

## Introduction

We take our responsibilities towards data protection and security extremely seriously. As a large organisation, we collect and use data about our colleagues, volunteers, and recruitment applicants. We're under a legal obligation to handle that information properly, fairly and securely.

This privacy notice describes how we collect and use personal information about you, and applies if you are or have been an employee, volunteer or a recruitment applicant. It also applies to workers, self-employed contractors, directors and non-executive directors. Except where distinguished, all of the above categories of people are collectively referred to as our people and applicants in this privacy notice.

If you have difficulty understanding this privacy because of a disability or because English isn't your first language, please discuss the situation with your line manager or the People Team as soon as possible.

This notice does not form part of any contract of employment or volunteer agreement and we may amend this notice at any time.

Within this privacy notice, Amnesty International UK (AIUK) will be your data controller. This means that we are responsible for how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy notice.

## Contents

1. Data protection principles .....	2
2. The kind of information we hold about you .....	3
3. How your personal information is collected .....	4
4. How we'll use information about you .....	5
5. How we use particularly sensitive personal information .....	8
6. Processing information about criminal convictions.....	9
7. Automated decision making .....	10
8. Data sharing.....	11
Why might we share your personal information with third parties?.....	11
Which third-party service providers process your personal information? .....	11

How secure is your information with third-party service providers and other entities in our group?..	12
When might we share your personal information with other entities in the group? .....	12
9. Data security .....	13
10. Other ways we look after your personal information.....	13
11. Data retention.....	14
12. Rights of access, correction, erasure, and restriction .....	15
Your duty to inform us of changes .....	15
Your rights in connection with personal information .....	15
Accessing your personal data .....	16
What we may need from you .....	16
Right to withdraw consent .....	16
13. Data privacy manager .....	16
14. Changes to this privacy notice .....	16

## **1. Data protection principles**

- 1.1 We'll comply with data protection law. This says that the personal information we hold about you must be:
- a) Used lawfully, fairly and in a transparent way.
  - b) Collected only for valid purposes that we've clearly explained to you and not used in any way that is incompatible with those purposes.
  - c) Relevant to the purposes we've told you about and limited only to those purposes.
  - d) Accurate and kept up to date.
  - e) Kept only as long as necessary for the purposes we've told you about.
  - f) Kept securely.

## **2. The kind of information we hold about you**

- 2.1 Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).
- 2.2 There are “special categories” of more sensitive personal data which require a higher level of protection.
- 2.3 If you are or have been a recruitment applicant we may collect, store and use the following categories of personal information about you as part of the application process:
  - a) Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses
  - b) Age group
  - c) Gender
  - d) Previous employment and relevant experience
- 2.4 If you are or have been one of our people we may collect, store and use the following categories of personal information about you:
  - a) Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses
  - b) Diversity demographic information including date of birth, marital status, gender identity, and caring responsibilities.
  - c) Next of kin and emergency contact information
  - d) Location of employment or volunteering or workplace
  - e) Recruitment information (including copies of references and other information included in an application form)
  - f) Employment or volunteer records (volunteering agreement, training records and review/supervision documentation)
  - g) CCTV footage and other information obtained through electronic means such as swipe card records
  - h) Information about your use of our information and communications systems
  - i) Photographs

- j) Marital status
- k) National insurance number
- l) Legal sex
- m) Bank account details, payroll records and tax status information
- n) Salary, annual leave, pension and benefits information
- o) Start date, job titles, work history and working hours
- p) Any changes to terms and conditions of employment
- q) Right to work documentation such as passports, visas or national identity cards
- r) Compensation history
- s) Performance information
- t) Disciplinary and grievance information
- u) Resignation letters and references

2.5 We may also collect, store and use the following “special categories” of more sensitive personal information:

- a) Information about your race or ethnicity, religious beliefs, sexual orientation
- b) Information about your health, including any medical condition, health and if you are or have been a volunteer/employee also sickness records.
- c) Information about criminal convictions and offences if you are offered a role (not a recruitment applicant).
- d) Information about your schooling, and childhood main household earner job category that indicates your socio-economic status.

### **3. How your personal information is collected**

3.1 We collect personal information about all our people from the application and recruitment process, either directly from candidates or sometimes from an employment agency or background check provider. We may sometimes collect additional information from third parties including former employers/volunteer supervisors, or other background check agencies such as the Disclosure and Barring Service (DBS).

3.2 If applicable, we'll collect additional personal information in the course of job/role related activities throughout the period of you working or volunteering for us if applicable.

## **4. How we'll use information about you**

4.1 We'll only use your personal information when the law allows us to. Most commonly, we'll use your personal information in the following circumstances:

- a) If you are or have been one of our people or applicant, where we need to perform the contract we've entered into with you. If you're currently a recruitment applicant, we may use your personal information to take steps which are preparatory to performing a contract we may enter into with you.
- b) Where we need to comply with a legal obligation, such as providing information to HMRC, to respond to requests from courts, law enforcement agencies and other public and government authorities.
- c) Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights don't override those interests.

4.2 We may also use your personal information in the following situations, which are likely to be rare:

- a) Where we need to protect your interests (or someone else's interests).
- b) Where it is needed in the public interest or for official purposes.

4.3 If you are or have been one of our people we'll need all the categories of information in the list above primarily to allow us to perform our contract with you and to enable us to comply with legal obligations such as the following:

- a) Making a decision about your recruitment or appointment.
- b) Determining the terms on which you work for us.
- c) Checking you are legally entitled to work in the work location in which you are based.
- d) Paying you and, if you are an employee, deducting tax and National Insurance/Social Security contributions.
- e) Providing benefits to you for example, pension, and other voluntary benefits which you may opt into during the course of your employment or appointment.

- f) Liaising with your pension provider.
- g) Administering the contract we've entered into with you.
- h) Business management and planning, including accounting and auditing.
- i) Conducting performance reviews, managing performance and determining performance requirements.
- j) Assessing qualifications for a particular job or task, including decisions about promotions.
- k) Gathering evidence for possible grievance or disciplinary hearings.
- l) Making decisions about your continued employment or engagement.
- m) Making arrangements for the termination of our working relationship.
- n) Assessing education, training and development requirements
- o) Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work.
- p) Ascertaining your fitness to work.
- q) Managing sickness absence.
- r) Complying with health and safety obligations.
- s) Preventing fraud.
- t) Monitoring your use of our information and communication systems to ensure compliance with our [IT Acceptable Usage policy](#).
- u) Ensuring network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.
- v) Conducting data analytics studies to review and better understand employee retention and attrition rates.
- w) Facilitating equal opportunities monitoring.

4.4 If you're currently a recruitment applicant and not yet one of our people or a volunteer, we may request from you the appropriate categories from the information set out above,

primarily to allow us to prepare to perform our contract with you and to enable us to comply with legal obligations as follows:

- a) Making a decision about your recruitment or appointment.
- b) Determining the terms on which you work for us.
- c) Checking you are legally entitled to work in the work location in which you are based.
- d) Complying with health and safety obligations.
- e) Facilitating equal opportunities monitoring.

4.5 If you are or have been one of our people, in some cases we may use your personal information to pursue legitimate interests of our own or those of third parties, provided your interests and fundamental rights don't override those interests. Guidance on what constitutes a legitimate interest can be found on the Information Commissioners Office (ICO) website here. A legitimate interest includes, for example:

- a) Making a decision about your recruitment, appointment or volunteer application.
- b) Complying with health and safety obligations.
- c) Unless you're a recruitment applicant and not yet one of our people, monitoring your use of our information and communication systems [to ensure compliance with our [IT Acceptable Usage policy](#)].
- d) Unless you're a recruitment applicant and not yet our people, ensuring network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.
- e) Facilitating equal opportunities monitoring.
- f) Assessing education, training and development requirements
- g) If you are or have been a volunteer, maintaining contact with you during your volunteering.
- h) If you are or have been one of our people:
  - to pay you through payroll.
  - to process sickness absence in order to facilitate the payment of statutory sick pay.

- monitoring your work emails during any period of absence.
  - to liaise with occupational health.
- 4.6 Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.
- 4.7 If you fail to provide certain information when requested, we may not be able to perform the recruitment process or contract or agreement we've entered into with you (such as paying you or providing a benefit, or facilitate your volunteering), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our people).
- 4.8 We'll only use your personal information for the purposes for which we've collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we'll notify you and we'll explain the legal basis which allows us to do so.
- 4.9 Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

## **5. How we use particularly sensitive personal information**

- 5.1 "Special categories" of particularly sensitive personal information require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information.
- 5.2 We may process special categories of personal information in the following circumstances:
- a) In limited circumstances, with your explicit written consent. If we need your consent we'll contact you separately about this.
  - b) Where we need to carry out our legal obligations and in line with our Data Protection Policy.
  - c) Where it is needed in the public interest, such as for equal opportunities monitoring or in relation to our occupational pension scheme, and in line with our Data Protection Policy and Equality and Diversity Policy.
  - d) Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone



else's interests) and you are not capable of giving your consent, or where you have already made the information public.

- e) If you are or have been an employee, where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards.

5.3 We'll use your particularly sensitive personal information in the following ways:

- a) We may use information about your physical or mental health, or disability status, to ensure your health and safety in the workplace, to provide appropriate recruitment/workplace adjustments and if you're an employee, to assess your fitness to work, to ensure you are treated fairly in organisational procedures, to monitor and manage sickness absence and to administer benefits.
- b) We'll use information about your race or national or ethnic origin, religion or belief, or sexual orientation and disability status, to ensure meaningful equal opportunity monitoring and reporting and to comply with employment and other laws, for example if you raise concerns about your employment which relate to a protected characteristic.
- c) If you are or have been one of our people, we'll use information relating to leaves of absence, which may include sickness absence or family related leave, to comply with employment and other laws.
- d) If you are or have been one of our people, we will use trade union membership fees through payroll when requested.

5.4 We don't need your consent if we use special categories of your personal information in accordance with our written policy, to carry out our legal obligations or exercise specific rights in the field of employment law. In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we'll provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your contract or volunteering agreement with us that you agree to any request for consent from us.

## **6. Processing information about criminal convictions**

6.1 We will only use information relating to criminal convictions where the law allows us to do so. This will usually be where it is necessary to carry out our legal and regulatory obligations (for example conducting safeguarding checks) and will always be done in line with our Data Protection Policy. Less commonly, we may use information relating to criminal convictions where it's necessary in relation to legal claims, where it's

necessary to protect your interests (or someone else's interests) and you're not capable of giving your consent, or where you've already made the information public.

- 6.2 We'll collect information about criminal convictions as part of the conditional offer process to become one of our people to ensure the role you are applying for does not place you at risk or put others at risk. We also ask that you notify us of such information directly in the course of you working/volunteering for us if you are convicted of a crime.
- 6.3 If you are offered a specific position that requires it, we'll collect information to undertake a criminal record check to assess suitability for:
- a) Roles with direct responsibility for the care of children or adults-at-risk in line with specific criteria set by the relevant criminal record check service.
  - b) For roles required to register with the gambling commission.
  - c) For specific finance roles within the organisation in line with criteria set by the relevant criminal record check service.

We'll seek to renew criminal record checks for roles which require it in line with our policy.

## **7. Automated decision making**

- 7.1 Automated decision-making is when an electronic system uses personal information to make a decision without human intervention. We're allowed to use automated decision-making in the following circumstances:
- a) Where we've notified you of the decision and given you 21 days to request a reconsideration.
  - b) Where it is necessary to perform the contract/agreement with you and appropriate measures are in place to safeguard your rights.
  - c) In limited circumstances, with your explicit written consent and where appropriate measures are in place to safeguard your rights.
- 7.2 Automated decision making at AIUK may be used in very limited circumstances, and only in the very early stages of the recruitment process in terms of establishing whether you have the right to work in the UK.
- 7.3 If we make an automated decision on the basis of any particularly sensitive personal information, we must have either your explicit written consent or it must be justified in

the public interest, and we must also put in place appropriate measures to safeguard your rights.

- 7.4 You'll not be subject to decisions that will have a significant impact on you based solely on automated decision-making, unless we've a lawful basis for doing so and we've notified you.

## **8. Data sharing**

- 8.1 We may have to share your data with third parties, including third-party service providers. We require third parties to respect the security of your data and to treat it in accordance with the law. We may transfer your personal information outside of the UK and/or outside the EU. If we do, you can expect a similar degree of protection in respect of your personal information.

### **Why might we share your personal information with third parties?**

- 8.2 We'll share your personal information with third parties where required by law, where it is necessary to administer the working relationship with you or where we've another legitimate interest in doing so.

### **Which third-party service providers process your personal information?**

- 8.3 "Third parties" includes third-party service providers (including contractors and designated agents) and other entities within our group. If you are or have been one of our people, the following activities are carried out by third-party service providers:
- a) Scottish Widows and Pensions Trust for pension administration
  - b) CIPHR Payroll Services for payroll administration
  - c) CIPHR iRecruit for recruitment applications
  - d) Eden Red for childcare and eyecare voucher administration
  - e) Busy Bees for childcare voucher administration
  - f) Clear Review, performance management web application
  - g) Cardinus, for ergonomic work set up assessments
  - h) great{with}talent for Leaver survey feedback
  - i) Agenda for engagement surveys

- j) Health Management for Occupational Health service provision
- k) Verifile for DBS administration and digital right to work in the UK checks
- l) CIPHR, our employee and volunteer database provider
- m) Charity Learning Consortium, for provision of online e-learning system
- n) Charitable Giving, a payroll giving service
- o) Unite, for administration of union subscription payment through payroll
- p) Barbican Independent Financial Services Limited, for provision of pension advice and brokering of group life cover

8.4 If you are or have been a volunteer, the following activities are carried out by third-party service providers:

- a) Charity Learning Consortium, for provision of online e-learning system
- b) CIPHR, our database provider

8.5 If you're a recruitment applicant and not yet one of our people, the following activities are carried out by third-party service providers:

- a) CIPHR iRecruit for recruitment applications.
- b) Broadbean for tracking which job boards clicked to reach a vacancy in our careers portal

**How secure is your information with third-party service providers and other entities in our group?**

8.6 All our third-party service providers and other entities in the group are required to take appropriate security measures to protect your personal information in line with our policies. We don't allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

**When might we share your personal information with other entities in the group?**

8.7 We'll share your personal information with the International Secretariat and other Amnesty Sections as part of our regular reporting activities on company performance, in the context of a business reorganisation or group restructuring exercise, for system

maintenance support and hosting of data.

### **What about other third parties?**

- 8.8 We may share your personal information with other third parties, for example with a regulator or to otherwise comply with the law.

### **Transferring information outside the EU**

- 8.9 We don't currently transfer the personal information we collect about you to countries outside the EU. We'll let you know if this changes.
- c) If it does change, to ensure that your personal information does receive an adequate level of protection we'll put in place appropriate measures to ensure that your personal information is treated by those third parties in a way that is consistent with and which respects the EU and UK laws on data protection.

## **9. Data security**

- 9.1 We've put in place measures to protect the security of your information. We have deployed leading cyber-security solutions for mobiles, laptops, desktops and servers. We have strict access control and encrypt all data at rest.
- 9.2 Third parties will only process your personal information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.
- 9.3 We've put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality.
- 9.4 We've put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

## **10. Other ways we look after your personal information.**

- 10.1 We report to our principal Boards (governing the Amnesty International UK Section and the Amnesty International UK Section Charitable Trust) on data protection through regular briefings, meetings and other appropriate channels where required.

- a) Compliance with Data Protection rules is overseen by the Head of Data and Insight, who is our main point of contact for data protection enquiries. They are responsible for: Training all our personnel and volunteers involved in data processing.
- b) Educating the organisation on the importance of being compliant.
- c) Maintaining comprehensive records of all data processing.
- d) Providing guidance and advice to the organisation and our personnel and volunteers as required.

10.2 We provide data protection guidance and training for our people in our offices and bookshops so they are aware of their data protection responsibilities. Training is provided when our people first join us, and periodically after this as refresher training. Our data protection training will usually cover UK data protection law, the risks associated with using personal information and how to handle personal information responsibly in compliance with the law.

## **11.Data retention**

- 11.1 We'll only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements.
  - 11.2 To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements. Details of retention periods for different aspects of your personal information are available in our retention schedule which is available on SharePoint. If you are:
    - a) For one of our personnel, we'll generally retain all data for six years post-employment except for payroll records which are generally securely held for 10 years post-employment.
    - b) a volunteer, we'll generally retain your data for six years post-volunteering.
- 8.1.1 a recruitment applicant, we'll generally retain your applicant data in the careers portal for six months from the point you provide or extend your consent.

11.3 In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you.

## **12. Rights of access, correction, erasure, and restriction**

### **Your duty to inform us of changes**

12.1 It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us or your application. If you're an employee, you're able to amend and update some of your new personal data directly through our Self-Service portal.

### **Your rights in connection with personal information**

12.2 Under certain circumstances, by law you have the right to:

- a) Request access to your personal information (commonly known as a “data subject access request”). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
- b) Request correction of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- c) Request erasure of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).
- d) Object to processing of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.
- e) Request the restriction of processing of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.
- f) Request the transfer of your personal information to another party.

12.3 If you are or have been an employee and you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact the [PeopleTeam@amnesty.org.uk](mailto:PeopleTeam@amnesty.org.uk) and [DataProtection@amnesty.org.uk](mailto:DataProtection@amnesty.org.uk).

### **Accessing your personal data**

12.4 You'll not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

### **What we may need from you**

12.5 We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

### **Right to withdraw consent**

12.6 In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the People Team. Once we've received notification that you have withdrawn your consent, we'll no longer process your information for the purpose or purposes you originally agreed to, unless we've another legitimate basis for doing so in law.

## **13.Data privacy manager**

We've appointed a Head of Data and Insight to oversee compliance with this privacy notice. If you have any questions about this privacy notice or how we handle your personal information, please contact [DataProtection@amnesty.org.uk](mailto:DataProtection@amnesty.org.uk). You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.

## **14.Changes to this privacy notice**



- 14.1 We reserve the right to update this privacy notice at any time, and we'll provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information. A copy of this notice is also available on the intranet if you're an employee or volunteer.
- 14.2 If you have any questions about this privacy notice, please contact the Data Protection team on [DataProtection@amnesty.org.uk](mailto:DataProtection@amnesty.org.uk).