

Privacy Policy

Palmer and Palmer Psychology Ltd is committed to protecting your privacy and handling personal information lawfully, fairly and securely. This policy explains what information we collect, why we use it, who we may share it with, how long we keep it and what rights you have under UK data protection law.

1. Who we are

Palmer and Palmer Psychology Ltd is incorporated in England and Wales with registered number 14602051. Our registered office is 7 The Close, Norwich, Norfolk, NR1 4DJ, England.

For data protection queries, please contact Dr Nick Palmer by email at npalmer@papps.org.uk or by telephone on 01603 555 670.

We are registered with the Information Commissioner's Office with reference number ZB511845.

2. What this policy covers

This policy applies when we collect or use personal information in connection with our psychological, therapeutic, educational, assessment, consultation, reporting, website and communication services. We process personal data in accordance with the UK GDPR and the Data Protection Act 2018.

3. The nature of our work

We provide services to children, young people and adults. Our work may involve sensitive information, including health, mental health, education, social care, special educational needs, safeguarding, family, legal and professional information. As practitioner psychologists, we are regulated by the Health and Care Professions Council and follow relevant professional standards, including those of the Health and Care Professions Council and the British Psychological Society.

4. What personal information we collect

- Contact and identity details, such as name, address, email address, telephone number and date of birth.
- E-signing and client portal records, including IP address, verified email address, timestamps, the version of our terms accepted, audit trail information, and the consents and acknowledgements you give.
- Clinical, therapeutic, assessment and professional records, opinions and reports.
- Health, mental health, education, social care and special educational needs information.
- Information about parents, carers, family members, schools, professionals and other people involved in a case.

- Payment, billing and financial information.
- Audio, video, written notes, transcripts or records from assessments, therapy sessions or consultations, where appropriate.
- Website, cookie and analytics information (please see our Cookie Policy for more detailed information).

5. How we collect information

We may collect information directly from you, from a parent or representative, from a commissioning organisation, or from other professionals involved in your care, education or legal matter. This may include information from referral forms, emails, telephone calls, video calls, in-person sessions, remote sessions, schools, solicitors, local authorities, NHS bodies, courts, tribunals, CAFCASS officers and other relevant organisations or professionals.

6. Why we use personal information

- To provide psychological, therapeutic, educational, assessment, consultation and reporting services.
- To communicate with clients, parents, carers, representatives, commissioning organisations and professionals.
- To prepare and maintain accurate clinical, administrative and financial records.
- To process payments and manage accounts.
- To comply with legal, regulatory, safeguarding and professional obligations.
- To manage complaints, requests, legal proceedings and professional responsibilities.
- To improve and administer our services, website and business operations.

7. Our lawful bases

We rely on different lawful bases depending on the purpose of the processing. These may include contract, legal obligation, legitimate interests and consent.

Where we process special category data, such as health or mental health information, we also identify a separate condition under Article 9 of the UK GDPR. For our clinical, therapeutic and assessment work, this will usually be that the processing is necessary for the provision of health or social care, carried out by or under the responsibility of a health professional subject to a duty of confidentiality (Article 9(2)(h) of the UK GDPR and Schedule 1 to the Data Protection Act 2018). Where we process criminal offence data, we only do so where authorised by law, including where necessary for safeguarding, legal claims, court or tribunal proceedings, or another relevant condition under the Data Protection Act 2018.

When you accept our terms, we may ask you to tick boxes confirming certain consents and acknowledgements. Where we rely on consent (for example, for the use of AI tools described in section 11), you can withdraw it at any time through your client portal (where available) or by contacting us, and we will record and act on your withdrawal for the future. Withdrawing consent

does not affect processing already carried out, and it does not require us to delete records that we must keep for the retention periods in section 12 or that we process on another lawful basis.

Where we rely on legitimate interests, we only do so where the processing is necessary, proportionate and balanced against your rights. You have the right to object to this type of processing, although we may continue where we have compelling legitimate grounds, professional duties, safeguarding responsibilities or legal obligations.

We may also rely on the basis of recognised legitimate interests, introduced by the Data (Use and Access) Act 2025, for certain limited purposes that support important public or organisational aims. These may include helping to prevent fraud or misuse of our services, supporting safeguarding and professional standards, responding to emergencies or protecting wellbeing, and improving accessibility and inclusion. We carry out a balancing test to ensure our interests do not override your rights, and you have the right to object to this type of processing at any time.

8. Confidentiality, safeguarding and legal proceedings

We treat personal information as confidential. However, confidentiality is not absolute. We may share information without consent where we reasonably believe this is necessary to protect a child, young person or adult from serious harm, to prevent or detect serious crime, to comply with a legal requirement or court order, or to meet our professional and safeguarding obligations.

Where we are instructed in legal, family or tribunal proceedings, including as an expert witness, our overriding duty may be to the court or tribunal. We may be required to disclose reports, records and related information to the court, parties, legal representatives, CAFCASS and other appointed professionals in line with relevant rules, directions and orders.

9. Who we share information with

We only share personal information where there is an appropriate lawful basis and where sharing is necessary. This may include sharing with commissioning organisations, parents or carers, schools, local authorities, NHS bodies, healthcare providers, social workers, solicitors, barristers, courts, tribunals, CAFCASS officers, professional partners, regulators, payment processors, accountants, insurers, lawyers, contractors, technical providers and other trusted service providers.

We require third parties who handle information for us to use appropriate safeguards. We aim to share only the minimum information necessary for the purpose.

As practitioners regulated by the Health and Care Professions Council, we are required to take part in clinical supervision, which involves discussing our work with another appropriately qualified professional to reflect on and improve our practice. When we discuss clients in supervision, we refer to them by first name only and keep identifiable information to a minimum.

10. Payments and marketing

We use third-party providers, including Stripe, Monzo and Xero, to process payments and manage financial records. These providers process payment data in accordance with their own data protection policies and applicable law.

If we send marketing communications, we will do so on the basis of consent or legitimate interests, where permitted. You can opt out at any time by contacting us or using the unsubscribe option in our communications.

11. Artificial intelligence

We use AI in a limited and controlled way to support tasks such as research, document preparation, statistical analysis, transcription during remote or in-person sessions where appropriate, administration and organisation of information.

AI supports our work but does not replace professional judgement. Important outputs are reviewed and verified by a suitably qualified person before being relied on or shared. The main AI tool we use is Heidi AI (provided by Heidi Health Limited), for transcription and note-taking support. We will ask for your consent before using AI with your (or your child's) information. Consent is given once for the instruction as a whole, rather than for each individual use, and you can withdraw it at any time. If you prefer, you can choose a service without AI; please note this may take longer to complete. More detail about our use of AI is set out in our AI policy which can be found on our website.

12. How long we keep information

- Children's records are usually kept until the child's 25th birthday (26 if they were 17 at conclusion), or 7 years after conclusion if that is later.
- Adult records are usually kept for seven years from the final date of contact.
- Once you have formally instructed us, records are held securely for the applicable retention period above and are then securely deleted, unless we need to keep them for longer for legal, regulatory, safeguarding or court-related reasons. Because we have professional and legal obligations to keep clinical records for these periods, we will not usually be able to delete them earlier, although we will consider any request in line with your rights under data protection law.
- Enquiries and referrals that do not proceed are usually kept for no longer than 28 days, unless professional, safeguarding or legal reasons require us to keep an appropriate record.
- Marketing information is kept until you opt out or tell us you no longer wish to receive marketing.
- Some information may remain in backups or archives for legal, tax, regulatory or security reasons.

13. Recordings and photographic materials

Any audio or video recordings and photographs we make during assessments, interventions, training or observations are used only to deliver our professional services. This may include assessing needs and forming recommendations, preparing reports or statutory advice (such as EHCP contributions), supporting staff training and reflective practice (anonymised where appropriate), and informing multidisciplinary discussions, planning or tribunal input.

All such materials are stored securely using encrypted systems with appropriate access restrictions. We keep them only for as long as necessary for the purpose for which they were made, typically no longer than 12 months, unless a longer period is legally required or agreed in writing.

It may be necessary for the parent and/or school to share video clips of the child as part of the assessment process. Please share these through our secure client portal (once it is available to you) or other secure means we specify. These recordings will be used solely to complete the assessment and will be deleted promptly after review and once the assessment is concluded, unless we are legally required to keep them for longer.

We will not disclose, share or publish recordings or photographs externally without separate written parental or client consent, unless disclosure is required by law, for example to meet our safeguarding obligations. We will honour deletion requests where lawful and feasible.

14. Security

We take the security of your information seriously and have measures in place to protect it against unauthorised access, loss, alteration or disclosure.

These include restricting access to your information to those members of our team who need it in connection with your care, confidentiality obligations on everyone working with us, encrypted storage for client records, secure disposal of information that is no longer needed, and secure arrangements for working remotely.

We are introducing a new clinical management system with a secure client portal. Once it is available to you, clinical documents will be shared through the portal rather than by email. Until then, we continue to use secure storage and secure methods of sharing information. We keep our security arrangements under regular review.

If a personal data breach is likely to result in a risk to your rights and freedoms, we will report it to the Information Commissioner's Office without undue delay and, where feasible, within 72 hours of becoming aware of it. If a breach is likely to result in a high risk to your rights and freedoms, we will also inform you without undue delay.

15. Where your information is held

We keep personal information in the UK wherever possible. Our email, calendar and video-calling services (Microsoft 365) are hosted in the UK, and our new client records system will be hosted in

the UK. During transition to that system, some client records remain in encrypted storage hosted in the EU. The service we use to send automated emails (such as portal notifications) is hosted in the EU.

Some of our providers are based outside the UK, or may occasionally access information from outside the UK, for example to provide technical support. Where this happens, we keep it to the minimum necessary and ensure an appropriate level of protection by relying on a UK adequacy decision for the relevant country, or by putting in place appropriate safeguards such as the ICO's International Data Transfer Agreement or the UK Addendum to the EU Standard Contractual Clauses.

You can contact us at npalmer@papps.org.uk for more information about these safeguards or to request a copy.

16. Children and young people

We are committed to protecting children's privacy. Where our services, website or content are likely to be used by children under 18, we take account of children's best interests, use clear language where appropriate, avoid unnecessary tracking or profiling, and seek parental or guardian involvement where required.

- Under 13: we require consent from a parent or person with parental responsibility.
- Ages 13 to 15: we usually require parental consent, although some young people may be able to consent themselves if they fully understand the implications.
- Ages 16 to 17: young people can generally consent to processing of their health data themselves, although parents or carers may be involved with the young person's agreement or where otherwise appropriate.
- Age 18 and over: adults control their own information, unless safeguarding or legal exceptions apply.

If parents are separated, both parents with parental responsibility generally have equal rights to information about their child unless a court order or other legal restriction says otherwise. Please tell us about any relevant arrangements or restrictions. Our client portal can give other parents or carers with parental responsibility their own access to view and contribute to the case file. We will offer this only where appropriate and lawful, and subject to our professional judgement and safeguarding obligations.

17. Your rights

You have rights under data protection law, including the right to access your information, ask us to correct inaccurate information, ask for erasure in certain circumstances, restrict processing, object to processing, and request data portability where applicable. These rights are not absolute and may be limited where information must be retained for professional, safeguarding, legal, regulatory or court-related reasons.

The right to correct information relates to objectively factual errors and does not extend to disputed professional opinion or interpretation. Where information is incomplete rather than inaccurate, we may add a supplementary statement rather than amending the underlying record.

To exercise your rights, withdraw consent where consent is our lawful basis, or make a data protection enquiry, please log in to your client portal (once it is available to you) or contact us at npalmer@papps.org.uk. We may ask for information to verify your identity before responding. If we decide not to take action on a request you make, we will explain why and let you know that you can complain to us and to the Information Commissioner's Office.

When you make a request to access your information (a subject access request), we will respond within one calendar month. If we need to verify your identity first, the time limit will not start until we have done so. Where a request is complex or repetitive, we may extend this period or limit its scope in line with the Data Protection Act 2018 and the Data (Use and Access) Act 2025, and we will explain our reasons and keep you informed.

18. Complaints

You have the right to complain to us directly if you think we have not handled your personal information in line with data protection law. Please contact us first so we have the opportunity to put things right.

You can complain by email at npalmer@papps.org.uk or in writing to Dr Nick Palmer at the address above. You do not need to use any particular wording, but it helps if you make clear that you are making a data protection complaint and provide enough detail for us to investigate. We will acknowledge your complaint within 30 days of receiving it, look into it without undue delay, keep you informed of progress and any expected delays, and tell you the outcome without undue delay.

You also have the right to complain to the Information Commissioner's Office at <https://ico.org.uk/>. Complaining to us does not affect your right to complain to the ICO at any time.

19. Changes to this policy

We may update this policy from time to time. The latest version will be available on our website. Please keep us informed if your contact details or other relevant information changes while we hold your data.