Data Protection Policy

Date Agreed	11th March 2026
Last reviewed	N/A
Review Date	

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

Other policies that are useful to consider in relation to this policy:

- Disciplinary Policy - this policy sets out the informal and formal actions PIRC may take to address concerns about the conduct of an employee, including incidents related to data processing and data security.

Scope and Purpose

This policy applies to all employees of PIRC. It also applies to trustees, workers, consultants, project partners, volunteers or any self-employed individuals working with us.

Introduction

We need to gather and use information or 'data' about you as part of our business and to manage our relationship with you. This Policy sets out the things we must tell you about data protection.

We take the security and privacy of your data seriously and intend to comply with our legal obligations under the *Data Protection Act 2018* (2018 Act), the *Data (Use and Access) Act 2025* and the *UK General Data Protection Regulation* (GDPR) in respect of data privacy and security.

This Policy applies to current and former employees, as well as any trustees, workers, consultants, project partners, volunteers or any self-employed individuals working with us. If you fall into one of these categories, then you are a 'data subject' for the purposes of this Policy. You should read this Policy alongside your contract and any other notice we issue to you from time to time in relation to your data.

PIRC is a 'data controller' for the purposes of your personal data. This means that we decide how and why we process your personal data.

This Policy explains how we will hold and process your information. It explains your rights as a data subject. It also explains your obligations when obtaining, handling, processing or storing personal data in the course of working for, or on behalf of, PIRC.

This Policy does not form part of your contract. We reserve the right to update this Policy at any time. It is intended that this Policy is fully compliant with the 2018 Act, the UK GDPR and the 2025 Data

Use and Access Act 2025 (DUAA). If any conflict arises between those laws and this Policy, PIRC intends to comply with the 2018 Act, the UK GDPR and the DUAA.

Data protection principles

Personal data must be processed in accordance with the following 'data protection principles.' It must:

- Be processed fairly, lawfully and transparently.
- Be collected and processed only for specified, explicit and legitimate purposes.
- Be adequate, relevant and limited to what is necessary for the purposes for which it is processed.
- Be accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay.
- Not be kept for longer than is necessary for the purposes for which it is processed.
- Be processed securely.

We are responsible for ensuring and demonstrating compliance with these principles.

How we define personal data

'Personal data' means information which relates to a living person who can be identified from that data (a 'data subject') on its own or when taken together with other information which is likely to come into our possession. It includes any expression of opinion about the person and an indication of the intentions of us or others in respect of that person. It does not include anonymised data.

This Policy applies to all personal data, whether it is stored electronically, on paper or in/ on other materials.

This personal data might be provided to us by you or by someone else (such as a former employer, your doctor or a credit reference agency), or it could be created by us. It could be provided or created during the recruitment process or during the course of your contract, or after it has ended. It could be created by other colleagues.

We may collect and use the following types of personal data about you:

- Recruitment information, such as your application form and CV, references, qualifications and membership of any professional bodies and details of any pre-employment assessments.
- Your contact details and date of birth.
- The contact details for your emergency contacts.
- Your gender.
- Your family details.
- Information about your contract, including start and end dates, role and location, working hours, details of promotion, salary (including details of previous remuneration), pension, benefits and holiday entitlement.
- Your bank details and information in relation to your tax status, including your National Insurance number.

- Your identification documents, including your passport and driving licence and information in relation to your immigration status and right to work for us.
- Information relating to disciplinary or grievance investigations and proceedings involving you (whether or not you were the main subject of those proceedings).
- Information relating to your performance and behaviour at work.
- Training records.
- Electronic information in relation to your use of IT systems and telephone systems.
- Your images (whether captured on video or by photograph).
- Any other category of personal data which we may notify you of from time to time.

How special categories of personal data are defined

'Special categories of personal data' are types of personal data consisting of information about:

- Your racial or ethnic origin
- Your political opinions
- Your religious or philosophical beliefs
- Your trade union membership
- Your genetic or biometric data
- Your health
- Your sexual orientation

We may hold the following types of special category data and use any of these special categories of personal data in accordance with the law:

- Your racial or ethnic origin
- Your religious or philosophical beliefs
- Your trade union membership
- Your health
- Your sexual orientation

For example, we collect this data for anonymised reporting to funders and as part of our developing our wellbeing offer as an employer.

See below for more information about how and when we process special category data.

How we define processing

'Processing' means any operation which is performed on personal data, such as collecting, recording, organising, storing, structuring, altering, disclosing or erasing data. 'Processing' includes processing personal data which forms part of a filing system and any automated processing.

How will we process your personal data?

We will process your personal data (including special categories of personal data) in line with our obligations under the 2018 Act. We will use your personal data:

- To perform the contract between us.
- To comply with any legal obligation.

- If it is necessary for our legitimate interests (or for the legitimate interests of someone else, for example for payroll). However, we can only do this if your interests and rights do not override ours (or theirs). You have the right to challenge our legitimate interests and request that we stop using your personal data. (See the ICO guidance on legitimate interests).

We can process your personal data for the purposes listed directly above without your knowledge or consent. We will not use your personal data for an unrelated purpose without telling you about it and the legal basis that we intend to rely on for processing it.

If you choose not to give us certain personal data, we may not be able to carry out some parts of the contract between us. For example, if we do not have your bank account details, we may not be able to pay you. It might also prevent us from complying with certain legal obligations and duties, such as paying the right amount of tax to HMRC or making reasonable adjustments in relation to disability.

Examples of when we might process your personal data

We have to process your personal data in various situations during your recruitment, employment (or engagement) and even following termination of your employment (or engagement).

For example:

- To decide whether to employ (or engage) you.
- To decide how much to pay you (as per our Socially Just Pay Policy) and the other terms of your contract with us.
- To check you have the legal right to work for us.
- To carry out the contract between us, including, where relevant, its termination.
- To train you and review your performance.
- To decide whether and how to manage your performance, absence or conduct.
- To carry out a disciplinary or grievance investigation or procedure in relation to you or someone else.
- To determine whether we need to make reasonable adjustments to your workplace or role if you are disabled.
- To monitor diversity and equal opportunities.
- To monitor and protect the security (including network security) of PIRC, you, our other employees, and others engaged in our work.
- To monitor and protect your health and safety and that of our other employees and third parties.
- To pay you and provide pension and other benefits in accordance with the contract between us.
- To pay tax and National Insurance.
- To provide a reference upon request from another employer.
- To pay trade union subscriptions.
- To monitor compliance by you, us and others with our policies and our contractual obligations.
- To comply with employment law, immigration law, health and safety law, tax law and other laws which affect us.

- To answer questions from insurers in respect of any insurance policies which relate to you.
- To run our organisation and plan for the future.
- For the prevention and detection of fraud or other criminal offences.
- To defend PIRC in respect of any investigation or litigation and to comply with any court or tribunal orders for disclosure.
- For any other reason which we may notify you of from time to time.

Sharing your personal data

Sometimes, we might share your personal data with our contractors and agents to carry out our obligations under our contract with you or for our legitimate interests. We require those people and companies to keep your personal data confidential and secure and to protect it in accordance with the law and our policies. They are only permitted to process your data for the lawful purpose for which it has been shared and in accordance with our instructions.

Our data privacy notices contain details of third parties who may have access to your data.

How should you process personal data for PIRC?

Everyone who works for, or on behalf of, PIRC has responsibility for ensuring data is collected, stored and handled appropriately in line with this policy and other relevant policies.

- You should only access personal data covered by this Policy if you need it for the work you do for, or on behalf of PIRC, and only if you are authorised to do so. You should only use the data for the specified lawful purpose for which it was obtained.
- You should keep personal data secure and not share it with unauthorised people.
- You should regularly review and update personal data which you have to deal with for work. This includes telling us if your own contact details change.
- You should not make unnecessary copies of personal data, and you should keep and dispose of any copies securely.
- You should use strong passwords.
- You should ensure that any data held on your computer or laptop or any other device used for your work is not accessible to anyone else.
- Personal data should never be transferred outside of the UK except in compliance with the law and with the authorisation of the trustees.
- Drawers and filing cabinets containing personal data should be kept locked. Do not leave documents that contain personal data anywhere that can be accessed by unauthorised people.
- Personal data should be shredded and disposed of securely when you have finished with it.
- You should seek support from the person named above if you are unsure about data protection or if you notice any areas of data protection or security we can improve upon.

Any deliberate or negligent breach of this Policy by you may result in disciplinary action being taken against you under our Disciplinary Policy. It is a criminal offence to conceal or destroy personal data which is part of a Subject Access Request (see below). This conduct could amount to gross misconduct under our Disciplinary Policy and you could be dismissed.

How to deal with data breaches

If this policy is followed, we should not have any data breaches. But if a breach of personal data occurs (whether in respect of you or someone else), then we must take notes and keep evidence of that breach.

If the breach is likely to pose a risk to the rights and freedoms of individuals, then we must notify the Information Commissioner's Office within 72 hours, where feasible. If the breach is likely to result in a high risk to your rights and freedoms, then we will let you know about it.

If you are aware of a data breach, then you must contact the person named above immediately and keep any evidence you have in relation to the data breach. They will use the ICO online tool to determine whether the breach needs to be reported.

Subject access requests

Data subjects can make a 'subject access request' (**SAR**) to find out what information we hold about them. This request must be made in writing. If you receive a SAR, you should forward it immediately to the person named above who will coordinate a response.

To make a SAR in relation to your own personal data, you should write to the data protection contact named above. We must respond within one month unless we need to clarify your request, in which case we can "stop the clock" until we hear from you. For example, if you are an employee and you request "all documents about my performance", we will need to seek clarification from you on the scope of your request to understand whether this includes informal notes or only formal performance appraisals.

If the request is complex or more than one request is received from the same person, the period in which we must respond can be extended by up to two months. If you make a SAR and we consider it to be complex, or if you submit multiple SARs, we will still reply to you within the first month to explain the reasons why we consider the extended period applies in your particular case.

There is no fee for making a SAR. However, if your request is manifestly unfounded or excessive, we may charge a reasonable administrative fee or refuse to respond to your request. We normally work on the basis that any request which will take more than a day to deal with is likely to be manifestly excessive, and in those circumstances, we may need to apply a reasonable charge.

Your data subject rights

You have the right to information about what personal data we process, how we process it and on what basis, as set out in this Policy.

You have the right to access your own personal data by way of a SAR (see above).

You can correct any inaccuracies in your personal data by contacting the person named above.

You have the right to 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. You can request erasure by contacting the person named above.

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. To do this, contact the person named above.

You have the right to 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.
You have the right to object if we process your personal data for the purposes of direct marketing.

You have the right to receive a copy of your personal data and, with some exceptions, to 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.

You have the right not to be subjected to automated decision-making.

You have the right to 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.

In most situations, we will not rely on your consent as a lawful ground to process your data. If we do request your consent to process your personal data for a specific purpose, you have the right not to consent or to withdraw your consent later. To withdraw your consent, you should contact the person named above.

You have the right to complain to the Information Commissioner. You can do this by contacting the Information Commissioner's Office directly. Full contact details, including a helpline number, can be found on the Information Commissioner's Office website (www.ico.org.uk). The Information Commissioner's Office website has more information on your rights and our obligations.

Data retention

We will only retain personal data and sensitive data for as long as necessary for the purposes for which we collected it. After this time, it will be deleted or archived.

We will maintain retention policies and procedures to ensure personal data is deleted after an appropriate time unless a law requires that data to be kept for a minimum time.

We will make sure data subjects are provided with information about the period for which data is stored and how that period is determined in any applicable Privacy Notice.

Data complaints procedure (employees only)

If you wish to make a complaint to PIRC as your employer about any aspect of how we have handled your data, you should put your complaint in writing and email or post it to the person named in this policy with responsibility for data protection. We will acknowledge your complaint as soon as we can,

and no later than 30 days as required by the Data Use and Access Act 2025. Your complaint will be investigated and we will inform you of the outcome as soon as we can. If the investigation is complex and likely to take some time, we will keep you informed along the way.

If you are not satisfied with our response, you have the right to raise a formal grievance.

Responsibility for Data Protection

At the time of writing this policy, the person responsible for data protection at PIRC is Anthony Jarrett. They hold the following responsibilities:

- Reviewing Data Protection and related policies
- Advising other staff and trustees on Data Protection issues
- Ensuring that Data Protection is covered in the induction process
- Notification of any changes to our data protection procedures or breaches
- Handling subject access requests
- Approving unusual or controversial disclosures of personal data

Contact: ant@publicinterest.org.uk

Useful information and guidance about the matters covered in this Policy can be found on www.ico.org.uk.