ACESO PATHWAY LIMITED

PRIVACY POLICY

1. Who we are

Aceso Pathway Limited ("Aceso", "we", "us" or "our") is a company registered in England and Wales.

Registered office: Chapel House, Leicester Road, Loughborough, England, LE11 2AF
Company number: 16251254
Telephone: +44 (0)1509 972221
Email: contact@acesopathway.co.uk
Website: https://acesopathway.co.uk
CQC registration number: 1-25880912014

Aceso Pathway Limited is the data controller for the processing described in this Privacy Policy where Aceso determines why and how personal information is used.

In some circumstances, another organisation may be the data controller, or Aceso may process personal information on behalf of another organisation as a data processor.

For privacy enquiries, complaints or requests to exercise your rights, contact Jamie Mackenzie, Data-protection lead, using the address, email or telephone number above.

2. What this Privacy Policy covers

This Privacy Policy explains how we collect, use, disclose, store and protect personal information when you:

- visit or use our website;
- contact us or make an enquiry about PTSD, trauma or related mental-health treatment;
- undergo an assessment or receive treatment, therapy, clinical support, follow-up or aftercare;
- communicate with our clinicians, administrators or other team members;
- provide information about an emergency contact, next of kin or person involved in your care; or
- otherwise interact with Aceso in connection with our services.

This Privacy Policy applies to information about patients, prospective patients and other individuals whose personal information we process in connection with our services.

What we mean by "processing"

"Processing" personal information means doing anything with personal information. This can include collecting, recording, organising, storing, reviewing, using, amending, transferring, sharing, restricting, deleting or otherwise handling information.

We aim to collect only information that is adequate, relevant and necessary for the purpose for which it is used.

Where certain information is necessary to assess, provide or safely manage your treatment, we may be unable to provide the relevant service if you do not provide that information.

This does not mean that every piece of information we request is mandatory. Where appropriate, we will explain whether information is necessary for your care or whether providing it is optional.

Aceso currently provides clinical assessment and treatment services only to adults aged 18 or over. Relevant information about relatives, representatives, emergency contacts and other people may also appear in our records.

3. Information we collect

Initial enquiries: our website contact form asks for your name and email address and offers an optional telephone field and a free-text message box. Submissions are emailed to contact@acesopathway.co.uk in Google Workspace. We do not ask for symptoms or trauma history at this stage and ask you not to include medical or trauma details. If you choose to include them, they may nevertheless appear in the enquiry record.

We enter basic contact information in Cliniko to administer your enquiry and any assessment. Clinical health information is first collected during an assessment with a psychiatrist or psychologist.

For assessment, treatment and follow-up, we collect information necessary for safe care. This may include identity and contact details, date of birth, relevant emergency contacts, physical and mental health, PTSD and trauma history, symptoms, diagnoses, medication and allergy information, clinical assessments, treatment plans, progress notes, consent records, risks, safeguarding information, appointment records and relevant correspondence.

Clinical records are held in Cliniko. Clinicians enter their notes directly there. We do not make audio or video recordings of clinical assessment or therapy sessions. We use Cliniko's integrated Telehealth service for online appointments. Cliniko describes this service as using encrypted peer-to-peer communications without retaining session recordings. Technical connection and access information may be processed to operate, secure and troubleshoot the service.

We use KashFlow for invoices and accounting. Invoices are emailed directly from KashFlow, and payments are made by bank transfer to Lloyds Bank. KashFlow and invoices contain administrative and payment information, not clinical health information.

We also process information in complaints, rights requests and service correspondence, and technical or security information needed to operate our website and systems.

Where necessary and relevant to care or safeguarding, clinical records may include other special-category information, such as racial or ethnic origin, religion, sexual life or sexual orientation. Records may contain allegations or offence information about identifiable offenders or suspected offenders. Victim or witness information alone is not criminal-offence data unless it also identifies an offender or suspected offender.

4. Health and special category information

Information about your health, including mental health, PTSD and trauma-related information, is special category personal data under UK data-protection law and receives additional protection.

We process health information only where both:

1. an Article 6 lawful basis under the UK GDPR; and

2. an applicable Article 9 condition for processing special category data are satisfied.

For the provision and management of health or social-care treatment, the relevant special-category condition will ordinarily be Article 9(2)(h) where its statutory requirements are satisfied, including professional-secrecy safeguards under Article 9(3) and applicable UK law.

Where applicable, other conditions may include explicit consent, legal claims, vital interests where the individual is physically or legally incapable of giving consent, or a relevant substantial-public-interest condition. We assess the condition for the specific activity.

Where required, we also comply with the additional conditions and safeguards in the Data Protection Act 2018.

We do not use consent as a substitute for another lawful basis simply because information is sensitive.

Where an appropriate policy document is required under the Data Protection Act 2018, Aceso will maintain the appropriate documentation, including relevant retention and deletion arrangements.

Criminal-offence information requires an Article 6 lawful basis and compliance with Article 10, including an applicable authorisation or condition under UK law. An Article 9 condition alone does not authorise processing criminal-offence information.

5. Why we use your information

We use information to respond to enquiries; assess suitability and clinical needs; provide assessment, treatment and follow-up; maintain clinical records; arrange appointments and send service communications; invoice and reconcile payments; manage clinical safety and safeguarding; handle complaints and rights requests; protect our systems; meet applicable record-keeping and regulatory duties; and establish, exercise or defend legal claims.

Clinical monitoring is through clinician-led contacts and appointments. We do not use patient apps, wearables or automated tracking to monitor patients.

We use clinical information for appropriate quality and patient-safety oversight. The Medical Director and Research Director are clinicians with full clinical-record access for their responsibilities.

Research-data preparation has not yet commenced. We plan to use anonymised data only for research and outcome analysis. The Research Director will remove identifying patient data before conversion to a CSV file; the CSV will contain no patient number, code or identifier linking it back to Cliniko. Source-data preparation remains processing of personal information. Before starting, we will document checks against indirect identification and handling of any temporary identifiable copies. Removing direct identifiers alone does not establish effective anonymisation. Healthcare quality evaluation is distinguished from scientific research.

We do not currently use AI tools with patient information. Any materially different use requires assessment of its lawful basis, confidentiality and safeguards and appropriate updated privacy information.

6. Lawful bases for processing

We use the following lawful bases for the purposes described. Contract applies only where processing is necessary to provide contracted services or take steps you request before entering a contract. Legal obligation applies only where an identified law requires the processing.

When we rely on legitimate interests, our interests include responding to enquiries, administering safe services, maintaining security and quality, and protecting legal interests. We assess necessity and balance those interests against your rights and freedoms.

Health and other special-category information requires both an Article 6 basis and an Article 9 condition. Healthcare uses Article 9(2)(h), with Article 9(3) professional-secrecy safeguards and the applicable UK healthcare condition. Other conditions below are used only where their statutory requirements are met.

Consent to treatment and permission to disclose confidential information are separate from consent as a GDPR lawful basis. A patient request to inform a GP or referring organisation is recorded with the permitted recipients and scope; it is not automatically treated as GDPR consent for every aspect of care.

Criminal-offence information additionally requires Article 10 authorisation under UK law. Where a substantial-public-interest, safeguarding or research condition is used, we apply its specific statutory conditions and any required policy document or safeguards.

Purpose	Article 6 basis	Sensitive-data condition where relevant
Initial enquiry responses and basic contact administration	6(1)(f): legitimate interests in answering enquiries and administering services. 6(1)(b) for assessment-booking steps you request towards a contract.	9(2)(h) only where necessary healthcare processing arises; unsolicited health detail is minimised and handled confidentially.
Clinical assessment, treatment, follow-up and necessary appointment communications	6(1)(b): necessary performance of the patient contract or requested pre-contract assessment steps.	9(2)(h): provision/management of healthcare; DPA 2018 Schedule 1 paragraph 2 and secrecy safeguards.
Clinical records required for regulated care	6(1)(c): applicable duties under the Health and Social Care Act 2008 (Regulated Activities) Regulations 2014, including Regulation 17, where applicable.	9(2)(h): necessary healthcare management with UK healthcare condition and secrecy safeguards.
Clinical quality and patient-safety oversight	6(1)(c) for applicable regulated-service governance duties; 6(1)(f) for distinct necessary quality improvement beyond those duties.	9(2)(h): necessary healthcare management. Scientific research is assessed separately.
Invoices, payments and statutory accounts	6(1)(b) for billing/payment administration; 6(1)(c) for applicable company/accounting/tax record duties.	No clinical health information included in KashFlow or invoices; reassess if data used changes.
Patient-requested GP/referrer confirmation letters	6(1)(b) where necessary as part of contracted care; 6(1)(f) for an optional requested	9(2)(h) where necessary for healthcare; separate disclosure authority and scope recorded.

	confirmation outside contractual necessity.	
Rights requests and data-protection complaints	6(1)(c): applicable statutory duties under UK data-protection law.	Condition follows sensitive information necessary for handling the request; 9(2)(h) for healthcare-record management or 9(2)(f) where legal claims require it.
Safeguarding or emergency disclosure	6(1)(c) where a specific legal duty requires it; 6(1)(d) where necessary to protect life; otherwise 6(1)(f) for necessary protection against serious harm, subject to assessment.	9(2)(h) where part of care; 9(2)(g) with applicable UK safeguarding condition where its tests are met; 9(2)(c) only where person is physically or legally incapable of consent.
Security, website operation and clinical complaints outside specific legal duties	6(1)(f): protecting services and resolving concerns; 6(1)(c) for distinct statutory security/complaint duties.	9(2)(h) for necessary healthcare management if clinical information used; otherwise identify condition for the specific sensitive use.
Legal claims	6(1)(f): establishing, exercising or defending legal claims; 6(1)(c) for specific required disclosures.	9(2)(f) where necessary for claims; separate Article 10 authorisation if offence data involved.
Preparing anonymised data for scientific research	6(1)(f): research into treatment and outcomes, subject to necessity, balancing and compatibility assessment.	9(2)(j), DPA Schedule 1 paragraph 4 and applicable research safeguards for necessary source processing; confidentiality requirements also apply. Research outputs must be genuinely anonymised.

7. Confidentiality

We understand that information concerning PTSD, trauma, mental health and personal experiences is particularly private.

We treat clinical and personal information confidentially and expect our staff, clinicians and relevant contractors to comply with applicable confidentiality duties, professional standards and information-governance procedures.

We will normally only disclose confidential information where:

- you have authorised the disclosure;
- disclosure is necessary and lawful for your care or service;
- disclosure is required or permitted by law; or
- another lawful justification for disclosure applies, including the applicable confidentiality requirements.

Confidentiality is not absolute.

We may share information without your consent where necessary and lawful to:

- protect vital interests;
- protect you or another person from serious harm;
- meet a safeguarding duty;
- comply with a legal obligation;
- respond to a court or lawful authority; or
- establish, exercise or defend legal claims.

Where information is shared, we will seek to ensure that the information disclosed is relevant and proportionate to the purpose for which it is being shared.

We also take account of the common law duty of confidentiality when deciding whether confidential patient information may be used or disclosed. A data-protection lawful basis alone does not remove that duty.

8. Safeguarding and serious risk

Because we provide PTSD and trauma-related treatment, we may receive information concerning suicide or self-harm, abuse, sexual or domestic violence, neglect, exploitation, safeguarding concerns or risks of serious harm to you or another person.

Where we reasonably believe that disclosure is necessary and lawful to protect you or another person from serious harm, or to meet a safeguarding or legal duty, we may share relevant information with appropriate professionals or authorities.

We will seek to respect your wishes and confidentiality wherever possible.

However, your consent may not always be required where the law permits or requires disclosure.

We will seek to share only information that is relevant and proportionate to the purpose.

9. Access and sharing

Ordinary treating clinicians can access only their assigned patients in Cliniko. The Medical Director (a GP) and Research Director (a clinician) have full clinical-record access for their oversight responsibilities. Administrators and Accounts staff cannot view clinical information. Administrative staff may delete records on instruction under Medical Director oversight; deletion authority does not itself grant clinical-content access.

We do not routinely send updates to your NHS GP or referring organisation. If you request they be informed, we send a confirmation letter from within Cliniko and keep a copy in your clinical record. We record your request and the intended recipients and scope.

We may make necessary and lawful disclosures for safeguarding, serious emergencies, legal claims, regulatory requirements or other lawful obligations as explained in Sections 7 and 8. These exceptional disclosures are separate from routine patient-requested updates.

Our service providers handle relevant information to operate the service: Cliniko (provided by Red Guava Pty Ltd) for clinical records and communications; Google Workspace for enquiry emails; KashFlow for invoices/accounts; Lloyds Bank for bank transfers; and GoDaddy for website building, hosting and contact-form processing. Providers may use subprocessors. The website also uses Google reCAPTCHA anti-spam technology; further details of deployed technologies are provided through website privacy/cookie information.

We limit information supplied to providers to what the service requires. KashFlow access is restricted to Accounts and the Operations Director. We do not sell personal information.

Clinical professionals' data-protection roles depend on actual decision-making and contractual arrangements. A professional may act on our behalf or as a separate or joint controller. Separate controllers have their own responsibilities and privacy information; we provide required information about any joint arrangement.

10. Information from other sources

Most clinical information is obtained during your assessment and care. We also receive entries and information from clinicians involved in your Aceso care and correspondence relevant to your enquiry, treatment or request.

Where necessary and lawful, relevant information may come from your authorised representative, referring professional or organisation, NHS GP, safeguarding body or public authority. We explain additional sources and categories where required, and provide privacy information unless an applicable exemption applies.

Clinical and safeguarding records may include information about relatives, children, witnesses or alleged perpetrators where necessary for your care or safeguarding. We handle it proportionately and assess any transparency exemption and confidentiality requirements rather than assuming we should contact those individuals.

11. Service communication and marketing

We do not currently send marketing communications or newsletters. We send communications needed for enquiries, appointments, treatment, safety, billing and other service administration. Appointment reminders are emailed from within Cliniko.

If we introduce direct marketing, we will assess the relevant privacy and electronic-marketing rules, provide appropriate privacy information and honour applicable consent and objection rights before starting. Holding health information does not give us permission to use it for marketing.

12. Website and similar technologies

Our website is built and hosted using GoDaddy and includes a contact form. Name and email address are required; telephone number is optional. A free-text message box is provided. Submissions are sent to our Google Workspace contact mailbox. GoDaddy also retains enquiry copies in its Conversations inbox. Access to Aceso's GoDaddy account and inbox is restricted to Jamie Mackenzie.

Our website includes a Google Analytics tag for website traffic analysis. A live inspection on 6 October 2026 found the tag before a consent choice and after selecting Decline; this alone does not establish whether analytics data is transmitted or analytics cookies are set in either state. The contact form also uses an invisible Google reCAPTCHA integration for spam and abuse prevention, which was present after Decline. These services may process technical information or use cookies or similar technologies. Exact cookie lifetimes and consent behaviour remain to be verified before publication.

Our cookie banner provides Accept and Decline choices. We describe the deployed technologies and applicable choices in our cookie information. Where consent is required, it must be obtained before the relevant technology is used; any applicable exception must meet its conditions. The current website cookie policy requires correction: it refers to Weebly although the website is built and hosted on GoDaddy. Google's current reCAPTCHA documentation describes processing under its Cloud terms and Data Processing Addendum from 2 April 2026; the older Google privacy/terms wording

displayed on the form requires review. These implementation and disclosure checks remain outstanding.

13. International processing and transfers

Our clinicians and team members do not access patient information from outside the UK. Cliniko has confirmed to us that our clinical data is hosted on UK servers. This does not mean every provider, support activity or subprocessor operates exclusively in the UK.

Cliniko is provided by Red Guava Pty Ltd in Australia. Its UK Data Processing Addendum contains EU standard contractual clauses with the UK International Data Transfer Addendum for relevant transfers. Google Workspace, KashFlow, website and communication providers may also involve overseas processing or access depending on the service and configuration. GoDaddy's published notices state that its US operating company and listed affiliates participate in the UK Extension to the EU–US Data Privacy Framework for covered transfers to the United States. Where that framework is unavailable, its terms provide for applicable contractual safeguards and supplementary measures. Further information is available in GoDaddy's Data Privacy Framework Notice and European Supplemental Privacy Notice at https://www.godaddy.com/en-uk/legal/agreements/data-privacy-framework-notice and https://www.godaddy.com/en-uk/legal/agreements/european-supplemental-privacy-notice.

Where a restricted transfer occurs, we use an applicable UK adequacy arrangement or appropriate safeguards, such as the UK International Data Transfer Agreement or UK Addendum to EU standard contractual clauses. We carry out the required data protection test and apply additional safeguards where necessary.

Contact our data-protection lead for information about relevant destinations, applicable safeguards and how to obtain a copy, subject to necessary redactions. We provide the specific transfer information required for the processing concerned.

14. Security

We use measures appropriate to the information and risks, including role-based access and written confidentiality obligations. Users have individual logins; there are no shared logins. Cliniko and Google Workspace use two-factor authentication. We do not claim every system uses two-factor authentication.

The Operations Director removes a team member's or clinician's system access immediately when their work with Aceso ends. We maintain written procedures for data breaches, record requests and data-protection complaints, coordinated by our data-protection lead.

We review access, retention, supplier safeguards and security arrangements and use appropriate backup/recovery and secure-disposal measures. Where a personal-data breach requires regulatory or individual notification, we notify the relevant authority and affected people as required by law.

15. How long we keep information

We keep personal information only for as long as necessary for the purpose for which it is processed and in accordance with our documented retention schedule.

Different types of information are subject to different retention periods.

Our retention periods take account of applicable legal and regulatory requirements, professional guidance, the nature of the information, the purpose for which it is held and the need to protect Aceso and individuals against potential legal claims.

15.1 Clinical and treatment records

Adult patients

Adult clinical and treatment records relating to mental-health and PTSD treatment will normally be retained for 20 years from the date of the last entry or contact, as Aceso's adopted healthcare records-management benchmark, taking account of continuity and safety of care, the nature of the information, regulatory requirements and legal claims. This is not a universal statutory retention period for private providers.

This includes relevant clinical assessments, treatment plans, progress notes, risk assessments, correspondence, referrals, reports, consent records, appointment records and other information forming part of the clinical record.

Deceased patients

Where a patient has died, relevant mental-health records will normally be retained for 10 years after the date of death.

Longer retention

Records may be retained for longer where:

- the patient's care or treatment is ongoing;
- a legal claim has been made or is reasonably foreseeable;
- a safeguarding matter remains active;
- there is an ongoing investigation;
- the records are required for an inquiry, inquest or regulatory process;
- another legal or regulatory requirement applies; or
- professional or clinical judgment supports longer retention.

Aceso's approved clinical-record retention schedule uses 20 years from the last clinical entry/contact, or ten years after the patient's death, for adult mental-health records including psychology records. Disposal remains subject to review and any applicable longer legal hold or active investigation.

15.2 Administrative and clinical correspondence

Administrative information that forms part of, or is necessary to understand, a patient's clinical care may be retained for the same period as the relevant clinical record.

Clinical correspondence, referrals, reports and communications relevant to treatment will normally form part of the clinical record and will be retained accordingly.

General business and contractual records may normally be retained for up to six years where necessary for contractual, legal, regulatory or legitimate business purposes. Routine correspondence that is no longer required is deleted earlier where appropriate.

15.3 Financial and accounting records

Invoices and accounting records in KashFlow are retained for six years from the end of the relevant financial year, subject to any applicable longer legal requirement or documented hold. The Accounts Department is responsible for expiry disposal.

15.4 Complaints

Records concerning complaints about clinical care will normally be retained with the relevant clinical record.

Complaint records that are not part of the clinical record are retained for six years from closure of the complaint, subject to any longer legal hold or active investigation.

Where a complaint is connected with a legal claim, regulatory investigation, safeguarding matter or other formal process, the relevant information may be retained for longer.

15.5 Safeguarding and serious incidents

Safeguarding information and records relating to clinical or serious incidents will normally be retained with the relevant clinical record where they form part of or relate directly to patient care.

Where a safeguarding matter, investigation, claim, inquiry or other formal process remains active, records will not be destroyed until the matter has been appropriately concluded and disposal is lawful and appropriate.

15.6 Marketing information

We do not currently undertake marketing communications. If introduced, their retention and any necessary suppression records will be assessed and explained before use.

15.7 Website and technical information

Jamie Mackenzie deletes enquiry copies from the GoDaddy Conversations inbox on a cycle every 30 days. This is separate from the six-month period from last contact for unassessed enquiry emails in Google Workspace. The inbox deletion cycle does not establish GoDaddy's technical-log or backup retention periods, which remain to be verified. Other website, technical, security and message-delivery information is retained for the necessary operational, security or legal purpose.

Retention periods will be documented and will be consistent with our Cookie Policy and the actual technologies and suppliers used by Aceso.

15.8 Legal claims and investigations

Where information is reasonably required for the establishment, exercise or defence of legal claims, or is subject to an investigation, court proceedings, regulatory process, public inquiry, inquest, access request or other lawful requirement, we may retain it for longer than the standard retention period.

Any extended retention will be documented and reviewed periodically.

15.9 Secure disposal

When personal information is no longer required, we securely delete, destroy or appropriately anonymise it. The Medical Director oversees review and disposal of clinical records; Administration deletes files on instruction after the applicable review. Supplier backup/deletion arrangements are handled under the relevant service safeguards.

We will not retain personal information indefinitely simply because it may be useful in the future.

Retention periods will be reviewed periodically to ensure that information is not kept for longer than necessary.

15.10 Enquiries and prospective patients

Where an enquiry does not proceed to clinical assessment, enquiry emails are deleted six months from last contact and basic Cliniko contact details are removed 12 months from last contact. The Administration team performs these deletions, subject to any necessary documented legal hold.

Where an assessment or clinical screening creates a clinical record, its retention is determined by the nature and purpose of that record, even if treatment does not follow. We do not automatically assign all prospective-patient information either a short enquiry period or a 20-year treatment period.

Information may be irreversibly anonymised where appropriate. Removing names alone is not necessarily anonymisation; pseudonymised information remains personal information.

16. Your rights

Subject to legal conditions and exemptions, you may have the right to:

- be informed about how we use your personal information;
- request access to your personal information;
- request correction of inaccurate or incomplete information;
- request erasure in certain circumstances;
- request restriction of processing in certain circumstances;
- object to certain processing;
- object to direct marketing;
- request data portability where the statutory conditions apply; and
- withdraw consent where processing is based on consent.

These rights are not absolute.

Legal obligations, confidentiality duties, clinical-record requirements and other statutory exemptions may affect what we can delete, disclose or change.

16.1 Right of access

You may ask us for a copy of the personal information we hold about you. This is commonly called a Subject Access Request (SAR).

We respond without undue delay and normally within one month, subject to the statutory rules. We carry out reasonable and proportionate searches for the information to which you are entitled. Where reasonably required and permitted by law, we may seek clarification of the information or processing activities requested and pause the response period while awaiting that clarification. We tell you when this applies.

Where a request is complex or where you have made a number of requests, the applicable legal extension may apply. Where we extend the response period, we will tell you within the applicable initial period and explain why.

We will normally provide access to your personal information without charge.

We may charge a reasonable fee or refuse to comply where a request is manifestly unfounded or excessive, in accordance with the law.

We may ask for proportionate evidence of your identity where necessary to ensure that personal information is not disclosed to the wrong person.

Where you request access to clinical or treatment records, we will consider applicable legal requirements, confidentiality obligations and exemptions before providing the information.

16.2 Right to rectification

If you believe that personal information we hold about you is inaccurate or incomplete, you may ask us to correct or complete it.

We will consider the information you provide and take appropriate steps where correction or completion is required.

In clinical records, information may need to be retained for an appropriate audit trail. Correcting a clinical record does not necessarily mean deleting the original entry.

16.3 Right to erasure

You may request that we erase your personal information in certain circumstances.

This right is not absolute.

It may not apply where processing is necessary for the provision or management of healthcare under the applicable statutory exception, where we have a legal obligation to retain information, where the information is required for the establishment, exercise or defence of legal claims, or where another lawful exemption applies.

16.4 Right to restriction

You may ask us to restrict processing of your personal information in certain circumstances, including where you contest the accuracy of information or have objected to processing.

16.5 Right to object

You may have the right to object to processing where we rely on legitimate interests as our lawful basis, subject to the circumstances and applicable legal requirements.

You have an absolute right to object to the processing of your personal information for direct marketing.

We will clearly bring your right to object to direct marketing to your attention.

16.6 Right to data portability

Where the statutory conditions apply, you may have the right to receive personal information that you have provided to us in a structured, commonly used and machine-readable format.

Where technically feasible and legally required, you may also have the right to have that information transmitted to another organisation.

This right applies only in specific circumstances, including where processing is carried out by automated means and is based on your consent or is necessary for the performance of a contract.

16.7 Withdrawal of consent

Where we rely on your consent as the lawful basis for processing, you may withdraw your consent at any time.

Withdrawal of consent does not affect the lawfulness of processing carried out before consent was withdrawn.

If another lawful basis applies to the processing, withdrawing consent will not necessarily require us to stop processing your information.

16.8 How to exercise your rights

To exercise any of your rights, contact Jamie Mackenzie, Data Protection Lead.

Email: contact@acesopathway.co.uk

Post:
Aceso Pathway Limited
Chapel House
Leicester Road
Loughborough
LE11 2AF

We may need to verify your identity before responding to your request.

We will deal with requests within the applicable statutory time limits and will explain where a lawful extension, restriction or exemption applies.

17. Automated decision, AI and session recording

Clinical assessment, treatment and monitoring are clinician-led. We do not make patient decisions solely by automated processing where they have legal or similarly significant effects.

We do not currently use AI tools with patient information. We do not audio- or video-record clinical assessment or therapy sessions. Administrative systems may automate reminders or security checks; this is separate from making significant clinical decisions.

Before changing these arrangements, we assess the processing, necessary safeguards and privacy information.

18. Adults who may require additional support

Aceso currently provides clinical assessment and treatment services only to adults aged 18 or over.

Some adults may require support to understand information, communicate with us, exercise their rights or make decisions about their care. We take account of capacity, communication needs, safeguarding circumstances, wishes and preferences, and applicable legal and professional requirements.

Where someone seeks to act on a patient's behalf, we take appropriate steps to establish their identity and authority before disclosing information or accepting instructions concerning the patient's information.

Although we do not treat children, information about a child may appear in an adult patient's clinical, family or safeguarding information. We process it only where necessary and lawful, with appropriate safeguards.

19. Clinical records and access

Aceso maintains clinical records to support safe and effective care and treatment and to meet applicable legal, professional, regulatory and CQC requirements.

Clinical records may include:

- assessments;
- diagnoses or clinical impressions;
- treatment plans;
- progress notes;
- risk assessments;
- safeguarding information;
- consent and decisions relating to care;
- correspondence;
- referrals;
- reports;
- test or diagnostic information where relevant;
- appointment information; and
- records of decisions relating to care and treatment.

Clinical records will be maintained securely and kept accurate, complete and contemporaneous as far as reasonably practicable.

Access to clinical records is restricted to authorised individuals who have a legitimate need to access the information.

Where a patient requests access to their clinical record, Aceso will deal with the request under applicable data-protection law and clinical confidentiality requirements.

Clinical records may contain information relating to other individuals. Where required, information relating to other people may be withheld or appropriately redacted in accordance with the law.

20. Data-protection complaints

If you are concerned about how we collect, use, share, store or otherwise process your personal information, you may complain by email, telephone or post to Jamie Mackenzie, Data-protection lead, using the contact details in Section 1. Please explain your concern and how we can contact you; we can help if you need support to make a complaint.

We acknowledge data-protection complaints within 30 days, investigate appropriately and without undue delay, keep you informed about progress where appropriate, and communicate the outcome without undue delay. We may request further information reasonably needed to investigate.

You also have the right to complain to the Information Commissioner's Office (ICO): Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF. Telephone: 0303 123 1113. Website: https://ico.org.uk/make-a-complaint/

Concerns about healthcare quality or safety may also be raised through our clinical complaints procedure and, where applicable, with CQC or another appropriate regulator.

21. Changes to this Privacy Policy

We may update this Privacy Policy to reflect changes in:

- our services;
- our systems or technology;
- our suppliers;
- our information-handling practices;

- applicable legislation;
- regulatory requirements; or
- relevant guidance.

The current version will be published on our website.

We will review this Privacy Policy at least annually and sooner where there is a material change in our processing activities or the applicable legal or regulatory framework.

Last reviewed: 5 October 2026
Next scheduled review: 5 October 2027, or sooner if there is a material change.

Where a change materially affects how we use your information or your rights, we take reasonable steps to bring it to your attention where appropriate.

22. Our data-protection governance

This policy is supported by our internal data-protection, information-governance, confidentiality, information-security, safeguarding, records-management and clinical-governance arrangements.

We keep those arrangements under review and update them where necessary to reflect changes in services, systems, suppliers, technology, processing and applicable law.

23. Legal and regulatory requirements

We process personal information in accordance with applicable UK data-protection and privacy law and the legal, regulatory, professional and confidentiality requirements applying to our healthcare services.

As a CQC-registered healthcare provider, we maintain appropriate clinical and governance records in accordance with applicable regulatory requirements.

24. Version and review information

Document: Privacy Policy Version 1

Prepared and reviewed: 8 October 2026

Effective date: 8 October 2026

Next scheduled review: 8 October 2027, or sooner following a material change.