

## **The National Autistic Society – Employee & Workers (UK) Privacy Notice**

This privacy notice applies to all employees of The National Autistic Society.

It is in line with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018, and outlines how we collect, use, store, and protect your personal information and how, in doing so we comply with our legal obligations to you during, and after your employment or engagement with us.

The National Autistic Society is a "data controller", this means we are responsible for deciding how we store and use personal information about you.

It is important that you read this privacy notice so that you know how and why we use your personal information. You should also read any additional privacy notices that we give you when we collect or process personal information about you.

If you have any questions about this notice or how we handle your personal information, please contact us at [dataprotection@nas.org.uk](mailto:dataprotection@nas.org.uk)

The National Autistic Society is registered with the Information Commissioner's Office under the registration number: Z7503397.

### **Contacting Our Data Protection Officer**

Data Protection Officer  
National Autistic Society  
2nd Floor  
Weston House  
42 Curtain Road  
London  
EC2A 3NH

Email: [dataprotection@nas.org.uk](mailto:dataprotection@nas.org.uk)

### **How We Collect Personal Information**

We typically collect personal information about employees in a variety of ways. For example, data is collected through application forms or CVs; obtained from your passport or other identity documents such as your driving licence; from forms completed by you at the start of or during employment (such as benefit nomination

forms); from correspondence with you; or through interviews, meetings or other assessments.

In some cases, the organisation collects personal data about you from third parties, such as references supplied by former employers, information from employment background check providers, information obtained from social media monitoring and information from criminal records checks permitted by law.

Additional personal information is collected throughout your employment through job-related activities.

Data is stored in a range of different places, including in your personnel file, in the organisation's HR and payroll management systems and in other IT systems (including the organisation's email system).

### **What if you do not provide personal data?**

You have some obligations under your employment contract to provide the organisation with data. In particular, you are required to report absences from work and may be required to provide information about disciplinary or other matters under the implied duty of good faith. You may also have to provide the organisation with data to exercise your statutory rights, such as in relation to statutory leave entitlements. Failing to provide the data may mean that you are unable to exercise your statutory rights.

Certain information, such as contact details, your right to work in the UK and payment details, have to be provided to enable the organisation to enter a contract of employment with you. If you do not provide other information, this will hinder the organisation's ability to administer the rights and obligations arising as a result of the employment relationship efficiently.

### **Categories of Personal Information**

"Personal data" or "personal information" refers to information about an individual from which that person can be identified. It does not include data where the identity of the person is anonymous.

There are special categories of more sensitive personal data which require a higher level of protection.

#### **Standard personal information includes:**

- **Contact Information:** Name, address, email, phone numbers.

- **Employment Details:** Job title, employment history, qualifications, references, and performance information.
- **Identification:** Date of birth, National Insurance number, and passport details.
- **Financial Information:** Salary, tax, and pension contributions.
- **IT Usage:** Information about your use of National Autistic Society IT systems, such as IP addresses, login details, and device information.

**Special category information includes:**

- **Health Information:** Details of any physical or mental health conditions, including any adjustments needed to support your work.
- **Diversity Data:** Information about your race, ethnic origin, religion, or sexual orientation.
- **Criminal Records:** Information about criminal convictions or offences as part of background checks.
- **Financial Information:** Bank details
- **Communication Records:** Emails, phone calls, and records of any meetings or discussions.
- **Trade union membership**

## **Purpose and Legal Basis for Processing Your Personal Information**

The National Autistic Society will process your personal information for various purposes necessary for your employment or engagement, including:

- **Contractual Necessity:** managing payroll, pensions, and benefits; maintaining employment records.
- **Legal Obligation:** compliance with employment, tax, and health and safety laws; DBS and background checks.
- **Legitimate Interests:** details of those legitimate interests are set out in more detail in the 'Legitimate interest' section below.
- **Consent:** voluntary participation in equality monitoring, optional marketing communications.

## **Legitimate Interests**

The National Autistic Society has a legitimate interest in processing personal data before, during and after the end of the employment relationship. Processing employee data allows the organisation to:

- run recruitment and promotion processes;
- maintain accurate and up-to-date employment records and contact details (including details of who to contact in the event of an emergency), and records of employee contractual and statutory rights;
- operate and keep a record of disciplinary and grievance processes, to ensure acceptable conduct within the workplace;

- ensure employees are complying with relevant policies and procedures;
- operate and keep a record of employee performance and related processes, to plan for career development, and for succession planning and workforce management purposes;
- operate and keep a record of absence and absence management procedures, to allow effective workforce management and ensure that employees are receiving the pay or other benefits to which they are entitled;
- obtain occupational health advice, to ensure that it complies with duties in relation to individuals with disabilities, meet its obligations under health and safety law, and ensure that employees are receiving the pay or other benefits to which they are entitled;
- operate and keep a record of other types of leave (including maternity, paternity, adoption, parental leave, shared parental leave, and parental bereavement leave), to allow effective workforce management, to ensure that the organisation complies with duties in relation to leave entitlement, and to ensure that employees are receiving the pay or other benefits to which they are entitled;
- ensure effective general HR and business administration;
- conduct employee engagement surveys;
- provide references on request for current or former employees;
- respond to and defend against legal claims and enforce its legal rights; and
- maintain and promote equality in the workplace.

Some special categories of personal data, such as information about health or medical conditions, or racial or ethnic origin, are processed to carry out employment law obligations (such as those in relation to employees with disabilities, for health and safety purposes and to ensure that employees have the right to work in the UK).

Where the organisation processes other special categories of personal data, such as information about ethnic origin, sexual orientation, health or religion or belief, this is done for the purposes of equal opportunities monitoring as permitted by the Data Protection Act 2018 and other relevant law such as the Fair Employment and Treatment (Northern Ireland) Order 1998. Data that the organisation uses for these purposes is anonymised or is collected with the express consent of employees, which can be withdrawn at any time. Employees are entirely free to decide whether to provide such data and there are no consequences of failing to do so.

As noted above, the organisation may process criminal records data to assess your suitability for employment both when you are recruited (through appropriate criminal records checks) and in the course of your employment.

## **Sharing Your Information**

Your information will be shared internally, including with members of the HR and recruitment team including payroll, your line manager, managers in the business area in which you work and IT staff, if access to the data is necessary for performance of their roles.

Your data may also be shared with employee representatives in the context of collective consultation on a redundancy or business sale. This would be limited to the information needed for the purposes of consultation, such as your name, contact details, role and length of service.

The organisation shares your data with third parties to obtain pre-employment references from other employers, obtain employment background checks from third-party providers, obtain necessary criminal records checks from the Disclosure and Barring Service in England and equivalent body in Scotland and Northern Ireland, or report suspected offences to the appropriate authorities. The organisation may also share your data with third parties for the purposes of enforcing its legal rights. The organisation may share your data with third parties in the context of a transfer of some or all of its business. In those circumstances the data will be subject to confidentiality arrangements.

The organisation also shares your data with third parties that process data on its behalf in connection with payroll, pensions, the provision of benefits and the provision of occupational health services.

We ensure suitable safeguards and compliance with data protection laws.

## **Anonymised and Combined Information**

We may use your information in an anonymised or aggregated format:

- For research and statistical analysis.
- To monitor diversity and inclusion.
- You will not be identifiable from this data.

## **Transferring Information Outside the UK**

Where possible the organisation will not transfer your data to countries outside the UK.

However, where necessary, your personal data may be transferred internationally. These transfers will only occur where adequate protection

measures are in place (e.g., adequacy decisions, Standard Contractual Clauses).

## How Long We Keep Your Personal Information

We retain your personal information for the duration of your employment and for an appropriate period thereafter, in line with legal requirements and National Autistic Society retention policies.

For specific details, contact [dataprotection@nas.org.uk](mailto:dataprotection@nas.org.uk)

## How does the organisation protect data?

The organisation takes the security of your data seriously. The organisation has internal policies and controls in place to try to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by its employees in the performance of their duties.

Where possible, automated system processes are in place to ensure compliance with data protection regulations by restricting access to data based on user roles and permissions. Additionally, automated systems are used to securely delete data in accordance with predefined retention policies.

Where the organisation 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.

## Your Rights

You have the right to access your information and to ask us to correct any mistakes and delete and restrict the use of your information. You also have the right to object to us using your information, to ask us to transfer information you have provided, to withdraw permission you have given us to use your information and to ask us not to use automated decision-making which will affect you. For more information, see below.

- **Right of access:** you have the right to make a request for details of your personal information and a copy of that personal information.
- **Right to rectification:** you have the right to have inaccurate information about you corrected or removed.
- **Right to erasure ('right to be forgotten'):** you have the right to have certain personal information about you deleted from our records.

- **Right to restriction of processing:** you have the right to ask us to use your personal information for restricted purposes only
- **Right to object:** you have the right to object to us processing (including profiling) your personal information in cases where our processing is based on a task carried out in the public interest or where we have let you know it is necessary to process your information for our or a third party's legitimate interest. You can object to us using your information for direct marketing and profiling purposes in relation to direct marketing.
- **Right to data portability:** you have the right to ask us to transfer the personal information you have given us to you or to someone else in a format that can be read by computer.
- **Right to withdraw consent:** you have the right to withdraw any permission you have given us to handle your personal information. If you withdraw your permission, this will not affect the lawfulness of how we used your personal information before you withdrew permission, and we will let you know if we will no longer be able to provide you with your chosen product or service.
- **Right in relation to automated decisions:** you have the right not to have a decision which produces legal effects which concern you or which have a significant effect on you based only on automated processing, unless this is necessary for entering into a contract with you, it is authorised by law or you have given your permission for this. We will let you know if we make automated decisions, our legal reasons for doing this and the rights you have.

Please note: other than your right to object to us using your information for direct marketing (and profiling for the purposes of direct marketing), your rights are not absolute. This means they do not always apply in all cases, and we will let you know in our correspondence with you how we will be able to meet your request relating to your rights.

If you make a request, we will ask you to confirm your identity if we need to, and to provide information that helps us to understand your request better. We have 21 days to respond to requests relating to automated decisions. For all other requests we have one month from receiving your request to tell you what action we have taken.

In order to exercise your rights, please email us at [dataprotection@nas.org.uk](mailto:dataprotection@nas.org.uk)

## How to Complain

You can always make a complaint if you are unhappy with the way we have used your data by contacting us at [Your.Views@nas.org.uk](mailto:Your.Views@nas.org.uk)

You can also complain to the ICO if you are either unhappy with how we responded to your complaint or with how we have used your data.



**The ICO's address:**

Information Commissioner's Office  
Wycliffe House  
Water Lane  
Wilmslow  
Cheshire  
SK9 5AF

Helpline number: 0303 123 1113

**Changes to this Privacy Notice**

We reserve the right to amend this privacy notice at any time.  
Updates will be posted on our intranet and/or notified to you.