



Royal Association for Deaf people

Employee privacy notice

Click [here](#) for a BSL version of this policy

Purpose and scope

This privacy notice explains how we use the personal information about you that we collect in the course of your employment with us, in accordance with the General Data Protection Regulation (GDPR).

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

This notice applies to all employees, volunteers and contractors.

The data protection principles

As your employer, RAD is a data controller, as defined by the GDPR. This means that we are responsible and accountable for deciding how we hold and use personal information about you.

In addition, the GDPR requires that the personal information we hold about you must be:

1. Used lawfully, fairly and in a transparent way.
2. Collected only for valid purposes that we have clearly explained to you.
3. Relevant to the purposes we have told you about and limited only to those purposes.
4. Accurate and kept up to date.
5. Kept only as long as necessary for the purposes we have told you about.
6. Kept securely.

The kind of information we hold about you

Personal data means any information about an individual which allows that individual to be identified.

We collect, store and use the following categories of personal data:

- Personal contact details such as name, title, addresses, telephone numbers and personal email addresses
- Date of birth
- Gender
- Marital status
- Next of kin and emergency contact information
- National Insurance number
- Bank account details, payroll records and tax status information
- Salary, annual leave, pension and benefits information
- Location of employment or workplace
- Copy driving licences and vehicle information
- Recruitment information, including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process

- Employment records, including job titles, work history, working hours, training records supervision notes, appraisal documents and membership of professional bodies
- Personal bibliographies and marketing profiles
- Performance information
- Disciplinary and grievance information
- Information about your use of our IT and communication systems
- Photographs

How we use your personal data

Under the GDPR, RAD will process your personal data for the following reasons:

- To fulfil our employment contract
- To carry out legally required duties
- For our legitimate interests
- To protect your interests
- Where something is done in the public interest

Special categories of information

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

- Information about your race or ethnicity and sexual orientation
- Information about your health
- Information about criminal convictions and offences

Article 9 of the GDPR only allows the processing of special categories of sensitive information in certain circumstances. We may process special categories of personal information as follows:

- In limited circumstances, with your explicit written consent
- Where we need to carry out our legal and health and safety obligations
- Where processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health
- 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 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.

How is your personal information collected?

We typically collect personal information about employees, workers and contractors through the application and recruitment process, either directly from candidates or sometimes from an employment agency or background check provider.

Reviewed by The Office of the Chief Executive

Date: July 2020

We may also collect personal information from third parties (such as references) and may collect personal information during your employment through job related activities.

Do we need your consent?

We do not need your consent if we use personal information, including special categories of personal information, to carry out our legal obligations or to exercise specific rights in the field of employment law.

We may, in limited circumstances, approach you for your written consent to allow us to process certain sensitive personal data. If we do so, we will 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 employment contract that you have to consent to any request that we make.

Information about criminal convictions

We will only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our legal obligations and in accordance with the GDPR.

Data sharing

Do we share data with third parties?

We may have to share your data with third parties explicitly in accordance with contractual requirements, including third-party service providers.

We require third parties to respect the security of your data and treat it in accordance with the law. We will inform you if we do share data. You are entitled to expect that third party to apply a similar level of protection in respect of your personal information.

Why might you share my personal information with third parties?

We may share your personal information with third parties where required by law, see below for further information:

Which third party service providers process my personal information?

'Third parties' include contractors and agents who may carry out services on our behalf such as payroll, pension administration, benefits provision and administration and IT services.

How secure is my information with third party service providers?

All our third-party service providers are required to take appropriate security measures to protect your personal information. We do not allow our third-party service providers to use your

personal data for their own purposes. We only permit them to process your personal data in adherence to contractual and specified purposes and in accordance with our instructions.

What about other third parties?

We may share your personal information with other third parties, for example when the provision of a service is coming to an end and staff information will be shared during the tender process under TUPE regulations. We may also need to share your personal information with a regulator or to otherwise comply with the law e.g. sharing tax and N.I. information with HMRC.

Data security

We have put in place measures to protect the security of your information.

Third parties will only process your personal information on our instructions. We will ensure that they agree to treat your information as confidential and keep it secure.

We have 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 information on our instructions and they are subject to a duty of confidentiality.

Data retention

We will only retain your personal information for as long as necessary to fulfil the purposes we collect it for, including for the purposes of satisfying any legal, insurance, accounting or reporting requirements. Details of retention periods for different aspects of your personal information are available in the section headed 'retention' of the data protection policy which is available on Cascade. T

When determining the appropriate retention period for personal data, we consider the amount, nature and sensitivity of the personal data, the potential risk or 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, insurance and compliance requirements.

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. Also, during the course of your work at RAD we may use photos for our website/leaflets and other official RAD publications which may remain in place after leaving employment with RAD.

Once you are no longer a RAD employee, worker or contractor we will retain and securely destroy your personal information in accordance with our data retention policy if we no longer have a legitimate reason for retaining it.

Rights of access, correction, erasure and restriction

Your duty to inform us of changes

It is important that the personal information we hold about you is accurate and current. Please keep us informed and make appropriate changes within the Cascade database, if your personal information changes during your working relationship with us.

Your rights in connection with personal information

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

- **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
- **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
- **Request erasure** of your personal information. This enables you to ask us to delete or remove your 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
- **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
- **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
- **Request the transfer** of your personal information to another party

Should you wish to review, verify or 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 HR officer in writing.

No fee is usually required

You will 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

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

On the limited occasions that RAD may obtain your consent to process personal data you will have the right to withdraw that consent at any time. To withdraw consent, you will need to contact the HR officer. Unless there is a legitimate lawful basis for RAD continuing to process the data, RAD will then cease specific processing of your personal data.

Data breaches

We are required under the GDPR to notify you without delay of any data breach which is likely to result in a high risk to your rights and freedoms.

Your right to complain

Complaints about the way in which your data has been handled should be made in line with RAD's grievance policy. You also have the right, in certain circumstances, to report concerns about data management to the [Information Commissioner's Office](#) .

Data protection lead

We have appointed a data protection lead to oversee compliance with this privacy notice. Our data protection lead is the office of the CEO.

If you have any questions about this privacy notice or how we handle your personal information, please email ceo@royaldeaf.org.uk. You may alternatively send your query to dataprotection@royaldeaf.org.uk .

Changes to the privacy notice

We reserve the right to update this privacy notice at any time, and we will provide you with updated versions when we make substantial updates.

Associated policies

Grievance policy

Complaints policy