



Data Protection Statement – Candidates for election to College memberships and applicants for academic posts

How we use your personal information

This statement explains how Trinity Hall (the “College”, “we” and “our”) handles and uses information we collect about applicants (“you” and “your”) for academic posts, senior memberships and Fellowships. In broad terms, we use your data to manage your application to the College and our subsequent recruitment or election processes.

The controller for your personal data is the Trinity Hall, Trinity Lane, Cambridge CB2 1TJ.

The designated Data Protection Officer appointed by the College under UK GDPR is Intercollegiate Services Limited (ISL, dpo@isl.colleges.cam.ac.uk).

Your primary contact for all data protection matters is the Governance and Compliance Officer, on compliance@trinhall.cam.ac.uk. This is the same address to contact if you want to exercise any of your data protection rights, including requesting copies of personal data the College holds about you, or making a complaint about how the College has managed your personal data.

The legal basis for processing your personal data is that it is necessary either in order for you to enter into a contract of employment with us, or for you to enter into membership of the College, where you will be subject to the College’s governing documents.

How your data is used by the College

Your data is used by us for in the first instance solely for the purposes of considering your suitability for employment or election and for us to manage our recruitment processes, including our monitoring of equality and diversity within the College.

If you have concerns or queries about any of these purposes, or how we communicate with you, please contact the Compliance Officer at the email address given above.

The College holds the following personal data relating to you, in line with the purposes above:

- personal details, including name, contact details (phone, email, postal)*;
- your application form and associated information submitted by you at that time*;
- other data relating to your recruitment (including references we take up as part of the recruitment process, any pre-employment assessment of you, and any assessment of you at an informal or formal interview);
- any occupational health assessments and/or medical information you have provided, and related work requirements*;
- evidence of your right to work in the UK (e.g. copies of your passport)*;
- information relating to your age, nationality, gender, religion or beliefs, disability and ethnicity*;any correspondence relating to the outcome of the recruitment process (either successful or unsuccessful).

We will not access personal data about you from social media sites, unless there is a legitimate interest for us to do so (for example, the role you have applied for has a significant public-facing element to it, or is involved with publicity and presenting us to the general public). Consequently, we do not routinely screen applicants' social media profiles but, if aspects of your social media profile are brought to our attention and give rise to concerns about your suitability for the role in question, we may need to consider them.

For certain posts, we may use the Disclosure and Barring Services (DBS) and/or Disclosure Scotland to help assess your suitability for certain positions of trust. If this is the case, we will make this clear to you in separate correspondence. Certificate and status check information is only used for this specific purpose, and we comply fully with the DBS Code of Practice regarding the correct use, handling, storage, retention and destruction of certificates and certificate information. We recognise that it is a criminal offence to pass this information on to anyone who is not entitled to receive it.

Who we share your data with

Information is not shared with other third parties without your written consent. Generally, personal data is not shared outside of the European Economic Area.

If you are successful in your application, the data is subsequently held as part of your employment or membership record with us.

If you are unsuccessful in your application, we retain all data and information for no more than twelve months after the closing date of the application process.

In either case, where the post has required a “resident market test” (needed if the post is open to applicants from outside the European Economic Area), the College will retain the application records of any shortlisted candidates for the duration of the sponsored post and twelve months thereafter.

Your rights

You have the right:

- to ask us for access to, rectification or erasure of your data;
- to restrict processing (pending correction or deletion); and
- to ask for the transfer of your data electronically to a third party (data portability).

Some of these rights are not automatic, and we reserve the right to discuss with you why we might not comply with a request from you to exercise them.

Failure to provide the information reasonably requested of you may result in an automatic disqualification from the recruitment process.

You retain the right at all times to lodge a complaint about our management of your personal data with the Information Commissioner's Office at <https://ico.org.uk/concerns/>