St Edmund's College
University of Cambridge

Data Protection Statement for Staff

How we use your personal information

This statement explains how St Edmund's College ("we" and "our") handles and uses information we collect about our staff ("you" and "your"). For these purposes, "staff" is intended to include employees, workers and casual workers and contractors (e.g. ad-hoc or temporary maintenance, kitchen or catering staff etc.) In broad terms, we use your data to manage your employment, engagement or other working relationship with the College, including your role and the performance of it, how we support you as an employer, and how you are paid, as well as other legal, statutory 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. When changes are made to this statement, we will publish the updated version on our website and notify you by other communications channels as we deem appropriate or necessary.

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.

Unless otherwise stated, the legal basis for processing your personal data is that it is necessary for the performance of the employment contract or other working arrangement we hold with you, or because it is necessary for the College to comply with legal obligations (e.g. processing your monthly salary, tax and pension contributions). In some cases, we may also process personal data because it is necessary for the College's legitimate interests, for the performance of tasks carried out in the public interest or in the exercise of official authority, or to protect vital interests. Where we process special category data, such as health information or equality and diversity 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 for a number of purposes, including:

A. supporting your employment and your performance in your role. Such personal data includes:

- *personal details, including name, contact details (phone, email, postal, both work and personal) and photograph;
- your current and any previous role descriptions;
- your current and any previous contracts of employment and related correspondence;
- any occupational health assessments and medical information you have provided, and related work requirements; and
- *your training and development qualifications, requests and requirements.

B. ensuring that you have the right to work for the College. Such personal data includes:

- *your recruitment information (including your original application form and associated information submitted at that time);
- other data relating to your recruitment (including your offer of employment and related correspondence, references we took up on your appointment, and any pre-employment assessment of you); and
- *evidence of your right to work in the UK (e.g. copies of your passport).

C. paying and rewarding you for your work. Such personal data includes:

- *your bank details;
- *details of your preferred pension scheme;
- your current and previous salary and other earnings (e.g. maternity pay, overtime), and the amounts you have paid in statutory taxes; and
- correspondence between you and the College, and between members and staff of the College, relating to your pay, pension, benefits and other remuneration.

In addition, we maintain records of your use or take-up of any benefit schemes provided by us, which we collate and monitor to review the effectiveness of these staff benefits. The legal basis for this processing is that it is in our legitimate interest to ensure that any staff benefit schemes represent good value for money to both you and us, and to administer those schemes fairly, consistently and in accordance with any applicable eligibility criteria or limits.

D. administering HR-related processes, including records of absences and regular appraisals of your performance and, where necessary, investigations or reviews into your conduct or performance. Such personal data includes:

- *records of your induction programme and its completion;
- *records of your performance appraisals with your line manager;
- records, where they exist, of any investigation or review into your conduct or performance;
- records of absences from work (including but not limited to annual leave entitlement, sickness leave, parental leave and compassionate leave); and
- correspondence between you and the College, and between members and staff of the College, regarding any matters relating to your employment and any related issues (including but not limited to changes to duties, responsibilities and benefits, your

retirement, resignation or exit from the College and personal and professional references provided by the College to you or a third party at your request).

E. maintaining an emergency contact point for you. Such personal data includes details of your preferred emergency contact, including their name, relationship to you and their contact details.*

F. monitoring equality and diversity within the College. Such personal data includes information relating to your age, nationality, gender, religion or beliefs, sexual orientation and ethnicity.* Where this involves special category data, it will be handled subject to additional safeguards and, where appropriate, used in anonymised or aggregated form for monitoring and reporting purposes.

G. disclosing personal information about you to external organisations, as permitted or required by law.

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.

Data marked with an * above relate to information provided by you, or created in discussion and agreement with you. Other data and information is generated by the College or, where self-evident, provided by a third party, such as referees, occupational health providers, pension providers, government bodies, professional advisers or other relevant organisations.

We will not normally monitor social media sites for any personal data relating to you, unless we consider that there is a lawful, fair and proportionate basis for us to do so (e.g. monitoring compliance with an agreed plan, such as a homeworking agreement) and only if we inform you we might do this in advance. Consequently, we do not routinely screen your social media profiles but, if aspects of these are brought to our attention and give rise to concerns about your conduct, we may need to consider them where it is lawful, necessary and proportionate to do so.

We also operate CCTV and Automatic Number Plate Recognition (ANPR) on our sites. 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 roles, the College may carry out criminal records checks through the Disclosure and Barring Service (DBS) or Disclosure Scotland where this is relevant and appropriate to the nature of the role. Such checks will only be undertaken where there is a lawful basis for doing so, for example where the role is eligible for a check under applicable legislation or, where this is not a legal requirement, where the College has identified a legitimate interest in carrying out the check and has considered the data protection implications. Where a check is required, the College will make this clear during the recruitment process and will specify the type of check to be undertaken. The College may use an approved third-party provider to administer DBS checks on its behalf. Any certificate information, status check information or related criminal records data will only be used for the specific purpose for which it was obtained and will be handled in accordance with the College's data protection obligations and, where applicable, the DBS Code of Practice, including requirements relating to use, handling, storage, retention

and destruction. The College recognises that criminal records information must be handled with particular care and will only be disclosed to those who are authorised to receive it.

Who we share your data with

We may publish your name, and where appropriate, photograph (if you have provided one) in College on a photoboard, and for certain senior staff your name, photograph, your email and College contact phone number may be published on our website and elsewhere where this is relevant to your role and the effective operation of the College.

We share your personal information where necessary and appropriate across the collegiate University. The University and its partners (including all of the Colleges) have a data sharing protocol to govern the sharing of staff and members' personal information. This is necessary because they are distinct legal entities. The parties may share any of the above categories of personal information. Any transmission of information between partners is managed through agreed processes that comply with UK data protection legislation.

We share relevant personal data with our service providers and processor (including but not limited to payroll and health and safety) and with relevant government agencies (e.g. HMRC) and your pension provider. Information is not shared with other third parties without your written consent, unless this is necessary and lawful, for example to administer your employment or engagement, comply with legal obligations, protect vital interests, support health and safety, obtain professional advice, manage insurance or legal claims, respond to lawful requests from public authorities, or otherwise support the proper operation of the College. Generally, personal data is not routinely transferred outside the UK. Where a transfer outside the UK takes place and the UK GDPR transfer rules apply, the College will ensure that an appropriate transfer mechanism and any required safeguards are in place.

We hold all information for the duration of your employment and for no more than twelve months after the end of your employment. After that time, we retain a small subset of personal data for up to seven years after your relationship with the College ends, in accordance with the College's Retention Schedule, unless a longer retention period is necessary and lawful:

This subset may include, where appropriate:

- *personal details, including name and your preferred personal contact details (if we still have these);
- your previous salaries and other earnings, pensions and the amounts you have paid in statutory taxes;
- records of your performance appraisals with your line manager;
- records, where they exist, of any investigation or review into your conduct or performance;
- your reasons for leaving and any related correspondence;
- any references we have written subsequent to your employment with us.

Those marked with an * relate to information provided by you, or created in discussion and agreement with you.

We reserve the right to retain personal data longer than the periods stated above, where it becomes apparent that there is a need to do so – for example, in the event of a major health or personal injury

incident, records may need to be kept for up to forty years , or where records are required for a complaint, investigation, grievance, disciplinary process, safeguarding matter, insurance claim, legal claim, regulatory enquiry or other lawful purpose.

We then store in a permanent archive your full name and title, and your job title(s) or College affiliation(s) and the corresponding dates of employment/membership for historical and archival purposes.

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 for your employment or engagement, or for the College to comply with its legal obligations, failure to provide it may mean that the College is unable to administer your employment or engagement properly. In appropriate cases, this may lead to action under relevant College procedures.

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 SIRO 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.