



Counselling in Prisons Network

Privacy Policy

Policy Name	Privacy Policy
Date published	22/10/2026
Date Approved by Board	13/10/2026
Renewal Schedule	12 monthly
Date of next Renewal	22/10/2027

Introduction and general terms

The Counselling in Prisons Network (CiPN) promises to take care of your personal data.

We commit to protecting any personal information we obtain about you, whether you are a financial supporter, client, volunteer, partner or campaigner.

This Privacy Policy sets out how and why we obtain, use and protect personal information if you interact with us in one of these roles.

In the event that you work with us in another way – for instance, enrol in a specific event, program, apply for a job, or are a member of staff, there may be a separate Privacy Policy which describes how we use that data.

Who we are

CiPN is a registered charity in England and Wales (charity number 1159028)

CiPN's registered address is 20 Candys Lane, Corfe Mullen, Wimborne, Dorset, BH21 2EL

CiPN can be contacted using the email address: contact@cipn.org.uk

This Privacy Policy relates to information which is obtained by CiPN and for which CiPN is the Data Controller. That is to say, data for which CiPN sets the purpose of the use as well as how this data will be used.

CiPN's Purpose

The CiPN was founded in 2007 primarily to provide a professional home for counsellors and therapists working in the criminal justice system. Our core vision is to pool expertise and best practice, to identify research agendas and develop excellence in working with offenders, with a view to pushing back the boundaries. We aim to develop and agree best practice for the engagement, management and treatment of female and male offenders who are resident in the custodial setting.

What information we collect, use, and why

We collect or use the following information to provide services, including third party referrals:

- Names and contact details
- Gender
- Pronoun preferences
- Addresses
- Date of birth
- Emergency contact details

- Photographs or video recordings
- Service use history
- Right to work information
- Information about work, home and living conditions
- Information about support requirements
- Criminal offence data
- Website user information (including user journeys and cookie tracking)
- Information relating to compliments or complaints

We also collect or use the following special category information:

- Racial or ethnic origin
- Religious or philosophical beliefs
- Health information

Our Legal Basis for Processing Special Category Data (DUAA 2025–26)

CiPN only processes special category data where it is strictly necessary and where both a lawful basis under Article 6 and a valid condition under Article 9 of UK GDPR apply. The Data (Use and Access) Act 2025 strengthens these requirements, particularly in relation to safeguarding and custodial environments.

Depending on the context, CiPN may rely on the following conditions for processing special category data:

- **Explicit consent** — where you have clearly agreed to the processing (for example, sharing health information so we can support your involvement in CiPN activities).
- **Substantial public interest** — including safeguarding, preventing or detecting unlawful acts, equality monitoring, and protecting individuals at risk.
- **Health or social care purposes** — where information is needed to support wellbeing, safety, or access to therapeutic or professional services.
- **Recognised Legitimate Interests (DUAA 2025–26)** — where processing is necessary for safeguarding, crime prevention, responding to ethical membership bodies, or protecting individuals within custodial environments.

CiPN ensures that special category data is handled proportionately, stored securely, accessed only by authorised individuals, and deleted when no longer required. We do not use special category data for marketing, profiling, or fundraising.

We collect or use the following information to receive donations or funding and organise fundraising activities:

- Names and contact details
- Addresses
- Payment or banking details

- Donation history
- Tax payer information (for Gift Aid purposes)
- Gifts in wills

We collect or use the following personal information for the prevention, detection, investigation or prosecution of crimes:

- Names and contact information
- Criminal offence data (including Disclosure Barring Service (DBS), Access NI or Disclosure Scotland checks)
- Witness statements and contact details
- Information required for Reporting to comply with requests from a member's ethical body (i.e. BACP, UKCP, etc)

We collect or use the following personal information for service updates or marketing purposes:

- Names and contact details
- Addresses
- Marketing preferences
- Recorded images, such as photos or videos
- Donation history
- Records of consent, where appropriate

We collect or use the following personal information for research or archiving purposes:

- Names and contact details

We also collect or use the following special category information for research or archiving purposes. This information is subject to additional protection due to its sensitive nature:

- Racial or ethnic origin
- Religious or philosophical beliefs
- Health information

We collect or use the following personal information for dealing with queries, complaints or claims:

- Names and contact details
- Address
- Payment details
- Purchase or service history
- Witness statements and contact details
- Relevant information from previous investigations
- Customer or client accounts and records
- Information relating to health and safety (including incident investigation details and reports and accident book records)
- Correspondence

- Information required for reporting to comply with requests from a member's ethical body (i.e. BACP, UKCP, etc)

We also collect or use the following special category information for dealing with queries, complaints or claims. This information is subject to additional protection due to its sensitive nature:

- Racial or ethnic origin
- Religious or philosophical beliefs
- Health information

These reasons are underpinned by a “lawful basis” under GDPR. There is a list of possible [lawful bases](#) in the UK GDPR. You can find out more about lawful bases on the ICO’s website. We outline in the next section what these are for our main activities.

Explaining the legal bases we rely on

The law on data protection sets out several different reasons for organisations to collect and process your personal data: When collecting your personal data, we will always make clear to you which data is necessary for a particular purpose. CiPN relies on the following legal bases in our marketing activities:

Consent

Wherever possible, we will ask for your consent to send you marketing information. We will do this through a clear statement of what you will receive and allow you to select only those channels that you wish to hear from us by.

For example, if you donate to CiPN, you will be asked whether you would like us to keep in touch about our research, fundraising activities, and events. You will also be asked which channel(s) of communication you would like us to use (with a choice of email, post and telephone being offered).

Legitimate interest

In specific situations, we process your data to pursue our legitimate interests in ways which might reasonably be expected and which do not materially impact your rights, freedom or interests. CiPN’s use of legitimate interest includes the following:

- Sending direct marketing information by post, to keep our supporters and members updated on CiPN’s research, fundraising activities, and events. We will only do this where we have reason to believe that this information will be of interest. We make it easy for you to opt out. You can opt out at any time by contacting us via the contact details at the beginning of this policy.
- Where you have interacted with CiPN in any form (such as contacted us about policies, attended events, etc) we will email you to tell you about other relevant offers. All such emails will include a simple opt out mechanism.

- If you have opted in to CiPN's communications we may use your details to link to your account on Facebook or other social media site to serve you CiPN content.
- We analyse your previous support of CiPN to offer relevant ways of supporting CiPN in the future.
- To help identify businesses who may wish to support CiPN, we send emails to individuals where relevant to their job, for instance people working in the Criminal Justice System or related organisations.

For activities other than marketing, we may rely on different legal bases:

Legal compliance

If the law requires us to, we may need to collect and process your data. For example, where you sign up to the Gift Aid scheme, we will process your data for the purposes of submitting a Gift Aid claim to HMRC.

Public Interest

In limited situations we may use data in the public interest. It is likely to be in the public interest to collect data to prevent crime or dishonesty, ensure that we are fair in our practices by carrying out equality and diversity monitoring, or safeguard the wellbeing of people with whom we work.

Recognised Legitimate Interests (DUAA 2025–26)

In certain circumstances, CiPN may process personal data under the lawful basis of Recognised Legitimate Interests, as defined in the Data (Use and Access) Act 2025. This basis applies where processing is necessary for specific activities that Parliament has identified as being in the public interest, including safeguarding, crime prevention, responding to requests from public authorities, and preventing dishonesty or harm.

CiPN may rely on this lawful basis when:

- identifying or responding to safeguarding concerns
- preventing or detecting crime or dishonesty
- complying with requests from ethical membership bodies (such as BACP or UKCP)
- supporting safety and wellbeing within custodial environments
- sharing information with relevant authorities where required to protect individuals or the public

Where we rely on Recognised Legitimate Interests, we ensure that processing is necessary, proportionate, and carried out with appropriate safeguards.

When and why we will send you personalised marketing communications

CiPN will only contact you for marketing purposes – for example keep you up to date on our work or let you know of ways in which you can support that work – where we have your consent or we are otherwise allowed to do so (see the next section below).

We will make it easy for you to tell us if you would like to receive marketing communications from us and hear more about our work and the ways in which you would like to receive this information (post, email, and phone). We will ask you to reconfirm your consent if we have evidence that suggests you may no longer wish to hear from us.

We will never send you marketing material if you have told us that you do not wish to receive it. There are a variety of ways you can do this (see the sections below on opting out of controlling how we contact you).

Other circumstances in which you may receive marketing information from CiPN

Legitimate Interest

We may send you marketing communications by direct mail where you are a regular supporter or member and we have evidence that you do not object to receiving marketing material through the post.

We will not use legitimate interest if you have opted out of direct mail whether direct to CiPN or by registering with the Mailing Preference Service (MPS) or the Fundraising Preference Service (FPS).

Soft opt in

This allows organisations to send marketing communications by email and SMS to individuals who have previously availed of our similar services, provided they were given the opportunity to opt out at the time. In CiPN's case, this allows us to send marketing emails and SMS to previous attendees of our events. We apply a 24-month time limit, and only communicate on this basis where you have attended an event within this period. We will not use the soft opt in option if you have opted out of receiving email and/or SMS, whether direct to CiPN or via the Fundraising Preference Service.

When we collect information about you

CiPN may collect your personal data in the following circumstances:

1. When you give it to us DIRECTLY

You may give us your personal data directly when you make a donation, sign up for one of our events, take part in a campaigning action, volunteer with us, or when you communicate with us.

2. When you give it to us INDIRECTLY

You may give us your information indirectly when you sign up to events, contribute to CiPN via fundraising sites like JustGiving or Virgin Money Giving, or participate in a campaigning action with a partner. These independent third parties will pass your data to CiPN where you have indicated that you wish to support CiPN and have given your consent or it is a necessary part of completing a contract with you.

Sometimes your personal data is collected by an organisation working on our behalf (for example a professional fundraising agency) but as they are acting on our behalf we are the “data controller” and responsible for the security and proper processing of that data.

3. When you access CiPN’s Social Media

We might also obtain your personal data through your use of social media such as Facebook, WhatsApp, Twitter or LinkedIn, depending on your settings or the privacy policies of these social media and messaging services. To change your settings on these services, please refer to their privacy notices, which will tell you how to do this.

4. When the information is publicly available

We might also obtain personal data about individuals who may be interested in giving major gifts to charities or organisations like CiPN. In this scenario, CiPN may seek to find out more about these individuals, their interests and motivations for giving through publicly available information. This information may include newspaper or other media coverage, open postings on social media sites such as LinkedIn, and data from Companies House. CiPN will not retain publicly available data relating to major donors without their consent, which will be sought at the earliest practical opportunity. Where we decide not to make contact, we will delete all personal data obtained, other than basic contact details, to which we will apply a suppression flag to ensure we do not make contact in the future.

We may also gather information if your activities relate to our work – for instance, if you are a public figure such as a Member of Parliament or you represent an organisation which we work with or which is related to one of our campaigns we may gather information about you in order to inform our campaigning and make decisions – for instance, whether we engage with you to seek your support for our work, ask your constituents to write to you, or choose to work you in another way.

5. When we use cookies

Cookies and Tracking Technologies (DUAA 2025–26)

Cookies are a useful way for us to understand how supporters use our website. When you visit the CiPN website, we may collect information from your computer or other device, such as a smartphone or tablet, through cookies and similar

technologies (including pixels, tags and local storage). These tools are created by your web browser when you visit our website, and each time you return, your browser will send the cookie file back to our server.

Cookies help improve your experience of using our website by remembering your preference settings, presenting information likely to be most relevant to you, and measuring how you use the site so that we can continuously improve it. Some cookies may also be used to show you relevant CiPN content on social media platforms such as Facebook; these are known as “retargeting” or “advertising” cookies.

In line with the Data (Use and Access) Act 2025, certain cookies that are used solely for measuring website performance or producing aggregate statistics may be set without consent, provided they do not identify you or track your activity across other websites. Other cookies, including those used for personalisation, advertising, or non-essential analytics, will only be set with your consent.

You can manage your cookie preferences at any time through your browser settings or via the controls provided on our website. For detailed information about the types of cookies we use, how long they last, and how you can control them, please refer to CiPN’s cookie policy. If you visit our website as an anonymous visitor (for example, by switching off cookies), CiPN may still collect certain limited information from your browser, such as your IP address (a number that can uniquely identify a computer or other internet device).

The CiPN website contains hyperlinks to websites owned and operated by other organisations. These include media organisations (such as the BBC), research bodies, charities, and CiPN affiliates in other countries. These third-party websites have their own privacy and cookie policies, which we encourage you to review. They govern the use of any personal information you submit or which is collected by cookies while visiting those websites. CiPN cannot accept responsibility or liability for the privacy practices of such third-party websites, and your use of them is at your own risk.

What information might CiPN collect about you?

We only collect personal data relevant to the type of transactions or interaction you have with CiPN. Whatever your interaction with us this information will be minimal and linked to the purpose for which we need it. For example, when you contact CiPN to make a donation, take a campaign action, or sign up to any of CiPN’s activities or online content or you telephone, email, write to or text CiPN, or engage with CiPN via social media channels, we may receive and retain personal information.

In these cases we are likely to process details such as your name, email address, postal address, telephone or mobile number, bank account details to process donations and whether or not you are a tax payer so that we can claim Gift Aid.

If you participate in an event we may (with your permission) take your photograph or video, or interview you. If you participate in market research, we may ask you questions regarding your experience with us, or other survey questions relating to your experience.

If you are a campaigner or work with our campaigns team, we may collect information such as correspondence with you regarding campaigning, details of your background and activities with us or relating to the issue, the events you attend, or how we would like to work with you.

Where we gather information about you which is publicly available – for instance as a major donor or your views on our campaigning activity – this may include your name, contact details, views and positions you have expressed, and details regarding your circumstances- for instance which political roles you hold or what your background is.

Sensitive Personal Data

We only collect “sensitive personal data” about our supporters, e.g. health status, where there is a clear and specific reason for doing so.

We collect this data where we need it to ensure that we provide appropriate facilities or support to enable you to participate in the event or carry out your role. Clear notices will be provided on application forms so that it is clear what information we need and why we need it. In certain circumstances we need to obtain information about criminal convictions (where these are unspent) in order to check that it is appropriate for you to undertake the role. This may also include seeking a DBS check.

If you apply for a role with us, we may collect this data for equality monitoring. Further details regarding this are outlined in our recruitment privacy policy.

Rarely, we may collect this data for the prevention of crime or dishonesty, to safeguard those with whom we work, or for another reason which is in the public interest. Where we do this we will do it carefully and in accordance with applicable laws.

Should you support CiPN in a substantial way, we may provide an account manager to help you tailor your relationship to suit your interests. If this is the case we may collect sensitive personal data where relevant to our relationship, such as your political or religious views. Should you disclose information to us about your health or your family, this may also be recorded, so that we can communicate with you in a considerate and appropriate manner.

All sensitive personal data is stored on a secure database, to which only a limited number of relevant staff have access. It is deleted when no longer relevant, is never shared with third parties, and is available to you at any point should you wish to see it.

How will CiPN use your personal data?

CiPN will use your personal information for the following purposes:

1. For administrative reasons, including:

- “service administration”, which means that CiPN may contact you for reasons related to administering any donations you have made, your tax status with regard to Gift Aid if claimed, the completion of commercial or other transactions you have entered into with CiPN or the activity or online content you have signed up for;
- to confirm receipt of donations (unless you have asked us not to do this), and to say thank you and provide details of how your donation might be used. for example if you donate via text you will receive a “bounce back” text message;
- in relation to correspondence you have entered into with us whether by letter, email, text, social media, message board or any other means, and to contact you about any content you provide;
- for internal record keeping so as to keep a record of your relationship with us;
- to fulfil contracts you have entered into with CiPN;
- to provide logistical and fundraising information to people who are taking part in a fundraising event in aid of CiPN;
- to communicate with CiPN volunteers – to support you in your designated role or administer that role and our organisation;
- to keep your data up to date – for instance we use the Royal Mail’s data on postal address changes to ensure that we can maintain contact with you where we believe you are happy to be contacted by post, we also use services which notify us of the recently deceased to avoid any distress that continued communications would cause;
- to implement any instructions you give us to with regard to withdrawing consent to send marketing information or informing us through the Fundraising Preference Service that you do not wish to receive any marketing information;
- to use IP addresses to identify the location of users, to block disruptive use and to establish the number of visits from different countries;
- to protect our staff and those with whom we work, or to prevent crime and dishonesty. This will involve frequent fraud and anti-terrorism screening of employees and partners. This may also include complying with requests from ethical bodies such as BACP, UKCP, and other such bodies.

2. For marketing and fundraising reasons

For more information on this see the section above: When and why we will send you personalised marketing communications.

3. For market research

- to invite you to participate in surveys or research about CiPN or our work (participation is always voluntary);

- to analyse and improve the activities and content offered by the CiPN website to provide you with the most user-friendly navigation experience. We may also use and disclose information in aggregate (so that no individuals are identified) for marketing and strategic development purposes.

Will CiPN share your personal information with anyone else?

We will only use your information within CiPN for the purposes for which it was obtained. CiPN will not, under any circumstances, share or sell your personal data with any third party for their own marketing purposes, and you will not receive marketing from any other companies, charities or other organisations as a result of giving your details to us.

CiPN's suppliers

We may need to share your information with service providers who help us to deliver our projects, fundraising activities, events and appeals, for instance through handling responses to our emergency appeals. These “data processors” will only act under our instruction and are subject to pre-contract scrutiny and contractual obligations containing strict data protection clauses. We do not allow these organisations to use your data for their own purposes or disclose it to other third parties without our consent and we will take all reasonable care to ensure that they keep your data secure.

Facebook and other social media sites

We may also use your email address and phone number to match to your account on Facebook or other social media sites in order to show you CiPN content while using these services. We only do this where you have opted in to marketing emails or phone calls and we keep your data secure by encrypting it. No data we hold about you is retained by the third party.

In addition, we may also use your email address and phone number to link to Facebook or other social media sites in order to identify other users of these sites whom we believe would be interested in CiPN, and we may then show them CiPN content. No data we hold about you is retained by the third party.

There are two ways to prevent this use of your data, you can either update your preferences at CiPN by opting out of the relevant channel of communication or you can do this via the social media site.

Updating your preferences with CiPN will not guarantee that you never see CiPN content on social media, since the social media site may select you based on other criteria and without your data having been provided by CiPN.

Current and former CiPN employees

When you leave CiPN, CiPN may process your data to respond to requests for employment references.

Where legally required

International Transfers (DUAA 2025–26)

CiPN may transfer personal data outside the United Kingdom where this is necessary for our operations or for the services we use. When we do so, we ensure that appropriate safeguards are in place to protect your information.

In line with the Data (Use and Access) Act 2025, any international transfer is assessed using the UK data protection test, which considers whether the destination country provides an adequate level of protection for personal data. Where required, we use approved safeguards such as the UK International Data Transfer Agreement (IDTA) or the UK Addendum to the EU Standard Contractual Clauses.

We will only transfer personal data internationally where we are satisfied that your information will be protected to UK GDPR standards.

Where ethically required

CiPN may share your data with relevant ethical membership bodies (such as BACP, UKCP, etc) in order to comply with investigations, or to comply with our ethical requirements under such bodies.

How long will CiPN keep your personal information?

We will hold your personal information on our systems for as long as is necessary for the relevant activity, for example we will keep a record of donations subject to gift aid for at least seven years to comply with HMRC rules.

If you request that we stop sending you marketing materials we will keep a record of your contact details and appropriate information to enable us to comply with your request not to be contacted by us.

Legacy income is vital to the running of the charity. We may keep data you provide to us indefinitely, to carry out legacy administration and communicate effectively with the families of people leaving us legacies. This also enables us to identify and analyse the source of legacy income we receive.

Where you contribute material to us, e.g. user generated content or in response to a particular campaign, we will only keep your content for as long as is reasonably required for the purpose(s) for which it was submitted unless otherwise stated at the point of generation.

How to control what we send you or request we update your personal information

The accuracy of your information is really important to us. We want to ensure that we are able to communicate with you in ways that you are happy with, and to provide you with information that is of interest.

If you wish to change how we communicate with you, or update the information we hold, then please contact us using the details at the beginning of this policy.

How long will it take for these changes to be effective?

We endeavour to action any requests from you as soon as possible. In some cases this can take up to 28 days, or even longer if marketing campaigns have been pre-arranged.

How CiPN keeps your data safe

We ensure that there are appropriate technical controls in place to protect your personal details. For example our online forms are always encrypted and our network is protected and routinely monitored.

We undertake regular reviews of who has access to information that we hold to ensure that your information is only accessible by appropriately trained staff, volunteers and contractors.

We use external companies to collect or process personal data on our behalf. We do comprehensive checks on these companies before we work with them, and put a contract in place that sets out our expectations and requirements, especially regarding how they manage the personal data they collect on our behalf, or have access to. We have a robust partner monitoring framework to ensure these contractual obligations are met. These organisations – referred to as “Data Processors” also have legal liability for the way in which your data is used, providing you with additional protection.

Children’s Data Protection (DUAA 2025–26)

CiPN recognises that children’s personal data requires a higher level of protection, in line with the Data (Use and Access) Act 2025. Where we process information relating to children or young people, whether directly or indirectly through safeguarding concerns, custodial settings, or professional activities, we apply additional safeguards to ensure their rights and wellbeing are protected.

We only collect the minimum amount of children’s data necessary for the relevant purpose, and we ensure that any processing is fair, proportionate and carried out with appropriate security measures. Access to children’s data is strictly limited to authorised individuals who require it for safeguarding, professional, or legal reasons.

Where children’s data is processed, we take steps to ensure:

- enhanced confidentiality and restricted access

- clear justification for why the data is needed
- careful consideration of risks to the child
- compliance with safeguarding legislation and professional ethical standards
- secure storage and timely deletion when no longer required

We do not use children's data for marketing, profiling, or fundraising. Any processing of children's data is carried out with their best interests in mind and in accordance with applicable law, including UK GDPR, DUAA 2025–26, and safeguarding requirements.

Your rights over your personal data

You have a variety of rights in respect of your data, including the rights to see, update, restrict, object to the use of or withdraw use of your data. In particular, depending upon why we hold your data, you may have the right to request:

- Access to the personal data we hold about you, including how we first obtained your details, free of charge in most cases (this is known as a 'Subject Access Request').
- The correction of your personal data when incorrect, out of date or incomplete.
- That we stop using your personal data for direct marketing (either through specific channels, or all channels).
- That we delete your personal data from our systems (this is known as the "Right to be Forgotten").
- That we no longer process your data automatically to decide whether particular marketing activities are likely to be of interest, or suggest an appropriate donation level based on your previous donation history. This is known as profiling, and helps us to ensure that our marketing is relevant and appropriate.

You can contact us to request to exercise these rights at any time via the contact details at the top of this policy.

Opting out of Direct marketing

You have the right to stop the use of your personal data for direct marketing activity through all channels, or selected channels. We will always comply with your request as soon as we can.

Where we are sending you direct marketing on the basis of our legitimate interest, you can also ask us to stop. In the case of postal marketing sent on this basis, we will always comply with your request to opt out. Similarly, where we send email marketing on a soft opt in basis we will also comply with all requests to opt out as soon as we can.

Right to be Forgotten

Upon request we will delete your personal data from our systems, to the extent that we are permitted to by law or regulatory guidelines. For instance under HMRC rules we are required to retain financial data for 7 years for audit purposes, and so will not be able to delete donation details until this time period has elapsed.

Opting out of profiling

Upon request we will cease using your personal data to decide whether you would be interested in particular updates and other marketing. Such requests may lead to you not hearing from us in future.

Automated Decision-Making and Profiling (DUAA 2025–26)

CiPN does not make any decisions about individuals that have legal or similarly significant effects using solely automated processing. All decisions relating to safeguarding, membership, volunteering, employment, complaints, or service access involve human review.

We may use limited profiling to tailor our communications, for example by analysing previous interactions or donation history to identify information that may be relevant to you. This profiling does not have legal or significant effects and is carried out in accordance with UK GDPR and the Data (Use and Access) Act 2025.

Under DUAA, you have the right to:

- request human involvement in any decision made using automated processes
- challenge or express concerns about profiling
- receive an explanation of how any automated process works
- object to profiling used for marketing or engagement purposes

We do not use automated decision-making involving special category data or criminal offence data. Any processing of such data is carried out with appropriate safeguards and human oversight.

Subject Access Requests (updated for DUAA 2025–26)

You have the right to request a copy of the personal information we hold about you. We will respond to your request within one month of verifying your identity, in line with the Data (Use and Access) Act 2025. If we need additional information to confirm your identity, we may pause (“stop the clock”) until verification is complete.

We will carry out a reasonable and proportionate search for the information we hold. If your request is complex or involves a large volume of data, we may extend the

response period by up to two further months. If this is the case, we will inform you as soon as possible.

To protect the confidentiality of your information, we will ask you to verify your identity before releasing any personal data. If you authorise a third party to act on your behalf, we may request evidence of this authorisation.

Checking your identity

To protect the confidentiality of your information, we will ask you to verify your identity before proceeding with any request you make under this Privacy Notice. If you have authorised a third party to submit a request on your behalf, we may ask them to prove they have your permission to act.

How to raise a data protection concern or complaint

If you have any questions about this policy, would like to update your personal information, or wish to raise a concern about how CiPN has handled your data, you can contact us using the details at the top of this policy.

We will acknowledge all data protection complaints within 30 days, in line with the Data (Use and Access) Act 2025, and we will provide a full response without undue delay. We may request additional information if needed to verify your identity or understand the nature of your concern. Where identity verification is required, the statutory response period will begin once verification is complete.

If you are unhappy with our response, or believe your data protection rights have not been upheld, you have the right to escalate your complaint to the Information Commissioner's Office (ICO):

- Telephone: 0303 123 1113
- Website: www.ico.org.uk

Changes to CiPN's Privacy Policy

This Privacy Policy will be updated annually and from time to time in-between, so you may wish to check it each time you submit personal information to CiPN. The date of the most recent revisions will appear on the front page of this policy. If you do not agree to these changes, please do not continue engaging with CiPN otherwise this will be taken as acceptance of these changes. If significant material changes are made to the Privacy Policy we will notify you by placing a prominent notice on the website.