

Privacy notice for the Remarkable Autism Ltd workforce

Under data protection law, individuals have a right to be informed about how the organisation uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice describes how we collect and use personal information about you during and after your work relationship with us, in accordance with the UK General Data Protection Regulation (UK GDPR).

Following Brexit, Regulation (EU) 2016/679, General Data Protection Regulation (GDPR) is retained EU law and known as UK GDPR. The UK GDPR sits alongside an amended version of the Data Protection Act 2018 that relate to general personal data processing, powers of the Information Commissioner and sanctions and enforcement. The GDPR as it continues to apply in the EU is known as EU GDPR.

This notice applies to all current and former employees, workers and contractors.

We, Remarkable Autism Ltd, are the 'data controller' for the purposes of data protection law. This means that we are responsible for deciding 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.

This notice does not form part of any contract of employment or other contract to provide services and we may update this notice at any time.

It is important that you read this notice with any other policies mentioned within this privacy notice, so that you are aware of how and why we are processing your information, what your rights are under data protection legislation and the procedures we take to protect your personal data.

Our Data Protection Officer is Judicium (see 'Contact us' below).

Data Protection Principles

We will comply with the data protection principles when gathering and using personal information, as set out in our data protection policy.

The personal data we hold

We process data relating to those we employ, or otherwise engage, to work within our organisation.

We may collect, store and use the following categories of personal information about you:

- Personal information and contact details such as name, title, addresses, date of birth, marital status, phone numbers and personal email addresses;
- Emergency contact information such as names, relationship, phone numbers and email addresses;
- Information collected during the recruitment process that we retain during your employment including references, proof of right to work in the UK, application form, CV, qualifications;
- Employment contract information such as start dates, hours worked, post, roles;
- Education and training details;
- Details of salary and benefits including payment details, payroll records, tax status information, national insurance number, pension and benefits information;
- Details of any dependants;
- Your nationality and immigration status and information from related documents, such as your passport or other identification and immigration information;
- Information in your sickness and absence records such as number of absences and reasons (including sensitive personal information regarding your physical and/or mental health);
- Criminal records information as required by law to enable you to work with children;
- Information on grievances raised by or involving you;
- Information on conduct and/or other disciplinary issues involving you;
- Details of your appraisals, performance reviews and capability issues;
- Details of your time and attendance records;
- Information about the use of our IT, communications and other systems, and other monitoring information;
- Details of your use of business-related social media;
- Images of staff captured by the organisation's CCTV systems;
- Your use of public social media (only in very limited circumstances, to check specific risks for specific functions within the organisation, you will be notified separately if this is to occur); and
- Details in references about you that we give to other;
- Recordings of staff from the organisation's video conferencing platform

We may also collect, store and use the following more sensitive types of personal information:

- Information about your race or ethnicity, religious beliefs, sexual orientation, and political opinions.
- Trade union membership.
- Information about your health, including any medical condition and sickness records, including:
 - where you leave employment and under any share plan operated by a group company the reason for leaving is determined to be ill health, injury or disability, the records relating to that decision;
 - details of any absences (other than holidays) from work including time on statutory parental leave and sick leave; [and]
 - any health information in relation to a claim made under the permanent health insurance scheme; and
 - where you leave employment and the reason for leaving is related to your health, information about that condition needed for pensions and permanent health insurance purposes.
- Genetic information and biometric data.
- Information about criminal convictions and offences.

How We Use Particularly Sensitive Information

Sensitive personal information (as defined under the UK GDPR as “special category data”) requires higher levels of protection and further justification for collecting, storing and using. We may process this data in the following circumstances:

- In limited circumstances, with your explicit written consent;
- Where we need to carry out our legal obligations in line with our data protection policy;
- Where it is needed in the public interest, such as for equal opportunities monitoring (or in relation to our pension scheme);
- Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards. Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is necessary to protect your interests (or someone else’s interests) and you are not capable of giving your consent.

We will use this information in the following ways:

- Collecting information relating to leave of absence, which may include sickness absence or family related leave;
- To comply with employment and other laws;
- Collecting information about your physical or mental health, or disability status, to ensure your health and welfare in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to manage sickness absence and to administer benefits;
- Collecting information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or sexual life or sexual

orientation, to ensure meaningful equal opportunity monitoring and reporting.

- To record trade union membership information to pay trade union premiums and to comply with employment law obligations.

Our lawful basis for using this data

We only collect and use personal information about you when the law allows us to. Most commonly, we use it where we need to:

- Fulfil a contract we have entered into with you
- Comply with a legal obligation
- Carry out a task in the public interest

Less commonly, we may also use personal information about you where:

- You have given us consent to use it in a certain way
- We need to protect your vital interests (or someone else's vital interests)
 - We have legitimate interests in processing the data

Where you have provided us with consent to use your data, you may withdraw this consent at any time. We will make this clear when requesting your consent, and explain how you go about withdrawing consent if you wish to do so.

Some of the reasons listed above for collecting and using personal information about you overlap, and there may be several grounds which justify the organisation's use of your data.

Criminal Convictions

We may 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 obligations. We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so.

Where appropriate we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you in the course of working for us.

Collecting this information

While the majority of information we collect from you is mandatory, there is some information that you can choose whether or not to provide to us.

Whenever we seek to collect information from you, we make it clear whether you must provide this information (and if so, what the possible consequences are of not complying), or whether you have a choice.

We may collect this information from you in your application form, but we will also collect information in a number of different ways. This could be through the Home Office, our pension providers, medical and occupational health professionals we engage with, your trade union, and even other employees. Information is also collected through CCTV, access control systems and any IT system the organisation has in place.

How we store this data

Personal data is stored in line with our Data Protection Policy.

We create and maintain an employment file for each staff member. The information contained in this file is kept secure and is only used for purposes directly relevant to your employment.

Once your employment with us has ended, we will retain this file and delete the information in it in accordance with our Data Protection Policy.

Our Data Protection Policy is available on our website via the following link: [Data Protection Policy](#).

If you would prefer to be sent either an electronic or paper copy of the policy, please contact our Data Protection Officer.

Data sharing

We do not share information about you with any third party without your consent unless the law and our policies allow us to do so.

Where it is legally required, or necessary (and it complies with data protection law), we may share personal information about you with:

- Our local authority
- The Department for Education (DfE)
- LADO
- Prospective Employers
- Training Providers
- Professional advisors such as lawyers and consultants
- Support services (including HR support, insurance, IT support, information security, pensions and payroll)
- DBS
- Recruitment and supply agencies
- Other schools and colleges
- Your family or representatives
- Educators and examining bodies
- Our regulators (e.g. Ofsted and CQC)
- Financial organisations (e.g. our pension advisors)
- Central and local government

- Our auditors
- Survey and research organisations
- Trade unions and associations
- Health authorities (NHS)
- Occupational Health
- Health and social welfare organisations (such as social services)
- Professional advisers and consultants
- Charities and voluntary organisations
- Police forces, courts, tribunals
- Professional bodies
- Employment and recruitment agencies

Transferring data internationally

Where we transfer personal data to a country or territory outside the UK or European Economic Area, we will do so in accordance with data protection law.

Retention Periods

Except as otherwise permitted or required by applicable law or regulation, the organisation only retains personal data for as long as necessary to fulfil the purposes they collected it for, as required to satisfy any legal, accounting or reporting obligations, or as necessary to resolve disputes.

Once you are no longer a staff member within the organisation, we will retain and securely destroy your personal information in accordance with our data retention policy. This can be found [here](#).

Security

We have put in place measures to protect the security of your information (i.e. against it being accidentally lost, used or accessed in an unauthorised way). 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. Details of these measures are available in our cyber security policy which is available in the Remarkable SharePoint Policies section.

You can find further details of our security procedures within our Data Breach policy, which can be found [here](#).

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.

Biometric Data

At Remarkable Autism we would like to use your information as part of an automated (i.e. electronically operated) recognition system. At present there are a limited number of thumb readers for students to be able to access the

IT network without the need for complex passwords, but we plan to extend this to all users in the future. The information that we wish to use is referred to as 'biometric information'. This data will only be processed once we have obtained appropriate specific consent. For further information in relation to this, please see Acceptable Use of IT Policy.

Your rights

How to access personal information we hold about you

Individuals have a right to make a **'subject access request'** to gain access to personal information that the organisation holds about them.

If you make a subject access request, and if we do hold information about you, we will:

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

You may also have the right for your personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request, please contact our Data Protection Officer.

Your other rights regarding your data

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

- Access your personal information (commonly known as a "subject access request"). This allows you to receive a copy of the personal information we hold about you and to check we are lawfully processing it. You will not have to pay a fee to access your personal information. 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.
- Correction of the personal information we hold about you. This enables you to have any inaccurate information we hold about you corrected.
- Erasure of your personal information. You can ask us to delete or remove personal data if there is no good reason for us continuing to process it.
- Restriction of processing your personal information. You can ask us to suspend processing personal information about you in certain

circumstances, for example, if you want us to establish its accuracy before processing it.

- To object to processing in certain circumstances (for example for direct marketing purposes).
- To transfer your personal information to another party.

If you want to exercise any of the above rights, please contact the Data Protection Lead in writing.

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).

Right to Withdraw Consent

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 our Data Protection Lead by emailing dataprotectionlead@remarkable-autism.org. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

To exercise any of these rights, please contact our Data Protection Officer.

Complaints

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance by emailing dataprotectionlead@remarkable-autism.org.

To make a complaint, please contact our Data Protection Officer.

Alternatively, you can make a complaint to the Information Commissioner's Office: Report a concern online at <https://ico.org.uk/concerns/>, call 0303 123 1113 or write to:

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

Contact us

We hope that the Data Protection Lead can resolve any query you raise about our use of your information in the first instance.
(Email: dataprotectionlead@remarkable-autism.org)

We have appointed a data protection officer (DPO) to oversee compliance with data protection and this privacy notice. If you have any questions about how we handle your personal information which cannot be resolved by the Data Protection Lead, then you can contact the DPO using the details below: -

Data Protection Officer: Judicium Consulting Limited
Address: 72 Cannon Street, London, EC4N 6AE
Email: dataservices@judicium.com
Web: www.judiciumeducation.co.uk
Lead Contact: Craig Stilwell

You have the right to make a complaint at any time to the Information Commissioner's Office, the UK supervisory authority for data protection issues.

Changes to this Privacy Notice

We reserve the right to update this privacy notice at any time, and we will 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.