



Privacy and Data Protection Policy

Sandco (South East) Ltd trading as BYND Mentoring

Policy owner: Sam Watson, Director

Version 1.0 | Issued 16 September 2026 | Review by 16 September 2027

What this policy explains

We respect the privacy of children, young people and families. This policy explains what information BYND collects, why we use it, who can see it, how long we keep it and how you can exercise your rights. It also sets mandatory data-handling standards for our employees and freelance workers.

BYND provides mentoring and therapeutic support to people aged 5 to 18 in Kent and Medway, in schools, homes and community venues. Qualified BACP-registered counsellors deliver counselling. This notice covers service users, parents and carers, school contacts and people making enquiries. Recruitment and employment information requires separate workforce privacy information.

Who is responsible

Sandco (South East) Ltd is the controller for personal information where BYND decides why and how it is used. Schools and independently practising counsellors may be separate controllers for their own records. We agree responsibilities for each service; if we act only on a school's documented instructions, the school's privacy notice and our processing agreement also apply.

ICO registration number: C2035627

Contact us about your information

Sam Watson, Director

Email: hello@gobynd.org | Telephone: 01227 686787

BYND Mentoring, Unit 40, District Park, Manston Road,
Margate, Kent, CT9 4JZ

Daisy Watson, Deputy Designated Safeguarding Lead: daisy@gobynd.org. Privacy requests may be made by email, telephone or post. Please tell us if you need an accessible format or help understanding this policy.

1 Information we collect and why

Information about young people and families

We collect information relevant to the support provided: names, dates of birth, home addresses, parent or carer and contact details, school details, referrals, session notes, progress reports, safeguarding concerns, diagnoses and relevant family circumstances. Information about health, disability or mental wellbeing is special category data and receives additional legal protection. Other sensitive information is recorded only where relevant and lawful.

We obtain information from the young person, parents or carers, referring schools and professionals involved in support or safeguarding. Our workers also create records from their observations and professional work. We distinguish facts, reported information and professional opinion, record sources where relevant and correct errors transparently.

How we use it

We use information to assess referrals, plan and deliver suitable support, arrange sessions, understand needs and risks, monitor progress, provide proportionate mentoring updates to schools, respond to concerns and complaints, and maintain appropriate records of our work. We also use necessary information to protect children and others from harm, meet legal duties, manage service agreements and invoices, and establish or defend legal claims.

We use enquiry details, including telephone numbers and the school, organisation or location the person is contacting us from, to respond and arrange follow-up. Website use can also generate technical information such as IP addresses, device or browser information, pages visited and cookie identifiers; section 6 explains this.

Collecting only what is needed

Staff must avoid unnecessary family detail, speculative diagnoses and unrelated third-party information. Access and sharing must be limited to the purpose concerned. We do not sell service-user records or use mentoring, counselling or safeguarding information to build advertising audiences.

There is no general legal duty on families to provide information to BYND. Some identity, contact and support information is necessary to arrange safe services. If it is not supplied, we will explain whether we can offer an alternative or cannot safely proceed. Optional information and advertising consent are not conditions of support.

Keeping people informed

We provide this notice when collecting information directly. For information received from a school or another source, we provide privacy information within a reasonable period and normally within one month, or earlier at our first communication or disclosure, unless a lawful exception applies. We explain relevant changes before using information for a new purpose.

2 Lawful use and consent

We apply the UK GDPR, the Data Protection Act 2018 and applicable Privacy and Electronic Communications Regulations, as amended by the Data (Use and Access) Act 2025. Permission to attend mentoring and the legal basis for handling information are related but distinct.

Routine support and administration

For referral administration, necessary mentoring records, progress monitoring, proportionate school updates and responding to enquiries, we normally rely on legitimate interests under Article 6(1)(f). These interests are providing safe, effective support, coordinating with the commissioning school and maintaining accountability. The Director must document necessity and balance these interests against the person's rights, giving particular weight to children's interests.

Article 6(1)(b), contract, applies only where processing is necessary for a contract with the individual, or steps they request before entering it. A school's contract does not automatically provide this basis for a child's information. We use Article 6(1)(c) for a specific applicable legal duty, and Article 6(1)(f) for necessary legal-claims administration where appropriate.

Health information and other sensitive records

An Article 6 basis is not enough for special category data. For routine mentoring involving health or diagnosis information, staff must obtain and record explicit consent under Article 9(2)(a), unless the Director has established and documented another applicable condition. The consent must expressly cover the sensitive information, purpose and intended sharing. A general referral signature alone is insufficient.

For eligible counselling or health or social care, Article 9(2)(h) and Schedule 1 paragraph 2 of the Data Protection Act may apply only where all conditions, including the required duty of confidentiality, are met. BACP registration alone must not be assumed to establish this. The counsellor must explain the basis for their clinical records. Necessary legal claims may use Article 9(2)(f).

Referral permission and the young person's choice

Parents or guardians normally provide referral consent to the school, which confirms that it holds that consent. BYND must check its scope and retain evidence or an auditable confirmation. A school confirms consent received; it does not acquire parental responsibility by signing a referral.

We explain the service, records and confidentiality limits in language the young person understands and seek their agreement to sessions. Capacity and understanding are considered individually; there is no blanket assumption that all under-16s cannot consent. At 18, the individual makes their own decisions unless a lawful capacity arrangement applies.

Where we rely on consent, it can be withdrawn through the worker or our contact details as easily as it was given. Withdrawal does not undo lawful earlier use. We explain any impact on support; records needed under a separately established legal basis, such as safeguarding or legal claims, may still be kept.

3 Sharing and confidentiality

Access within BYND

Access is limited to authorised people with a need to know, including the worker supporting the child, the Director and the Deputy Safeguarding Lead. Team membership alone does not justify access to every file. Safeguarding files have separate restricted permissions. Staff must observe confidentiality during and after their engagement.

Mentoring reports for schools

Mentoring session updates and reports are shared through a secure portal with authorised school staff. Updates explain relevant activities, themes, progress and agreed actions. They must be accurate and proportionate, avoiding unnecessary private detail or verbatim disclosures. We explain this routine sharing to the young person and parent or carer before support begins.

Counselling records remain separate

Counsellors keep separate clinical records, with paper records secured in a locked filing cabinet. These are not routinely included in mentoring reports or uploaded to the school mentoring portal. Any counselling summary requires an appropriate agreed purpose and lawful basis, subject to safeguarding or other legal exceptions. Necessary clinical supervision must preserve confidentiality and minimise identifying information.

Before counselling starts, the counsellor must explain who controls the clinical records, their retention period, confidentiality limits and how to request access. Keeping records separately does not, by itself, determine whether the counsellor or BYND is the controller. This responsibility must be agreed and made clear to the family.

Safeguarding and legally required disclosures

We may share necessary information with school safeguarding leads, children's or adult social care, police, health professionals and other appropriate safeguarding bodies. We record the recipient, purpose, information shared and lawful basis. We explain sharing where safe, but do not seek consent or notify a family member if this would put someone at risk or undermine an investigation.

For qualifying safeguarding purposes we may rely on recognised legitimate interests under Article 6(1)(ea), an applicable legal obligation under Article 6(1)(c), or vital interests under Article 6(1)(d) where necessary to protect life. Special category safeguarding data may rely on Article 9(2)(g) and Schedule 1 paragraph 18, where its conditions are met; Article 9(2)(c) applies only to vital interests where the person cannot physically or legally consent. Required appropriate policy documentation must be maintained. Criminal-offence data also requires an Article 10 and domestic-law condition.

Other recipients and safeguards

Technology providers support storage, the portal, communications and the website. Necessary information may also go to professional advisers, insurers, regulators or courts. Recipients must have a defined lawful purpose; service providers acting for us require appropriate processing terms. The Director verifies school and counsellor agreements, permissions and secure transfer arrangements. Parent or carer requests are considered alongside the young person's rights and confidentiality; access is not automatic.

4 Secure storage and digital tools

Records and access controls

BYND stores electronic records on Google Drive and Dropbox using strong passwords and two-factor authentication. Staff must use approved work accounts, restricted folders and named access permissions, and must not create public sharing links for client files. The Director must review access, remove it promptly when duties end and check sharing settings and recovery arrangements.

Devices used for work must be protected with screen locks, current security updates and appropriate encryption. Staff must avoid unattended unlocked devices and unnecessary downloads. Paper files must remain in locked storage when not in use and be transported only where necessary and securely. Relevant records must be recoverable; backups and deleted-file retention require controlled access and scheduled review.

Internal WhatsApp use

WhatsApp is used only internally within the team where required, not to communicate with schools, parents or young people. It is not the official case-record system. Staff must minimise personal information, use case references where possible and keep clinical notes, full session reports and detailed safeguarding records in the approved systems. Relevant decisions must be transferred to the official record; unnecessary message copies must then be removed in line with retention rules. Group membership, linked devices and backups require Director approval.

AI assistance and dictated notes

BYND uses ChatGPT and Microsoft Copilot to assist with drafting and with notes dictated by a worker after a session. We never record mentoring or counselling sessions. Post-session dictation describes the worker's recollection; it is not a recording of the child or the session.

Staff must remove names and other identifying details before using AI unless the Director has expressly approved the particular account, purpose and safeguards for identifiable data. Initials alone may not anonymise a record: school, location, family detail and unusual circumstances can identify a person. Where sufficient anonymisation is not possible and approval is absent, the worker must prepare the record without entering it into AI.

Approval for identifiable or pseudonymised information requires a documented lawful basis and special-category condition, provider terms and security review, retention and international-transfer checks, and a data protection impact assessment where processing is likely to create high risk. Approved settings must prevent client content being used to train general-purpose models. No assumption may be made that every ChatGPT or Copilot account has the same protections.

A worker must check every draft against their own notes, correct errors and remove invented or unnecessary content before saving or sharing it. AI must not make diagnoses, safeguarding judgements or decisions about eligibility or support. BYND does not make decisions with legal or similarly significant effects solely by automated processing. Temporary prompts, outputs and dictation audio must be deleted when the checked record is complete, subject to justified holds and verified provider retention arrangements.

5 Retention and overseas processing

How long we keep records

BYND's mentoring and safeguarding case records are normally retained until the young person's 25th birthday, followed by a documented review and secure disposal. This is BYND's retention policy, not a universal statutory period. It supports continuity, safeguarding accountability and the handling of concerns that may emerge after childhood.

We retain particular records longer only where necessary and justified, for example for an active investigation, legal claim, preservation requirement or continuing safeguarding need. A contract does not justify unnecessary indefinite retention. The Director records the reason, restricted access and a further review date. Unnecessary duplicates and working material are removed sooner.

Separately controlled counselling records follow the counsellor's disclosed clinical retention schedule. Where BYND controls such records, the Director and counsellor must establish a suitable documented clinical retention period and explain it before treatment; the mentoring period does not automatically apply.

Enquiries that do not lead to a service are kept only while needed to respond and manage reasonable follow-up, then reviewed for deletion. Complaints are kept through resolution and any proportionate period needed for accountability or legal claims. Financial and contractual records follow the applicable statutory and claims requirements. The Director must record the period or objective criteria for each category in the retention schedule, avoiding unnecessary child-level information in financial records.

Cookie lifetimes and analytics retention must be specified in the website's current cookie information and provider settings. Temporary AI material follows section 4. Paper records are cross-shredded or securely destroyed; electronic disposal must address local copies, portal copies, recycle bins and backup cycles. Records awaiting backup expiry remain protected and must not return to routine use. Disposal is logged without retaining the discarded sensitive content.

Processing outside the United Kingdom

Our cloud, AI, communications and website providers may process information outside the UK, including through overseas support or subprocessors. We must not assume that Google Drive, Dropbox, ChatGPT, Microsoft Copilot, WhatsApp or Wix processing is UK-only.

Before permitting a restricted international transfer, the Director must establish a lawful transfer mechanism. This may be UK adequacy regulations where applicable, or appropriate contractual safeguards such as the UK International Data Transfer Agreement or UK Addendum, supported by the required assessment and additional protections where necessary. A provider's general statement of GDPR compliance is not a substitute for this check.

You can contact the Director for details of the providers and destinations applicable to your information and a copy or explanation of the relevant safeguards, with confidential commercial information redacted where necessary. New providers or changes affecting personal information must be assessed and reflected in our privacy information before use.

6 Website privacy and your rights

Website enquiries cookies and advertising

Our Wix website collects basic enquiry information, including telephone number and where the person is contacting us from, to enable a response. Please do not submit detailed health, counselling or safeguarding records through a general enquiry form; contact us to arrange a secure route.

The website uses cookies, analytics and advertising tracking. Essential technologies support site operation and security. Analytics helps us understand use, while advertising technologies may measure campaigns and track visits or interests. Relevant technical identifiers and activity may be received by Wix and the analytics or advertising providers enabled on the site.

BYND requires prior opt-in consent for optional analytics and advertising tracking. These technologies must remain blocked until consent, with an equally accessible way to reject them and change preferences. Essential technologies do not require consent where the legal exception applies. Consent to advertising is separate from permission for mentoring.

The Director must maintain an accurate website cookie list naming the actual providers, purposes, lifetimes and relevant transfers, and verify that the banner controls all enabled trackers. This policy does not replace that configuration or detailed cookie information. Clinical, referral, safeguarding and portal content must never be passed to advertising tools or used to target children. Tracking must not operate on confidential portal pages.

Your information rights

You may ask to see or receive a copy of your personal information, correct inaccuracies, request erasure or restriction, and receive portable information where the legal conditions apply. Rights depend on the basis and circumstances; deletion may be limited by safeguarding, legal duties or claims. We explain any lawful refusal and how to challenge it.

Your right to object

You can object to processing based on ordinary legitimate interests for reasons relating to your situation. We must stop unless we demonstrate compelling overriding grounds or need the information for legal claims. You can object to direct marketing at any time, and we will stop using your information for that purpose. Contact hello@gobynd.org.

Requests from children and parents

These rights belong to the young person. We consider their understanding and wishes, parental responsibility and any authority to act, third-party confidentiality and safeguarding risks. A parent does not automatically receive all records. We can help a child make a request directly and explain the outcome in accessible language.

Requests may be verbal or written and do not need legal wording. We may reasonably verify identity and authority. We respond without undue delay and normally within one month, free of charge. Where law permits an extension of up to two further months for complexity or number, we explain it within the first month. Any lawful clarification-related pause or exception will be explained. Consent-based use can be stopped by withdrawing consent through the same contact routes.

7 Complaints incidents and accountability

Privacy concerns and complaints

Please contact Sam Watson at hello@gobynd.org, 01227 686787, or the postal address on page 1. Tell us what happened and the outcome you seek; you do not need to use a special form. We assist people who need help to complain, acknowledge data-protection complaints within 30 days and investigate and respond without undue delay, keeping you informed.

You may also complain to the Information Commissioner's Office. Our complaints process does not remove your right to contact the ICO or seek a judicial remedy. We explain findings, remedial action and escalation options in our response.

[ICO complaints and advice](#)

ICO telephone: 0303 123 1113

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

Lost information and security incidents

Staff must report suspected loss, misdirected messages, unauthorised access or disclosure immediately to the Director or deputy. We contain the incident, preserve evidence, assess harm and record the decision. We notify the ICO without undue delay and, where feasible, within 72 hours of becoming aware if the breach is likely to risk people's rights and freedoms. If it is likely to create a high risk, we notify affected people without undue delay unless a lawful exception applies. We document all breaches, including those not reported.

Responsibility and review

The Director is accountable for implementation, staff guidance, permissions, provider contracts, lawful-basis records, retention, complaints and incident management. Staff must read this policy and receive training appropriate to their role. The Director must maintain required processing records and appropriate policy documents, carry out impact assessments for likely high-risk processing and check security controls in practice.

This policy is reviewed at least annually and sooner when services, technology, legal duties or risks change. It must be read alongside BYND's Safeguarding and Child Protection Policy. Changes must be communicated to staff and affected people; necessary safeguarding action must never wait for a privacy enquiry to be resolved.

A short explanation for young people

We keep notes to help us support you. Only people who need them for their work should see them. Your school gets relevant mentoring updates through a secure system. Counselling notes are separate. We never record your sessions. If we are worried someone is unsafe, we may need to tell someone who can help. You can ask what we write, tell us if something is wrong, or speak to Sam if you are worried about your information.

Guidance supporting this policy

[ICO guidance on privacy information](#)

[ICO guidance on children and the UK GDPR](#)

[ICO guidance on special category information](#)

[ICO guidance on cookies and tracking technologies](#)

[ICO overview of the Data Use and Access Act changes](#)