



PRIVACY NOTICE

Website, services and Microsoft Teams events

Last updated: 5 August 2026

At a glance

Bridge the Gap Child Mental Health C.I.C. provides emotional wellbeing and mental health support, training and events. This notice explains what personal information we collect, why we use it, who we may share it with, how long we keep it and the choices and rights available to you.

Who this notice is for

This notice applies to children and young people, parents and carers, service users, website visitors, event attendees, customers, donors, supporters, referrers and other people who contact or work with us.

Separate privacy notices may apply to staff, job applicants, contractors, students and volunteers.

When we provide a service commissioned by a school, local authority, NHS body or another organisation, that organisation may also be a controller of your information. Its privacy notice will explain how it uses your information. We will explain the arrangement where it affects you.

1. Who we are

Bridge the Gap Child Mental Health C.I.C., referred to in this notice as “Bridge the Gap”, “we”, “us” or “our”, is the controller for the personal information described in this notice unless we tell you otherwise.

Organisation details	Information
-----------------------------	--------------------

Legal name	Bridge the Gap Child Mental Health C.I.C.
------------	---

Registered office	10/11 St. Mary’s Gate, Derby DE1 3JR
-------------------	--------------------------------------



Organisation details Information

Service address 10/11 St Mary's Gate, Derby DE1 3JR

Company number 12191993

ICO registration number ZB201892

Privacy contact nikkiwebster@jwbridgethegap.com

Website www.wearebridgethegap.com and www.jwbridgethegap.com

2. The law that applies

We handle personal information in accordance with:

- the UK General Data Protection Regulation, known as the UK GDPR;
- the Data Protection Act 2018;
- the Privacy and Electronic Communications Regulations 2003, known as PECR;
- the Data (Use and Access) Act 2025; and
- any other relevant legislation, as amended or replaced from time to time.

“Personal information” means information that identifies you or could reasonably be linked to you.

Some information needs additional protection. This includes information about:

- physical or mental health;
- racial or ethnic origin;
- religious or philosophical beliefs;
- sex life or sexual orientation;
- genetic information; and
- biometric information used to identify someone.

This is known as special category data.



Information about criminal allegations, proceedings or convictions also has additional protection.

3. Information we may collect

We may collect and use:

- identity and contact details, including your name, preferred name, age or date of birth, pronouns, address, telephone number, email address and emergency contacts;
- information about a child or young person and their family, education, development, relationships, communication, wellbeing, mental or physical health, neurodivergence, support needs, strengths, goals and preferences;
- service information, including enquiries, referrals, assessments, consent and parental-responsibility information, appointment and attendance records, session notes, plans, reviews, outcomes, reports, correspondence and safeguarding records;
- information received from or shared with parents and carers, schools, health and social care professionals, local authorities, funders, commissioners and other agencies involved in providing support;
- payment and transaction information. Card payments are normally handled by our payment provider, and we do not normally receive or retain your full card details;
- event and training information, including bookings, organisation or role, access requirements, attendance, questions, feedback and certificates;
- Microsoft Teams information, including registration and attendance details and, where an event is recorded, information captured in the recording or transcript;
- communications, complaints and feedback, including emails, messages, telephone notes, survey responses and testimonials where you have agreed to provide them;
- marketing preferences and records of when and how you subscribed, unsubscribed or objected;



- website and device information, such as your IP address, approximate location, browser, device, referring page, pages viewed and cookie or similar identifier information, according to your cookie choices; and
- photographs, audio or video where there is a clear purpose and an appropriate lawful basis. We will provide additional information where needed.

4. How we obtain information

We may obtain information:

- directly from you;
- directly from a child or young person;
- from a parent, carer or person with parental responsibility;
- from a school, commissioner, health or social care professional, local authority or other referrer;
- through event, booking and payment platforms;
- automatically when you use our website or online services; and
- from publicly available sources where this is relevant and lawful.

If we receive personal information from another source, we will provide appropriate privacy information within the time required by law unless an exemption applies.

Please only give us another person's information when you are authorised to do so and the information is necessary.

5. Why we use information and our lawful bases

We must have a lawful basis under Article 6 of the UK GDPR for each way in which we use personal information.

If we use special category data, we must also identify an additional condition under Article 9 of the UK GDPR and, where required, a condition under the Data Protection Act 2018.

The basis we use will depend on the service and circumstances. We record our lawful bases within our internal data-protection records.



Purpose	Typical Article 6 lawful basis	Additional condition where relevant
Responding to enquiries and arranging and delivering privately purchased support, assessments, coaching, counselling, workshops or training	Contract or taking steps at your request before entering a contract. Legitimate interests may apply to related administration.	Health or social care where the legal conditions are met. Otherwise, explicit consent or another appropriate Article 9 condition may apply, depending on the service.
Delivering commissioned or referred services and reporting appropriately to the commissioner	Contract, legitimate interests or public task, depending on the arrangement.	Health or social care, substantial public interest, explicit consent or another condition appropriate to the arrangement.
Keeping service records, monitoring quality and outcomes, providing clinical or safeguarding supervision, evaluating services and managing risk	Legitimate interests, legal obligation, contract or public task, depending on the circumstances.	Health or social care, safeguarding children and individuals at risk, substantial public interest or legal claims.
Protecting a child, young person or another person and responding to safeguarding concerns, emergencies, crime or legal requests	Legal obligation, vital interests, legitimate interests or public task.	Vital interests, health or social care, safeguarding children and individuals at risk, preventing or detecting unlawful acts or legal claims.
Administering Microsoft Teams events, confirming attendance, providing joining details, access	Contract where the event has been booked or legitimate interests in	Normally not applicable. If health or other special category information is volunteered, the applicable



Purpose	Typical Article 6 lawful basis	Additional condition where relevant
support, resources, certificates and event follow-up	delivering and evaluating the event.	condition will depend on why it is necessary. We minimise the information collected.
Recording a Microsoft Teams event where recording has been clearly announced	Usually legitimate interests in providing a replay or training resource, balanced against attendees' privacy. In some circumstances, we may ask for consent.	We aim not to capture special category information about attendees. A separate condition and additional safeguards would be required if we intentionally included this information.
Managing our organisation, accounts, insurance, legal claims, audits, fraud prevention, security and regulatory compliance	Legal obligation, legitimate interests or contract.	Legal claims, employment or social protection, substantial public interest or another relevant condition.
Sending service messages, including booking confirmations, changes, reminders and essential updates	Contract or legitimate interests. These are service messages and not marketing.	Not normally applicable.
Sending newsletters, fundraising messages or information about services and events	Consent or legitimate interests where PECR permits an applicable soft opt-in. Every electronic marketing message will include an easy way to opt out.	Not normally applicable. We do not use health or therapeutic information to target marketing.



Purpose	Typical Article 6 lawful basis	Additional condition where relevant
Operating and securing our website, using essential cookies, measuring our audience and displaying advertising	Legitimate interests for website security and strictly necessary technologies. Consent is used for non-essential cookies and similar technologies.	Not normally applicable.

Where we rely on legitimate interests

Where we rely on legitimate interests, we consider:

- the purpose for which we want to use the information;
- whether using the information is necessary;
- the possible impact on the person;
- whether the person would reasonably expect the information to be used in this way; and
- whether additional protections are needed.

We pay particular attention where children or sensitive information are involved.

You may object to processing based on legitimate interests. We will stop unless we have compelling legitimate grounds to continue or the information is required for legal claims.

Where we rely on consent

Consent is not always our lawful basis.

Where we rely on consent, you may withdraw it at any time. Withdrawing consent does not make our earlier use of the information unlawful. It may not require us to delete information that we must retain under another lawful basis.

6. Children and young people

Children's information deserves particular protection.



We only use children's information where it is necessary and proportionate. We use privacy-protective settings and consider:

- the child's best interests;
- their age and understanding;
- their communication needs;
- their evolving capacity;
- the nature of the service; and
- any safeguarding concerns.

We explain our use of information in language the child or young person can understand and involve them in decisions where appropriate.

Depending on the child's age, understanding, the service and the legal basis, we may seek:

- agreement from the child or young person;
- consent or authority from a person with parental responsibility; or
- agreement from both.

A parent's access to a child's information is not automatic in every circumstance. We must consider the child's rights, understanding, confidentiality, safeguarding needs and the law.

We may keep some information confidential from a parent or carer where this is appropriate and lawful.

We may share information without agreement if we reasonably believe that a child or another person is at risk, if the law requires us to share it, or where another lawful safeguarding basis applies.

We will normally explain this unless doing so would increase the risk of harm or would be unlawful.

7. Safeguarding and confidentiality



Our services are confidential within professional, safeguarding and legal limits.

Staff and relevant volunteers only have access to information they need for their role. They are subject to confidentiality, safeguarding and information-security requirements.

We may share relevant and proportionate information with:

- safeguarding partners;
- emergency services;
- the police;
- children's or adult social care;
- health professionals;
- schools;
- commissioners;
- courts and regulators; or
- other organisations involved in protecting or supporting someone.

We may do this where it is necessary to:

- protect a child or another person;
- meet a legal duty;
- respond to a court order;
- establish, exercise or defend legal rights;
- prevent or detect serious harm or crime; or
- fulfil another lawful safeguarding purpose.

We document the reason for the decision and share no more information than is needed.

8. Website, bookings, payments and cookies



Our website, booking, payment, email and analytics providers may process information for us.

Their privacy notices may also apply where they act as independent controllers, for example when providing you with their own account or payment service.

Cookies and similar technologies

Strictly necessary cookies and similar technologies may be used without consent where they are essential to:

- provide a service you have requested;
- keep the website secure;
- process a booking or payment; or
- remember a privacy choice.

We ask for consent before using non-essential:

- analytics cookies;
- advertising cookies;
- social-media cookies; or
- similar tracking technologies.

You can accept, reject or change your non-essential cookie choices through our website's cookie controls.

Refusing non-essential cookies should not prevent you from accessing the website's core functions.

Our website should also provide a current cookie list showing:

- the name of each cookie or technology;
- the provider;
- its purpose; and
- how long it remains on your device.



9. Microsoft Teams meetings, webinars and events

We use Microsoft Teams to deliver some appointments, training sessions, webinars and live events.

Microsoft generally acts as our data processor when providing the Teams service. Microsoft's own privacy terms may also apply to information it processes for its independent purposes or through your own Microsoft account.

Registration and attendance

When you register for or attend an event, we may collect:

- your name;
- your email address;
- your organisation or role;
- booking information;
- access requirements; and
- your marketing preferences.

Microsoft Teams may generate technical and attendance information, including:

- your display name;
- your joining and leaving times;
- the length of time you attended;
- your email address or Microsoft account identifier;
- your IP address; and
- device or connection information.

Event organisers and authorised Bridge the Gap staff may be able to access attendance reports.

What other attendees may see

Depending on the event settings and how you join, other attendees may see:



- your display name;
- your profile image;
- your camera image;
- anything you say;
- reactions;
- poll responses;
- content you share; and
- messages you post in a meeting chat or Q&A.

Please use a suitable display name and keep your camera and microphone switched off when you do not wish to be seen or heard.

Please do not post confidential or sensitive information about yourself, a child or anyone else in a shared chat or Q&A space.

Recordings, captions and transcripts

We do not treat every Microsoft Teams event as recorded by default.

If we intend to record or transcribe an event, we will tell you:

- within the booking information or before the event;
- before recording or transcription begins;
- what the recording is intended to capture;
- who will be able to access it;
- whether it will be published or shared privately; and
- how long it will be kept.

Microsoft Teams will normally also display an on-screen notification when recording or transcription begins.

A recording may capture:



- the presenter;
- shared presentations and materials;
- attendee display names and profile images;
- voices and camera images;
- chat contributions;
- questions;
- reactions; and
- information visible on a shared screen.

Live captions may process speech even where a transcript is not permanently retained.

Our safer webinar approach

For webinars that are intended to be made available as a replay, we aim to record the presenter and presentation only.

Where the event format allows:

- attendee cameras and microphones will be disabled;
- questions will be managed through a moderated or anonymous Q&A function;
- we will pause or stop the recording before sensitive discussion or personal questions;
- attendees will be reminded not to share identifying or confidential information;
- unintended attendee information will be edited or removed before wider publication where reasonably possible; and
- access to recordings will be limited to the intended audience.

If attendee participation may be captured, we will explain this before the event.

Where practicable, you may be able to:

- keep your camera and microphone switched off;



- avoid contributing to the shared chat;
- submit a question privately;
- use an anonymous Q&A option; or
- contact us to request another way of accessing the information.

If active participation is essential to the event, we will explain this before you book.

Please do not make your own recording, screenshot or transcript of an event containing other people unless Bridge the Gap and everyone affected have expressly agreed and it is lawful to do so.

Event follow-up and marketing

We may send you:

- joining instructions;
- reminders;
- changes to the event;
- resources;
- feedback requests;
- attendance certificates; and
- other essential event information.

These messages relate to the event you requested and are not necessarily marketing.

We will only send wider marketing where we have your consent or another basis permitted by PECR.

You can unsubscribe from marketing at any time without affecting essential event messages.

10. Who we share information with

We only share personal information where it is necessary and proportionate.

Recipients may include:



- authorised employees, sessional workers, students, volunteers and professional supervisors who need the information for their role;
- parents, carers or people with parental responsibility, taking account of the child or young person's rights and safeguarding needs;
- schools, commissioners, funders, local authorities, NHS bodies, health and social care professionals and other agencies involved in delivering the service;
- safeguarding partners, emergency services, police, courts, regulators and other public authorities where required or permitted by law;
- professional advisers, insurers, auditors, accountants and legal representatives;
- organisations supporting our website, bookings, payments, email, surveys, document storage, case management, IT security, backup and Microsoft 365 or Teams; and
- a successor organisation if our activities are restructured or transferred, subject to appropriate confidentiality and data-protection safeguards.

We do not sell personal information.

We require organisations acting as our processors to:

- handle information only on our instructions;
- keep it secure;
- maintain confidentiality;
- help us meet our data-protection duties; and
- delete or return the information when the arrangement ends, where appropriate.

11. International transfers

Some technology providers may store or access information outside the UK.

Before making a restricted international transfer, we use an appropriate safeguard recognised by UK law.

This may include:



- UK adequacy regulations;
- the UK International Data Transfer Agreement;
- the UK Addendum to approved standard contractual clauses; or
- another safeguard permitted under UK data-protection law.

We complete a transfer risk assessment where one is required.

We may rely on a specific legal exception in limited circumstances where it applies.

You can contact us for more information about the safeguards relevant to your personal information.

12. How long we keep information

We keep information only for as long as it is needed for:

- the purpose for which it was collected;
- safeguarding and continuity of support;
- legal or regulatory requirements;
- contractual requirements;
- insurance;
- responding to complaints; and
- establishing or defending legal claims.

The appropriate period depends on:

- the person's age;
- the nature of the service;
- the sensitivity of the information;
- safeguarding considerations;
- commissioning requirements;
- professional guidance;



- insurance requirements; and
- whether there is an ongoing complaint, investigation or legal claim.

At the end of the relevant period, we securely delete or anonymise the information unless a legal hold, safeguarding reason or other lawful requirement means we need to keep it for longer.

Record type	Retention position
Enquiries that do not become a service	Normally kept for up to 12 months after the last meaningful contact, unless the information is needed for a complaint, safeguarding matter or legal claim.
Child, young person and family support records	Kept for the period set out in our approved clinical and service retention schedule, taking account of the child's age when support ends, safeguarding, insurance and commissioning requirements. [INSERT APPROVED PERIOD]
Safeguarding records	Kept separately and for the period required by our safeguarding retention schedule and relevant guidance. [INSERT APPROVED PERIOD OR CRITERIA]
Adult coaching or counselling records	Kept for the period set out in our approved service retention schedule and in accordance with professional, insurance and legal requirements. [INSERT APPROVED PERIOD]
Bookings, invoices and financial records	Normally kept for six years after the end of the relevant financial year, or longer where tax or legal rules require it.
Complaints and incident records	Normally kept for six years after the complaint or incident is closed, or longer where the person's age, safeguarding, insurance or legal considerations require it.



Record type	Retention position
Event registration and attendance reports	Normally kept for 12 months after the event, unless needed for certification, contractual reporting, safeguarding, a complaint or a legal claim.
Microsoft Teams chat and Q&A	Normally deleted or anonymised within 90 days after event follow-up is complete, unless relevant information has been incorporated into another record for a valid reason.
Microsoft Teams recordings and transcripts	A private event replay is normally available for no more than 90 days. A recording deliberately retained as an ongoing training resource is reviewed at least annually and removed when no longer needed. Individual booking information will explain where a different period applies.
Marketing records	Kept until you unsubscribe or object. We then retain the minimum suppression record needed to ensure we respect your choice.
Cookie and analytics information	Kept for the periods stated in our current cookie list and according to your consent choices.

13. Security

We use proportionate technical and organisational measures designed to protect personal information from:

- loss;
- misuse;
- alteration;
- unauthorised access; and
- unauthorised disclosure.

Our measures include, where appropriate:



- role-based access;
- confidentiality requirements;
- secure systems;
- passwords and access controls;
- multi-factor authentication;
- device and account management;
- backups;
- staff and volunteer training;
- supplier checks;
- secure disposal; and
- procedures for responding to information-security incidents.

No internet or storage system can be guaranteed to be completely secure.

If a personal data breach is likely to create a risk to people, we will notify the Information Commissioner's Office where required.

If the breach is likely to create a high risk, we will also notify affected people without undue delay where required.

14. Your data-protection rights

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

- be informed about how we use your personal information;
- ask for access to your personal information and related supplementary information;
- ask us to correct inaccurate or incomplete information;
- ask us to erase information in certain circumstances;
- ask us to restrict how we use information in certain circumstances;



- object to processing based on legitimate interests or public task;
- object at any time to direct marketing;
- receive certain information in a portable format where the right applies;
- withdraw consent at any time where we rely on consent; and
- not be subject to a decision based solely on automated processing that has a legal or similarly significant effect, except where the law permits this and appropriate safeguards apply.

These rights are not absolute. The rights available will depend on the information, circumstances and lawful basis.

We may need to verify your identity and authority before acting on a request.

We normally respond without undue delay and within one month. The law allows this period to be extended in certain circumstances.

We may also pause the response period where we reasonably need further information to identify the information or understand the request.

We do not normally charge a fee. The law allows us to charge a reasonable fee or refuse to act in limited circumstances, including where a request is manifestly unfounded or excessive.

Your right to object

You have an absolute right to object to your personal information being used for direct marketing.

You may also object where we rely on legitimate interests or public task.

Please tell us what you object to and why. We will consider your circumstances and explain our decision.

To exercise one of your rights, contact:

Email: nikkiwebster@jwbridgethegap.com

Post: Bridge the Gap Child Mental Health C.I.C., 10/11 St. Mary's Gate, Derby DE1 3JR



A child or young person may exercise their own data-protection rights if they have sufficient understanding.

A parent, carer or representative may make a request on someone's behalf, but we may need evidence of their authority. We must still consider the child or young person's rights, understanding and confidentiality.

15. Complaints

If you are concerned about how we use personal information, please contact us at:

Email: nikkiwebster@jwbridgethegap.com

Post: Bridge the Gap Child Mental Health C.I.C., 10/11 St. Mary's Gate, Derby DE1 3JR

You may make a complaint electronically or in writing.

Please tell us:

- what happened;
- which information or service is involved;
- the outcome you would like; and
- how we can contact you.

We will acknowledge a data-protection complaint within 30 days.

We will investigate the complaint without undue delay, keep you appropriately informed and tell you the outcome and any action taken.

If we cannot complete the investigation within 30 days, we will provide a progress update and continue to update you at appropriate intervals.

You may also complain to the Information Commissioner's Office.

We would welcome the opportunity to resolve the matter first, but you do not have to contact us before approaching the ICO.

Visit: <https://ico.org.uk/make-a-complaint/>

Telephone: 0303 123 1113



You may also seek a judicial remedy where applicable.

16. Links and third-party services

Our website or communications may include links to services that we do not control.

The privacy notices of those services will apply to their own collection and use of personal information.

We are not responsible for another controller's privacy practices, although we assess providers that process information on our behalf.

17. Changes to this notice

We review this privacy notice regularly and update it when our services, technology or legal duties change.

We will publish the current version on our website and show the date it was last updated.

If a change materially affects how we use personal information, we will take reasonable steps to bring it to the attention of affected people.

We will seek new consent where consent is required.

18. Contact us

For privacy questions, data-protection rights requests or complaints, please contact:

Contact method	Details
Email	nikkiwebster@jwbridgethegap.com
Post	Bridge the Gap Child Mental Health C.I.C., 10/11 St. Mary's Gate, Derby DE1 3JR
Telephone	01332 600827