CHRIST'S COLLEGE
UNIVERSITY OF CAMBRIDGE

Data protection statement – staff and senior members

How we use your personal information

This statement explains how Christ's College ("the College", "we" and "our") handles and uses information we collect about our staff and senior members/Fellows ("staff", "you" and "your"). For these purposes, "staff" is intended to include office holders, employees, workers, casual workers and contractors (including undergraduate supervisors, ad-hoc or temporary maintenance, kitchen and catering staff etc.) In broad terms, we use your data to manage your employment and/or membership 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 statutory requirements.

The controller for your personal data is Christ's College, St Andrew's Street, Cambridge CB2 3BU. The person within the College responsible for data protection, and the person who is responsible for monitoring compliance with relevant data protection legislation, is the Bursar, Michael Parsons, bursar@christs.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.

The Data Protection Officer for the College is Intercollegiate Services Limited (ISL), 64 Bridge Street, Cambridge CB2 1UR; email: 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.

Unless otherwise stated, the legal basis for processing your personal data is that it is necessary for the performance of the employment contract or agreement we hold with you, or for statutory purposes (e.g. processing your monthly salary, tax, and pension contributions).

How your data is used by the College

Your data is used by us for several purposes, including:

A. supporting your employment and your performance in your role:

Personal data includes:

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

B. ensuring that you have the right to work for the College:

Personal data includes:

(i)* your recruitment information (including your original application form and associated information submitted at that time);
(ii) 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);
(iii)* evidence of your right to work in the UK (e.g. copies of your passport).

C. paying and rewarding you for your work:

Personal data includes:

(i)* your bank details;
(ii)* details of your preferred pension scheme;
(iii) your current and previous salary and other earnings (e.g. maternity pay, overtime), and the amounts you have paid in statutory taxes;
(iv) 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 (e.g. healthcare), 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 ensure that you do not overuse your entitlements.

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:

   Personal data includes:

   (i)* records of your induction programme and its completion;
   (ii)* records of your performance appraisals with your line manager;
   (iii) records, where they exist, of any investigation or review into your conduct or performance;
   (iv) records of absences from work (including but not limited to annual leave entitlement, sickness leave, parental leave and compassionate leave)
   (v) correspondence between you and the College, and between members and staff of the College, regarding any matters relating to your employment and/or membership 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:

   Personal data includes details of your preferred emergency contacts, including their name, relationship to you and their contact details.*

F. monitoring equality and diversity within the College:

   Personal data may include information relating to your age, gender, sexual orientation, marital status, religion or belief, race, ethic or national origin and any disability including neurodiversity and caring responsibility for someone with protected characteristics. *

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 above. Data marked with an * 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.

We do not routinely screen your social media profiles but, if aspects of these are brought to our attention and give rise to concerns, we may consider them. Our social media guidelines for staff are available on the College HR system which is linked from: https://intranet.christs.cam.ac.uk/information-college-staff.

We also operate CCTV on our site, which will capture footage of you. Our CCTV policy can be viewed at https://www.christs.cam.ac.uk/college-administrative-information-and-policy-documents.

For certain posts, we may use the Disclosure and Barring Services (DBS) and Disclosure Scotland to conduct a criminal record check, and we may also conduct other pre-employment checks (specifically we may ask for proof of qualifications, training or licences required for the job role). If this is the case, we will make this clear to you in separate correspondence and obtain your prior consent to conducting these checks. Please note that obtaining a satisfactory criminal record check is a legal requirement for holding certain roles at the College.

An up-to-date list of the roles which require a criminal record check and other pre-employment checks can be found in the attached addendum. Criminal record checks and other pre-employment checks are conducted to help the College assess your suitability to be appointed and/or continue your employment in one of the roles set out in its Safeguarding Policy. This information is only used for this specific purpose, and we comply fully with our own Data Protection Policy and the DBS code of Practice regarding the correct use, handling, storage, retention and destruction of this information. We recognise that it is a criminal offence to pass this information on to anyone who is not entitled to receive it.

We will use CareCheck as our agents to conduct criminal record and other pre- employment checks.

In almost all cases, criminal record and other pre-employment checks will be deleted once the results have been fully considered by the College and just a record of the date that the check was performed and whether it yielded a satisfactory or unsatisfactory result will be retained. The CareCheck service itself will delete its record after six months.

In exceptional circumstances, the College will retain a copy of the criminal record and other pre- employment checks where the results are relevant to your ongoing employment. In these circumstances, the checks will only be held for the period that you work for the College.

Who we share your data with

For senior members we would normally publish (on our website and elsewhere) your name, photograph (if you have provided one), and your email address and basic biographical information relating to your College and University posts.

We share relevant personal data with our sub-contracting agents and with relevant government agencies (e.g. HMRC) and your pension provider. Information is not shared with other third parties without your written consent, other than your name, role and employment contact

details which may be made publicly available. Generally, personal data is not shared outside of the United Kingdom.

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 of the College information. This is necessary because they are distinct legal entities. The parties may share any of the above categories of personal information, and the agreement can be viewed in full at https://www.ois.cam.ac.uk/policies-and-protocols/data-sharing-protocols. Any transmission of information between partners is managed through agreed processes that comply with UK data protection legislation.

We hold all staff information for the duration of your employment and for the year in which you leave plus seven years after the end of your employment. After that time all staff information is destroyed.

We reserve the right to retain the 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.

For senior members, we may hold information for the lifetime of the College. Basic information on staff serving for twenty-five years or more will be held which will include their photograph, name and period of employment.

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 disciplinary action taken by the College, which could ultimately lead to your dismissal from employment.

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/

Addendum - DBS Checks

The Disclosure and Barring Service (DBS) provides an online "DBS eligibility tool" to help determine whether a specific role is eligible for one of the three types of checks listed below.

Basic DBS check

- Shows unspent convictions and conditional cautions
- May be requested by self-employed people or employers who want to get a sense of a candidate's character

Standard DBS check

- Shows spent and unspent convictions, cautions, reprimands, and final warnings
- Commonly requested in industries that require security and legal checks

Enhanced DBS check

- Shows the same information as a standard check, plus any relevant information held by local police
- May be requested for roles that involve working with vulnerable people

Safeguarding

The following require enhanced checks:

- Director of Admissions
- Senior Admissions and Outreach Officer
- Admissions and Outreach Officer
- Chaplain
- College Nurse and Wellbeing Advisor
- College Nurse/Clinical Roles

The following require a basic check:

- College Porters
- Housekeeping Team
- Tutors
- Senior Tutor

Access or Handling of Sensitive Data

The following require **standard checks** (access to financial/IT data and systems):

- Financial roles – Bursar, Head of Finance, Management and Investment Accountant, Financial Accountant, Payroll and Pensions Manager, Purchase Ledger, Commercial Accountant
- HR roles – Head of HR, Assistant to Head of HR
- IT roles – IT Manager, Deputy IT Manager

The following require **basic checks** (access to personal and sensitive data e.g. applicants, students, alumni)**:**

- Tutorial staff members
- Admissions staff members (not specified above)
- Development staff members
- Bursar's Assistant and Master's Assistant