



Data Protection Statement for Job Applicants and Applicants for Senior Membership

How we use your personal information

This statement explains how St Edmund's College ("we" and "our") handles and uses information we collect about applicants ("you" and "your") for jobs, 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, including assessing your suitability, communicating with you, taking up references where appropriate, and meeting legal and regulatory requirements.

This Data Protection Statement is reviewed regularly and updated where necessary to reflect changes to the College's processing activities, including where personal data is used for a new or materially different purpose.

The controller for your personal information is St Edmund's College, Mount Pleasant, Cambridge CB3 0BN. The Data Protection Officer for the College is Intercollegiate Services Limited (ISL) (64 Bridge Street, Cambridge CB2 1UR; 01223 768745; dpo@isl.colleges.cam.ac.uk). ISL should be contacted if you have any concerns about how the College is managing your personal information, or if you require advice on how to exercise your rights as outlined in this statement.

The person within the College with overall responsibility for the protection of information is the Senior Information Risk Owner, who at the time of issue is the Bursar. The Bursar can be contacted at bursar@st-edmunds.cam.ac.uk. Day-to-day responsibility for monitoring compliance with relevant legislation and dealing with concerns relating to the College's data protection arrangements sits with the College Data Protection Lead, who at the time of issue is the Governance, Risk & Compliance Manager. The Governance, Risk & Compliance Manager is the primary contact for all data protection matters and can be contacted at grcm@st-edmunds.cam.ac.uk. This is also the address to use if you wish 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 in order to take steps prior to entering into an employment contract with us, engagement or other working arrangement with us, or in order to consider your application for senior membership or Fellowship of the College, where you will be subject to the College's governing documents. In some cases, we may also process personal data because it is necessary for compliance with a legal obligation, for example right to work checks, or because it is necessary for the College's legitimate interests, for example managing fair and effective recruitment, selection and election processes. Where we process special category data, such as health, disability, religion or belief, sexual orientation or ethnicity information, we will also identify an appropriate condition under Article 9 UK GDPR. Where we process criminal offence data, including DBS or Disclosure Scotland information, we will do so only where authorised by law and subject to appropriate safeguards.

How your data is used by the College

Your data is used by us in the first instance for the purposes of considering your suitability for employment or election and for us to manage our recruitment, selection or election processes, including our monitoring of equality and diversity within the College, complying with legal obligations, communicating with you, and keeping appropriate records of the process and outcome.

If you have concerns or queries about any of these purposes, or how we communicate with you, please contact us at the address given below.

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 address);
- *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 or other relevant identity or immigration documents);
- *information relating to your age, nationality, and gender, and, if you have provided us with it, information relating to your religion or beliefs, sexual orientation and ethnicity which we do not otherwise routinely collect;
- any correspondence relating to the outcome of the recruitment, selection or election process (either successful or unsuccessful).

Those marked with an * relate to information provided by you. Other data and information is generated by us or, where self-evident, provided by a third party, such as referees, recruitment agencies, occupational health providers, DBS or Disclosure Scotland, professional advisers or relevant public bodies. Where the College uses an external recruitment agency to support a recruitment, selection or appointment process, the agency may provide the College with recruitment-related information about you, including application details, assessment information, correspondence and other information relevant to the role or membership category for which you have applied.

Where we process equality and diversity information, this will normally be used for monitoring, reporting and supporting fair recruitment and selection processes. Where appropriate, it will be used in anonymised or aggregated form.

We will not normally access personal data about you from social media sites, unless there is a lawful, fair and proportionate basis 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 where it is lawful, necessary and proportionate to do so.

If you attend College premises as part of a recruitment, selection or election process, you may be captured by CCTV or Automatic Number Plate Recognition (ANPR) systems. These may capture images of individuals and, in the case of ANPR, vehicle registration marks. CCTV and ANPR are used for purposes including safety and security, crime prevention and detection, protection of College buildings, assets and information, management of emergencies and incidents, health and safety, and parking management and enforcement. Routine CCTV and ANPR recordings are normally retained for no more than 30 days, unless they are required in connection with an incident, investigation, legal claim or other lawful purpose. Our CCTV and ANPR policy can be viewed at www.st-edmunds.cam.ac.uk/data-protection.

For certain posts, we may use the Disclosure and Barring Service (DBS) and 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. DBS and Disclosure Scotland information may include criminal offence data and will be handled only where authorised by law and subject to appropriate safeguards.

Who we share your data with

If you have applied for a post using CASC (Colleges' Administrative Software Consortium) Fellowship Application System, please see their [Data Protection Statement](#).

If recruitment to the post or membership category to which you are applying is being undertaken or supported by an agent, external recruitment agency or other service provider of the College, which may include CASC, we may share relevant personal data with that agent, agency or service provider where necessary for the recruitment, selection, appointment or election process. This may include your application details, contact information, assessment information, interview arrangements and outcome information. Where a third party processes personal data on the College's behalf, appropriate contractual or data protection arrangements will be in place. Information is not shared with other third parties unless this is necessary and lawful, for example to administer the recruitment, selection or election process, take up references, obtain occupational health or professional advice, comply with legal obligations, conduct right to work or suitability checks, manage insurance or legal claims, respond to lawful requests from public authorities, or otherwise support the proper operation of the College. Where personal data is transferred outside the UK and the UK GDPR transfer rules apply, the College will ensure that an appropriate transfer mechanism and any required safeguards are in place. If you are successful in your application, the data is subsequently held as part of your employment, engagement or membership record with us and will be handled in accordance with the relevant Data Protection Statement for staff, members or other applicable category.

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, unless a longer period is necessary and lawful, for example in connection with a complaint, investigation, safeguarding matter, insurance claim, legal claim, regulatory enquiry or other lawful purpose.

Where the post or engagement involves immigration, right to work or sponsorship requirements, the College may retain relevant application and recruitment records for the period required to comply with applicable immigration, sponsorship and audit obligations, and for a reasonable period thereafter where necessary and lawful.

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); to ask for the transfer of your data electronically to a third party (data portability); and to object to processing in certain circumstances. 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 where the law allows us to do so.

Where information is reasonably required to consider your application, manage the recruitment, selection or election process, or comply with legal obligations, failure to provide it may mean that the College is unable to progress your application. In appropriate cases, this may result in your application being withdrawn from the process.

Complaints

If you are concerned about how the College has handled your personal data, you may raise this with the College Data Protection Lead, the SRO or the DPO using the contact details above. The College will consider data protection complaints fairly and proportionately, and will normally acknowledge receipt within 30 days.

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