to direct marketing;
- withdraw consent at any time where we rely on consent, without affecting earlier lawful processing; and
- ask for applicable safeguards where a significant decision is made solely by automated means.

These rights are qualified and do not apply in every situation. To exercise a right, contact compliance@lendology.org.uk. We may need information to confirm your identity and understand your request. We will respond within the period required by data protection law.

Complaints about your personal information

We take protecting your personal information seriously. If you are unhappy with how we have handled your information, please let us know so we can look into it.

How to make a complaint

You can make a data protection complaint by emailing compliance@lendology.org.uk or calling **01823 461099** and asking to make a GDPR complaint.

If you email us, please include:

- a brief description of your complaint
- your preferred contact method
- your case reference number, if you are an active customer.

For other types of complaints, please see our Complaints Policy [use link]. We can provide a paper copy upon request.

What happens next?

We will acknowledge your complaint in writing within 30 days of receiving it, although we aim to respond sooner. The period starts the day after you make the complaint and includes weekends and bank holidays.

We may ask you to confirm your identity or provide evidence that you are authorised to act for someone else. If we need this, we will let you know when we acknowledge your complaint.

We will take appropriate steps to respond without undue delay, keep you informed and confirm the outcome as soon as practicable after any investigation.

If your complaint involves another organisation, such as a joint controller or third party, we may pass it to them to deal with under their own complaints process.

Where appropriate, we may also involve a partner organisation, council or joint controller in investigating your complaint.

If you remain unhappy

You have the right to complain to the Information Commissioner's Office (ICO):

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire

SK9 5AF

Telephone: 0303 123 1113

Website: [Information Commissioner's Office \(gov.uk\)](https://www.informationcommissioner.gov.uk)

CUSTOMER SECTIONS

At a glance

- We use information to assess enquiries and applications, administer loans, provide support, prevent fraud, meet legal and regulatory duties and improve services.
- We work with councils and public sector partners that fund or support loan schemes.
- We may use health or vulnerability information to understand and meet your support needs.

Purpose and scope

This notice applies to customers, applicants, borrowers, former borrowers, guarantors, representatives and other people connected with a loan. It explains what information Lendology CIC uses, why, who receives it, how long it is kept and your rights.

Information we collect

Category	Examples
Identity and contact	Name, date of birth, address, email, telephone, National Insurance number, signatures and identity documents.
Financial	Income, expenditure, employment, bank details, savings, debts, borrowing, repayments and credit information.
Property	Ownership, title, Land Registry information, valuations, energy efficiency and home improvements.
Household and relationships	Dependants, household composition, relationship status, attorneys, executors and representatives.
Communications	Letters, emails, calls and recordings, webchat, messages, complaints and feedback.
Special category and vulnerability	Health, disability, accessibility, communication needs and circumstances affecting support.
Fraud, legal and regulatory	Identity, fraud, sanctions, financial-crime, court, complaint and regulatory information.

Where information comes from

Most information comes from you. We may also receive it from councils and public sector partners, authorised representatives, mortgage lenders, credit and fraud-prevention agencies, professional advisers, executors and attorneys. Public sources may include HM Land Registry, Companies House, the Probate Registry, The Gazette and property databases.

Purposes and lawful bases

Purpose	Lawful basis
---------	--------------

Respond to enquiries and assess applications	Steps requested before contract; legitimate interests where not contractual.
Enter into, administer and manage a loan	Contract and legal obligation.
Assess affordability, eligibility and risk	Pre-contract steps, contract, legal obligation and legitimate interests in responsible lending.
Manage repayments, arrears and recovery	Contract, legal obligation and legitimate interests in fair account management and recovery.
Meet FCA, Consumer Duty, anti-money laundering, fraud, tax, accounting, complaints and court duties	Legal obligation; recognised legitimate interests only where statutory conditions apply.
Deliver council-funded schemes	Contract, legal obligation, legitimate interests and public task where supported by law.
Meet accessibility or vulnerability needs	Legal obligation and an applicable Article 9 condition, or explicit consent where appropriate.
Improve service, quality and customer outcomes	Legitimate interests.
Marketing and optional referrals	Consent where required.
Legal claims	Legitimate interests and legal claims condition for special category information.

Councils and scheme partners

We may share application, property, loan, repayment, fraud, complaint, audit and safeguarding information with the relevant council or public sector partner where necessary. Depending on the scheme, the parties may be independent controllers, joint controllers, or controller and processor.

Who we share information with

We share only what is necessary as follows:.

Recipient	Purpose
Your council or public sector scheme partner	Eligibility, funding, administration, assurance, audit, complaints, safeguarding and reporting.
Authorised credit or fraud agencies	Creditworthiness, identity, fraud prevention and responsible lending checks where applicable.
Technology Providers	Email, collaboration and document management.
Loan Management System	Customer and Case Management where used.
Communication Systems	Chat, telephony, messaging and accessible communications.
Document and Postal Services	Electronic signature, document delivery and correspondence.
Address Searches	Address checking and verification.
Feedback Platforms	Reviews, feedback and authorised marketing.
Formal Partners	Property or energy-related services where relevant.
Advisers	Accounting, audit, legal and professional advice.
Government Bodies	Verification, statutory functions, regulation, compliance and legal claims.
Other approved processors	Secure technology, hosting, security, customer support and operations.

Some recipients act as processors under our instructions. Others, including councils, regulators, credit reference agencies and professional advisers, may be independent or joint controllers.

Special category and vulnerability information

We use health, disability, accessibility and vulnerability information to adapt our service and support fair customer outcomes. Providing it is normally voluntary. We restrict access and use it only where an Article 6 lawful basis and Article 9 condition apply. You may ask us to correct or remove information, although law or regulation may require some retention.

Retention

Withdrawn or declined applications are anonymised two years after closure and completed and repaid loans anonymised seven years after repayment. Other records may have different periods because of law, regulation, tax, accounting, complaints, fraud, audit, insurance or legal claims.

Recruitment Privacy Notice

At a glance

- We use candidate information to manage applications, assess suitability, arrange interviews and complete appropriate pre-employment or regulatory checks.
- We do not make recruitment decisions solely by automated means.

Purpose

This notice explains how Lendology CIC collects, uses, shares, stores and protects personal information during recruitment. It also explains your rights and how to exercise them.

Scope

This notice applies to candidates for team member, worker, contractor, volunteer, apprenticeship and Board roles, and to referees and other people whose information is provided during recruitment. Successful candidates are covered by the Team Member and Board Member Privacy Notice from the point their working relationship or appointment begins.

Information we collect

Category	Examples
Identity and contact	Name, address, email, telephone number, date of birth where required and preferred contact method.
Application and professional	CV, application form, employment history, education, qualifications, skills, experience, professional memberships and salary expectations.
Assessment	Shortlisting records, interview notes, scores, test or exercise results and selection-panel feedback.
Eligibility and verification	Right-to-work evidence, identity documents, references and information needed to verify qualifications or professional history.
Role and availability	Role applied for, preferred location, availability, notice period and working arrangements.

Special category	Health, disability and reasonable-adjustment information; equality, diversity and inclusion monitoring information where collected.
Criminal offence and regulatory	DBS information and fitness, propriety, conduct or regulatory information where lawful and relevant to the role.
Communications	Emails, letters, telephone or video-call details and correspondence about the application.

Where information comes from

We collect most information directly from you. We may also receive information from recruitment platforms or agencies, referees, former employers, professional bodies, the Disclosure and Barring Service, regulators and public registers where lawful and relevant. We will tell you if a particular check requires additional information or consent.

Purposes and lawful bases

Purpose	Typical information	Lawful basis
Receive and manage an application	Name, contact details, CV, application form, employment history, qualifications, skills, experience and correspondence relating to the application	Taking steps at your request before entering into a contract. We may also rely on our legitimate interests in administering recruitment applications fairly and efficiently.
Shortlist, interview, assess and select candidates	CV information, application forms, interview notes, assessment results, references and selection panel feedback	Taking steps at your request before entering into a contract and Lendology's legitimate interests in selecting suitable candidates fairly and consistently.
Communicate about the application and request feedback	Contact details, application status, interview arrangements, correspondence and feedback responses	Taking steps at your request before entering into a contract and Lendology's legitimate interests in administering and improving recruitment processes.
Verify identity, qualifications, employment history and references	Identity documents, qualifications, professional memberships, employment history, references and right-to-work evidence	Taking steps at your request before entering into a contract, compliance with legal obligations where applicable, and Lendology's legitimate interests in ensuring information is accurate and recruitment decisions are based on reliable information.
Confirm right to work and meet employment law obligations	Identity information, passport or immigration documents, right-to-work records and related correspondence	Compliance with legal obligations.
Make reasonable adjustments and meet equality duties	Health information, disability information, accessibility requirements, equality monitoring information and adjustment requests	Compliance with legal obligations. Where special category information is involved, we apply an additional condition under data protection law.
Conduct DBS, fitness and propriety or regulatory checks for relevant roles	DBS information, criminal offence information, references, conduct information, qualifications, employment history and regulatory information	Compliance with legal obligations where a legal or regulatory requirement applies, or Lendology's legitimate interests where checks are necessary and proportionate for the role. Where criminal offence information is processed, an additional condition under the Data Protection Act 2018 applies.

Establish, exercise or defend legal claims	Application records, correspondence, interview notes, references, investigation records and other information relevant to a complaint, dispute or legal matter	Lendology's legitimate interests in establishing, exercising or defending legal claims. Where special category information is involved, an additional condition under data protection law applies.
Keep details for future vacancies	Contact details, CV information, application history and stated preferences	Consent, where this is optional, separate from the current application and can be withdrawn at any time.

Who we share information with

We share information only where necessary for recruitment or a legal or regulatory requirement. The following entries reflect current internal records and must be validated against the live supplier register before approval.

Recipient	Purpose
Technology Providers	Email, application receipt, collaboration and storage of authorised recruitment records.
Payroll, pension, insurance and benefit providers	HR administration and storage of successful-candidate records where used.
Recruitment Platforms	Advertising, receiving or managing applications where the role is advertised through that service.
Recruitment agencies	Candidate introduction and recruitment support where used.
Referees and former employers	Reference and employment-history checks.
Disclosure and Barring Service or approved checking provider	Criminal-record checks for eligible roles.
Professional bodies and regulators, including the FCA where relevant	Qualification, approval, certification, fitness and propriety or regulatory checks.
HR/legal advisers	Employment and recruitment advice where necessary.
IT and security providers	Secure operation and protection of recruitment systems.

We do not share candidate information with councils, credit reference agencies or customer-service suppliers unless a specific, evidenced recruitment or regulatory purpose applies. We do not use candidate information for third-party marketing.

Retention

Record	Current internal period
Applications that do not progress to interview	One year.
Interview records, application notes and forms for unsuccessful candidates	One year.
Successful candidate records	Transferred to the team member record and retained under the Team Member and Board Member Privacy Notice.
Future vacancy or talent-pool information	Only for the period stated when separate consent is requested.
DBS and regulatory-check information	Indefinitely

Retention may be extended where required for an active complaint, investigation, regulatory matter or legal claim, and the reason must be recorded.

Team Member Privacy Notice

At a glance

- We use personal information to manage working relationships, Board appointments, pay and benefits, governance, regulatory duties, security and organisational improvement.
- We collect only the information we need and restrict access to people with a legitimate business need.
- We use different lawful bases for different purposes. We do not rely on consent where you have no genuine choice.
- We do not use solely automated decision-making to make decisions about team members or Board members.

Purpose

This notice explains how Lendology CIC collects, uses, shares, stores and protects personal information about team members and Board members. It also explains your data protection rights and how to exercise them.

This notice is not part of any contract of employment, service agreement or letter of appointment. We may update it when our processing, legal duties or working practices change. We will make material changes clear.

Scope

This notice applies to current and former team members, workers, secondees, volunteers, Board members, committee members and office holders. Recruitment candidates are covered by the Recruitment Privacy Notice until they join Lendology.

Some processing differs between team members and Board members. Where this happens, the relevant section says so.

The information we use

We may collect and use the following categories of personal information, where relevant to your role or appointment:

Category	Examples
Identity and contact	Name, address, personal and work contact details, date of birth, photograph, signature, National Insurance number, emergency contact and next-of-kin details.
Working relationship or appointment	Role, job title, employment or appointment history, qualifications, references, right-to-work evidence, contracts, terms, working arrangements, start and leaving dates.
Pay, benefits and finance	Salary or fees, bank details, payroll, tax, pension, expenses, benefits and deductions.
Attendance and availability	Working hours, work location, annual leave, family-related leave, sickness absence, other absence and flexible-working information.
Performance, development and conduct	Objectives, appraisals, one-to-ones, supervision, training, skills, competency, recognition, capability, disciplinary, grievance and whistleblowing records.
Health, safety and wellbeing	Accident and incident records, risk assessments, occupational health information, workplace support and reasonable adjustments.
Governance and regulatory	Board and committee papers, minutes, attendance, decisions, voting, declarations of interest, fit-and-proper

	assessments, Senior Managers and Certification Regime records, regulatory approvals and statutory records.
Systems, communications and security	Username, permissions, device and system records, audit logs, security events, business communications, building access and records created through Lendology systems.
Equality information	Information used, where lawful, to support equality monitoring and prevent discrimination.
Special category information	Information given extra protection by law, such as health, disability, racial or ethnic origin, religious or philosophical beliefs, trade union membership or sexual orientation.
Criminal offence information	Disclosure and Barring Service information and other criminal offence information where checks are lawful, necessary and relevant to the role.

Where we get information from

We collect most information directly from you. We may also receive information from:

- recruitment agencies, referees and former employers;
- HM Revenue & Customs, pension and benefit providers;
- occupational health providers, healthcare professionals and insurers, where lawful;
- the Disclosure and Barring Service and other background-check providers, where lawful;
- professional bodies, regulators, public registers and Companies House;
- line managers, other team members, Board members, customers, suppliers or advisers where information is relevant to a legitimate workplace or governance matter; and
- Lendology systems, devices, access controls, communications and business records.

Why we use information and our lawful bases

Data protection law requires us to have a lawful basis for each use of personal information. The basis depends on the purpose and the information involved.

Purpose	Typical information	Lawful basis
Set up and manage the working relationship or appointment	Identity, contact, contract, role, working arrangements and Board appointment records	Necessary to enter into or perform a contract, including a service or appointment agreement, where applicable. Legitimate interests may apply to non-contractual governance administration.
Pay salary, fees, expenses, tax, pension and benefits	Identity, bank, payroll, tax, pension and expenses	Contract and legal obligation.
Manage duties, hours, leave, attendance and organisational resources	Working, attendance, location and availability information	Contract, legal obligation and legitimate interests in effective resourcing and continuity.
Support performance, development, training and succession	Objectives, appraisals, one-to-ones, training and competency records	Contract, legal obligation where regulated competence applies, and legitimate interests in developing people and maintaining effective services.
Meet employment, company, tax, equality, health and safety, safeguarding, data protection and regulatory duties	Relevant identity, HR, governance, health and regulatory records	Legal obligation. Where appropriate, performance of a task in the public interest may apply only if supported by law.
Administer Board and committee governance	Appointment, attendance, papers, minutes, decisions, voting, declarations and statutory records	Legal obligation and legitimate interests in effective governance and accountability.

Assess fitness, propriety and regulatory suitability	Qualifications, employment history, references, financial soundness, conduct, conflicts and DBS information where relevant	Legal obligation and legitimate interests in regulatory compliance and risk management.
Protect people, premises, systems, information and assets	Access, device, audit, security and communications records	Legitimate interests in security, fraud prevention, continuity and protecting confidential information; legal obligation where applicable.
Investigate complaints, grievances, disciplinary matters, conflicts, fraud, misconduct or security incidents	Relevant communications, witness information, system records and case records	Legal obligation, contract and legitimate interests in fair investigation, risk management and legal claims.
Communicate optional photographs, biographies or testimonials	Photographs, biography and stated preferences	Consent where participation is genuinely optional. Consent can be withdrawn.
Establish, exercise or defend legal claims	Relevant records connected with the claim	Legitimate interests and, for special category information, the legal claims condition.

Regulatory checks and Board records

Lendology may carry out and record checks needed for regulated roles and Board appointments. These may include identity, qualification, employment history, references, conflicts of interest, financial soundness, competence, conduct and criminal-record checks. The exact checks depend on the role and applicable legal or regulatory requirements.

Certain Board member and office-holder details may be placed on statutory registers, filed with Companies House, supplied to the Financial Conduct Authority or otherwise made public where required by law.

Systems, communications and monitoring

Lendology processes information generated through its equipment, accounts, systems and premises for access management, information security, fraud prevention, regulatory compliance, business continuity, service quality and investigation of suspected misuse.

Any monitoring must be lawful, necessary and proportionate. Lendology does not install management software on personal devices or access personal information on them.

Who we share information with

We share information only where it is necessary, proportionate and lawful. Recipients may include:

Recipient	Why information may be shared
Payroll, pension, insurance and benefit providers	To administer pay, tax, pensions, insurance and benefits.
Technology, communications and HR providers	To provide email, collaboration, document management, HR, payroll, security, telephony, electronic signature and other business systems.
Professional advisers	Legal, accounting, audit, banking, insurance, occupational health, HR and consultancy support.
Regulators and public authorities	HMRC, Companies House, the Financial Conduct Authority, the Information Commissioner's Office, pension authorities, law enforcement, courts and tribunals where applicable.
Board, committee and governance stakeholders	For lawful oversight, decision-making, declarations, statutory records and reporting.
Councils and public sector partners	For contract management, assurance, audit, safeguarding, funding or regulatory purposes where relevant.
Other recipients	Where necessary for a legal claim, investigation, corporate transaction or another lawful business purpose.

Where a provider acts as our processor, it must use information only on our instructions and under appropriate confidentiality and security terms. Some recipients, such as regulators or pension providers, may act as independent controllers for their own purposes.

How long we keep information

We keep identifiable information only as long as needed for the purpose, legal or regulatory duties, audit, complaints, insurance, limitation periods, investigations and legal claims. The following periods are taken from current internal records and must be checked against the approved retention schedule before adoption.

Record category	Current internal retention position
Core team member record, including disciplinary, holiday, sickness, absence, working time, training, DBS information, redundancy and right-to-work evidence	Six years after employment ends.
Payroll records, including income tax, National Insurance returns and correspondence with HMRC	Six years.
Workplace accident records	Three years from the last entry for minor accidents. Different periods may apply to serious accidents or records involving younger people; consult the approved retention schedule.
Parental leave records	Five years from birth or adoption, with a longer period recorded internally where the child receives a disability allowance.
Maternity and paternity leave records	Three years after the end of the tax year in which the leave ends.
Retirement benefit scheme records	Six years from the end of the scheme year in which the event occurred.
Board and committee records, declarations, statutory records and FCA records	Indefinitely
Security, access, call, communications and system logs	Indefinitely

When information is no longer required, we securely delete, destroy or anonymise it. We may keep information longer where required by law, litigation, regulatory action, an active complaint or investigation. Any exception must be documented and approved by the record owner and Governance.