

**Job Applicant Privacy Notice**

The College is a “data controller” in relation to personal data. This means that we are responsible for determining how we hold and use personal information about you.

As Data Controller, we are obliged to inform you of the types of data we collect and hold about you, in this instance for the purposes of the recruitment exercise. This privacy information also sets out how we use your information, how long we keep it for and other relevant information about your data. It provides you with certain information that must be provided under the UK General Data Protection Regulation (UK GDPR).

**Data protection principles**

Please see the [RCOG Data Protection Policy](https://www.rcog.org.uk/en/about-us/policies/data-protection-policy/) for details. In summary, the College commits to processing your personal data in compliance with the **data protection principles**.

This means that the personal information we hold about you will be:

1. Used fairly, lawfully and in a transparent way.
2. Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
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 for only as long as necessary for the purposes we have told you.
6. Kept securely.

**Types of personal data we hold about you**

In connection with your application for work with us, we may collect, hold and use the following types of personal data about you:

* Information included on your CV and covering letter including references, education history, employment history and qualifications.
* Information provided as part of the application process including your name, title, address, email address, phone numbers, date of birth and gender.
* Any information you provide to us during an interview.
* Documentation relating to your right to work in the UK.
* Your photograph or digital image.

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

* Information about your race or ethnicity, religious or philosophical beliefs and sexual orientation.
* Information about your health, including any medical condition.
* Information about criminal convictions and offences.

**How we collect your personal data**

We collect personal data about candidates from the following sources:

* You, the candidate. We use Applied, an anonymised applicant tracking system (ATS) from Be Applied Ltd, to process recruitment applications. Applied will seek consent to process your personal data as outlined above. With your explicit consent, they may use this data for statistical analysis and research purposes The College is not responsible for Applied’s privacy notice therefore, please [see Applied’s privacy notice](https://www.beapplied.com/privacy) for further details on how information is processed and used. Applied’s Privacy Policy can be found at <https://www.beapplied.com/privacy>

This is likely to include the information you would normally include in a CV or a job application cover letter, or notes made by our recruiting officers during any recruitment application or interview process. Other details may be collected directly from you in the form of official documentation such as copies of your driving licence, passport or other right to work evidence.

* In some cases, we collect data about you from appropriate third parties. This may include:
	+ Employment or recruitment agencies, from which we collect the following categories of data including home address, education history, employment history and qualifications.
	+ Former employers and other named referees, from whom we collect the following categories of data including the dates of employment and job title.
	+ If applicable to the role in question, the Disclosure and Barring Service in respect of criminal convictions.

Your personal information is stored securely within the Applied ATS. The RCOG has a contract with Applied and assurance that your data is stored in accordance with data protection laws. Applied’s Privacy Policy can be found at https://www.beapplied.com/privacy

**Disability Confident scheme**

We are committed to supporting applicants with disabilities and are a member of the Disability Confident employer scheme. As part of the commitment we will ask you to voluntarily declare if you have a disability. We guarantee an interview for candidates with disabilities who meet the minimum essential scoring criteria. The data collected will be kept anonymously, treated confidentially and processed in line with our data retention and processing policy as outlined in this notice.

**Why we use information about you**

We use the personal information we collect about you to:

* Assess your skills, qualifications, and suitability for the role.
* Carry out background and reference checks, where applicable.
* Communicate with you about the recruitment process.
* Keep records related to our hiring processes.
* Comply with legal or regulatory requirements.
* Monitor and assess demographics anonymously

It is in our legitimate interests to decide whether to appoint you to the role in question, since it would be beneficial to our business to appoint someone to that role.

We also need to process your personal information to decide whether to offer you the role and subsequently enter into a contract of employment with you.

**How we use particularly sensitive personal information**

Particularly sensitive personal information, or “special category data”, includes, for example, information relating to your:

* health,
* racial or ethnic origin,
* sexual orientation,
* religion or philosophical belief.

We use your special category data in the following ways:

* We use information about disability status to consider whether we need to provide appropriate adjustments during the recruitment process, for example whether adjustments need to be made during an interview or test.
* We use information about your race or ethnic origin, sexual orientation and religion or philosophical beliefs for the purposes of meaningful equal opportunities monitoring and reporting.
* anonymised data will be used to monitor demographics to improve diversity at RCOG

We do not need your consent if we use special categories of personal data in order to carry out our legal obligations or exercise specific rights under employment law. However, we may ask for your consent to allow us to process certain particularly sensitive data. If this occurs, you are made fully aware of the reasons for the processing. As with all cases of seeking consent from you, you have full control over your decision to give or withhold consent and there are no consequences where consent is withheld. Consent, once given, may be withdrawn at any time. There are no consequences where consent is withdrawn.

**Criminal conviction data**

We may process information about criminal convictions.

We only collect such data where it is appropriate and necessary, given the nature of the role in question and where the law permits us to do so. This data is usually collected at the recruitment stage, if we would like to offer you the role (conditional on checks and any other conditions, such as references, being satisfactory).

We may be required to carry out a criminal records check, for specified roles, in order to satisfy ourselves that there is nothing in your criminal convictions history, which makes you unsuitable for the role.

**If you do not provide your data to us**

One of the reasons for processing your data is to allow us to carry out an effective recruitment process.

Whilst you are under no obligation to provide us with your data, if you fail to provide information when requested, which is necessary for us to consider your application (such as evidence of qualifications or work history), we may not able to process or continue with your application.

By way of further example, if we require a credit check or references for this role and you fail to provide us with relevant details, we will not be able to take your application further.

**Sharing your data**

Your data is only shared with:

* Our applicant tracking system, Applied. They will also seek your consent to process your personal data for their research and marketing purposes but you are not obliged to do so and this will not affect your application in any way. This is a different processing purpose to that of the College hence the need for your consent. As such, the College is not responsible for Applied’s privacy notice therefore, so please [see their privacy notice](https://www.beapplied.com/privacy) for full details on how they would like to process and use your personal information.
* colleagues within the College where and to the extent that it is necessary for them to undertake their duties with regard to recruitment. This includes, for example, the HR department, those in the department where the vacancy is who are responsible for screening your application and interviewing you, and the IT department where you require access to our systems to undertake any assessments requiring IT equipment; and
* legitimate partners contracted by the College to process your data on our behalf, such as Applied (the supplier of the College’s applicant tracking system. All such partners have contracts that comply with data protection law.

When we only share your personal information with legitimate third parties for the purposes of processing your job application – for example:

* *named referees to obtain references as part of the recruitment process.*
* *Applied our applicant tracking system .*

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 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 for specified purposes and in accordance with our instructions.

We aggregate your special category data from alongside all applicants and anonymise it so we can track trends, which we then share with partners to the College who assist us in improving our employment practices. You will not be identifiable from these datasets.

Transferring information outside the UK

Please see the [RCOG Privacy Policy](https://www.rcog.org.uk/en/legal/privacy-policy-cookies/). In summary:

The College is an international organisation so we process and transfer personal information with the EU/EEA and across the World.

We ensure adequate safeguards are in place to process and transfer your personal information securely.

**Data Security**

Please see the [RCOG Privacy Policy](https://www.rcog.org.uk/en/legal/privacy-policy-cookies/). In summary:

The College is certified by the Cyber Essentials Plus security accreditation, which is audited every year. We ensure all our partners processing personal information on our behalf meet the same or equivalent standards.

This means 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. Details of these measures are available upon request.

In addition, we limit access to your personal information to only those employees, agents, contractors and other third parties who have a business need-to-know.

Where we share your personal data with third parties, we require them to ensure that your data is only processed on our instructions, is treated as confidential and is kept securely and in line with data protection requirements. Third parties must implement appropriate technical and organisational measures to ensure the security of your data.

We have established 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.

**Data retention**

In line with data protection principles, we only keep your data for as long as is necessary to fulfil the purposes for which we collected it. The length of time we retain your data partly depends on whether or not you are successful in obtaining employment with us.

If your application is successful, your data is kept on your employee record for the duration of your working relationship with us, and is transferred to the systems we administer for employees. We have a separate privacy notice for employees and workers, which is provided to you on commencement of employment.

If your application is not successful, we will keep your data for the period of six months in accordance with the [RCOG Retention Schedule](https://www.rcog.org.uk/globalassets/documents/about-us/policies/rcog-retention-schedule.pdf) once the recruitment exercise ends and we have communicated to you our decision about whether to appoint you to the role in question. We retain your personal information for that period so that we can show, in the event of a legal claim, that we have not discriminated against candidates on prohibited grounds and that we have conducted the recruitment exercise in a fair and transparent way. After this period, we will securely destroy your personal information in accordance with the [RCOG Retention Schedule](https://www.rcog.org.uk/globalassets/documents/about-us/policies/rcog-retention-schedule.pdf).

We retain statistical information to help inform our recruitment activities and improve diversity at the College. This information retained is anonymised and no individuals may be identified from this data.

**Automated decision-making**

No decision about you, which has a significant impact on you, is made solely on the basis of automated decision making (i.e. using an electronic system without human involvement).

**Your rights in relation to your data: access, correction, erasure and restriction**

Please see the [RCOG Privacy Policy](https://www.rcog.org.uk/en/legal/privacy-policy-cookies/) and [Individual Rights Requests guidance](https://www.rcog.org.uk/en/about-us/policies/data-protection-policy/individual-rights-requests/) for further details.

The law on data protection gives you certain rights in relation to the data we hold on you. These are:

* **The right to be informed.** This means that we must tell you how we use your data, and this is the purpose of this privacy notice
* **The right of access.** You have the right to request access to the personal information that we hold about you (commonly known as a “data subject access request”). This enables you to receive a copy of the information we hold about you and to check that we are lawfully processing it.
* **The right for any inaccuracies to be corrected.** If any personal information that we hold about you is incomplete or inaccurate, you are able to require us to correct it.
* **The right to have information deleted.** If you would like us to delete or remove the personal information we hold about you, you have the right to ask us to delete it from our systems where you believe there is no good reason for us to continue processing 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).
* **The right to object to the processing of your personal information**. You have the right to object to the 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.
* **The right to request restriction of the 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.
* **The right to request transfer.** You may request the transfer the personal information that we hold about you to another party.

If you wish to exercise any of the rights explained above, please see the RCOG [Individual Rights Requests guidance](https://www.rcog.org.uk/en/about-us/policies/data-protection-policy/individual-rights-requests/) or contact: *dataprotection@rcog.org.uk**.*

**Data Protection Officer**

We are a small organisation with less than 250 employees so we do not have a Data Protection Officer. This function is shared between the Senior Information Risk Officer (SIRO) and the Deputy SIRO. They are responsible for overseeing compliance with this privacy notice*.* If you have any questions about this privacy information or how we handle your personal information the SIRO and Deputy SIRO can be contacted on: dataprotection@rcog.org.uk.

The supervisory authority in the UK for data protection matters is the Information Commissioner’s Office (ICO). If you think your data protection rights have been breached by us, you are able to make a complaint at any time to the ICO.