Third Parties Privacy Notice

Data controller: Public Interest Research Centre (PIRC)
Data protection contact: Anthony Jarrett Email: ant@publicinterest.org.uk

PIRC collects and processes personal data relating to any third parties working with us in order to manage the relationship. PIRC is committed to being transparent about how it collects and uses that data and to meeting its data protection obligations.

What information does PIRC collect?

PIRC collects and processes a range of information about you.

This may include:

- Recruitment information, such as your application form, CV and references if requested.
- Information about your age, ethnic origin, religion, disability, sexual orientation and gender to monitor equal opportunities.
- Your contact details including your home address.
- Your date of birth.
- The contact details for your emergency contacts.
- Details about your current work.
- Publicly-available information about you during recruitment, e.g. if you have a website.
- Your bank details if you claim any expenses.
- Electronic information in relation to your use of IT systems.
- Your images (whether captured on video or by photograph).
- Records of participant data to ensure that we are monitoring, evaluating and learning from our previous work.
- Any other category of personal data which we may notify you of from time to time.

PIRC collects this information in a variety of ways. For example, data is collected through correspondence with you at the start of or during your appointment and through meetings with you.

In some cases, PIRC may collect personal data about you from third parties, such as references.

Why does PIRC process personal data?

PIRC needs to process data to enter into a relationship with you.

PIRC has a legitimate interest in processing personal data before, during and after the end of your engagement. This includes maintaining accurate and up-to-date contact details.

Where PIRC relies on legitimate interests and legal obligations as a reason for processing data, it has considered whether those interests are overridden by the rights and freedoms of third parties working with us and has concluded that they are not. In order to do this, we will normally carry out a Legitimate Interests Assessment, using the template and guidance provided by the ICO.

In some circumstances a Legitimate Interests Assessment will not be necessary if the reason for processing the data falls under the recognised legitimate interests (RLI) set out in the Data Use and Access Act 2025. This allows for a new lawful basis for processing data without the need for a legitimate interest assessment in certain scenarios. Examples of RLI include processing which is necessary for disclosures for safeguarding vulnerable individuals, and disclosures for crime prevention and for detection and responding to emergencies.

Who has access to my data?

Your information will be shared internally with members of the team and other trustees where this is necessary in the performance of their roles.

We will not transfer your data to countries outside the EEA.

Accountants
Prentis & Co are our accountants and we share data with them to the extent needed to carry out their service for us.. Their privacy policy can be found here.

Bookkeeping
We use Xero for our bookkeeping. Their privacy policy can be found here.

The Co-operative Bank
Our business banking is carried out via The Co-operative Bank and we share your payment data with them in order to make payments. Their privacy policy can be found here.

Google Workspace
Google Workspace provides server space for our documents and emails, some of which will contain your personal information. Any information sent via email, or saved in document will therefore be stored and backed up on their servers. Only those who need to use your data as part of their role have access to it. Click here to view Google Workspace's cloud storage compliance, and here for Google's privacy policy.

Slack
Slack provides server space for our internal messaging. Any information sent in Slack messages will therefore be stored and backed up on their servers. Their privacy policy can be found here.

We might, from time to time, use other messaging services, apps or online services for our work. These will always be within the bounds of legitimate interest in relation to our engagement with you.

How does PIRC protect my data?

PIRC takes the security of your data seriously. We have internal policies and controls in place to try to ensure that your data is not lost, accidentally destroyed, misused or disclosed. All personal data is stored in secure folders and only accessible to the staff team and trustees as necessary for the performance of their duties.

Where PIRC engages third parties to process personal data on its behalf, they do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

How long does PIRC keep my data?

We will hold your personal data for the duration of your engagement. The periods for which your data is held after the end of your engagement are set out in the retention periods below.

Your rights

As a data subject, you have a number of rights. You have the right to:

- ask PIRC for information about what personal data we process, how we process it and on what basis;
- access your own personal data by way of a Subject Access Request (see details in our Data Protection Policy);
- require PIRC to correct any inaccuracies in your personal data;
- request that we erase your personal data where we were not entitled under law to process it or where it is no longer necessary to process the data for the purpose for which it was collected. During the process of requesting that your personal data be corrected or erased, or while you are contesting the lawfulness of our processing, you can ask for the data to be used in a restricted way only;
- object to data processing where we rely on a legitimate interest to do so and you think that your rights and interests outweigh our own and you wish us to stop;
- object if we process your personal data for the purposes of direct marketing;
- receive a copy of your personal data and, with some exceptions, transfer your personal data to another data controller (we will not charge for this and will, in most cases, aim to do this within one month);
- not to be subjected to automated decision-making;
- be notified of a data security breach concerning your personal data where that breach is likely to result in a high risk of adversely affecting your rights and freedoms;
- withdraw your consent if we have requested consent to process your personal data for a specific purpose (in most situations, we will not rely on your consent as a lawful ground to process your data.); and
- complain to the Information Commissioner if you believe that PIRC has not complied with your data protection rights - www.ico.org.uk.

If you would like to exercise any of these rights, please contact the named data protection contact.

What if I do not want to provide personal data?

Certain information, such as contact details, have to be provided to enable PIRC to enter an engagement with you and appoint you as a trustee.

Do you use automated decision-making?

Appointment decisions are not based on automated decision-making.

How long will my data be kept for?

We will hold your personal data for the duration of your engagement with us. We may also keep records of participant data, for example, to ensure that we are monitoring, evaluating and learning from our previous work. To comply with our duties under data protection regulations we will keep this information for no longer than is necessary to capture and anonymise participant feedback, and in any event for no longer than two years after your participation.

We will also comply with the relevant statutory retention period to determine how long any other data is held after the end of your engagement.

These include:

- **Accounting records:** 6 years
- **Subject access request:** 1 year following completion of the request.
- **Whistleblowing documents:** 6 months following the outcome (if a substantiated investigation). If unsubstantiated, personal data will be removed immediately.
- **Accident records:** 3 years from the date of the recorded incident.