UNIVERSITY COLLEGE OXFORD

DATA PROTECTION POLICY

The information and guidelines within this policy are important as this policy aims to ensure all University College Oxford ("the College") members and employees understand what personal data is, how its use is regulated and how the College complies with the rules for protecting personal data and the importance of doing so.

This policy is relevant to all members and staff (which includes students, alumni, contractors, consultants, temporary workers, agents and other workers, including personnel affiliated with third party providers who access/use the personal data) of the College who shall in this policy be referred to as the "College Community". This policy should be read in conjunction with the following policies:

- IT Policy
- Home Working Policy

All members of the College Community who process personal data on behalf of the College must ensure that they comply with the College's obligations under the Data Protection Act 1998 ("the DPA") and with the College's Data Protection Policy and IT Policy, Procedures and Guidance ("IT Policy") (including any other policies, procedures and/or guidelines which may be issued from time to time). A breach of this Data Protection Policy (which may cause the College to be in breach of its obligations under the DPA) may result in disciplinary proceedings.

What is Personal data?

Personal data is any information (for example, a person's name) or combination of information which relates to a living person and which allows that living person to be identified (for example a first name and an address).

Examples of personal data which may be used by the College in its day to day business include names, addresses (email and land addresses), telephone numbers and other contact details, CVs, performance reviews, payroll and salary information. The definition also includes opinions, appraisals or statements of intent regarding individuals (eg. employees, job applicants, students, individual consultants, personal contacts at suppliers or customers and individual suppliers,

customers or members of the public).

The laws governing how personal data can be used apply whether the personal data is stored electronically (for example, in e-mails, on IT systems, as part of a database or in an electronic document) or in paper records (for example, in paper files in a filing cabinet).

What activities are covered by this policy?

Like all educational establishments, the College holds and processes data on its members, employees, applicants, students, alumni and other individuals for various purposes. Examples of such purposes are:

Recruitment
Employee performance, management and administration
Contract administration, finance, accounting and payments
The administration of the admissions process, including marketing to potential students;
The provision of academic and welfare services
Research and development
Fundraising
The provision of references and certificates
Legal and regulatory compliance and good governance

When the College uses personal data in any way, including its collection, storage, use or destruction, this is called processing and is regulated by this policy and UK law. This applies to hard copy data as well as electronic data. If you read, amend, copy, print, or delete personal data, that is also processing. Where you share or send personal data to another organisation or to an individual outside the College, that disclosure is also regulated and will not automatically be lawful.

To comply with data protection law, in particular, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully (as set out in more detail below).

Why should I worry about complying with this policy?

Data protection laws are enforced in the UK by the Information Commissioner's Office ("the ICO"). The ICO can investigate complaints, audit the College's use or processing of personal data and can take action against College (and you personally in some cases) for its breach of UK law. Action may include making the College pay a fine and/or stopping the use of the personal data by the College, which may prevent the College carrying on its business. Organisations which breach laws protecting personal data (called data protection laws) also often receive negative publicity which damages the reputation of the College.

The College is **dependent** upon you to meet its legal obligations and you have an **individual responsibility** to help do so and to comply with this policy. To achieve best practice and compliance, it may be helpful to ask yourself: "how would I reasonably expect this personal data

to be treated if it were mine?" The College is entrusted with personal data about individuals, called data subjects, and must maintain that trust. If it fails to do so, those data subjects can also make individual compensation claims against the College.

When does it matter?

Where the College uses personal data for its own internal purposes, the College will act as a "data controller", that is, it will normally control the collection and use of the personal data and in particular will make decisions about the purposes for which it will be used, e.g., paying salaries and providing academic services, as well as the manner in which such purposes are carried out, e.g., by inputting staff details into the College's HR database or adding information to the current members' database. As a data controller, the College is responsible for complying with UK data protection laws in relation to the use of that personal data.

College Data Protection Officer

The College Data Protection Officer ("DPO") is the Master. The DPO has been appointed to help the College comply with data protection laws. All queries about College policy and procedures should be addressed to the DPO. The DPO is not the legal data controller.

In addition, the DPO may delegate responsibility for dealing with certain types of personal data and purposes of data processing to other authorised individuals (termed "data holder contacts") within the College. Please make yourself familiar with these details set out in Schedule 1.

Notification to the ICO

The College has an obligation as a Data Controller to tell the ICO about the processing of personal data carried out by the College. This is often called notification, registration or filing on the Register of Data Controllers held by the ICO.

Unless an exempted use, the College is only permitted to process personal data in accordance with the stated purposes in its notification to the ICO. The scope of such processing should be reviewed regularly by the College and at least annually. The notification must be renewed each year and must be updated promptly as and when necessary by the College.

Full details of the College's data protection registration/notification with the ICO can be obtained from the DPO or from the ICO's website (http://www.ico.org.uk).

Details notified normally relate to the type of purpose for which personal data is used and within that, the type of personal data, type of data subject about whom such personal data is held, whom it may be shared with and where it may be transferred in the world.

If you begin carrying out new data processing activities or are involved in a new database

project and/or for any reason you suspect that the College notification is invalid or incomplete, please contact the DPO immediately and discuss the details with them first in case any notification needs to be updated. Failing to have a required, up to date notification (and any required approval) may be a criminal offence.

The main purposes for which the College is covered under its notifications are normally:

- staff, agent and contractor administration;
- advertising, marketing, public relations and general advice services;
- accounts and records;
- education;
- student and staff support services;
- research;
- other commercial services
- publication of the magazine
- crime prevention and prosecution of offenders; and
- alumni administration.

It may in some cases be possible to convert personal data into anonymous personal data, such as aggregated statistical data where data subjects cannot be identified, or to use it for research provided not used to impact or affect any data subject individually. However, it may be necessary to have warned data subjects in advance that this might happen, to explain any research and in some cases to obtain their consent. Data protection laws in this area are currently developing, so please speak to the DPO if you wish to convert personal data into anonymous data or use it for research before doing so, or if you have any concerns about current use.

Data Protection Principles

The College, as a Data Controller, must comply with the Data Protection Principles that are set out in the DPA. In summary, these state that personal data shall:

- be obtained and processed fairly and lawfully and shall not be obtained or processed unless certain conditions are met;

- be obtained for specified and lawful purposes and shall not be processed in any manner incompatible with those purposes;

- be adequate, relevant and not excessive for those purposes;

- be accurate and kept up to date;

- not be kept for longer than is necessary for those purposes;

- be processed in accordance with the data subject's rights under the DPA;.

- have appropriate technical and organisational measures in place against the unauthorised or unlawful processing of that personal data and against the accidental loss or destruction of or damage to, that personal data;

- not be transferred to a country outside the European Economic Area ("the EEA"), (being the EU member states plus Iceland, Liechtenstein and Norway) unless that country has equivalent levels of protection for personal data.

What does "fair and lawful use of Personal Data" mean?

One of the key obligations under the DPA, requires the College to process personal data fairly and lawfully. In practice, this means that the College must ensure that:

- all and any use of personal data by it or for it is lawful; and

- its use of personal data is fair (which means it should be within the reasonable expectations of the data subject).

'Fair' use of personal data is normally achieved by providing suitable details of proposed data use to the data subject before or at the time the personal data is collected or obtained, or as soon as possible afterwards, but should be before starting to use such personal data (see below). This may be through provision of a fair processing or privacy notice, such as the template privacy notice issued by the College (see Appendix 1). Some uses of personal data are exempt from the need to warn the data subject in advance. For example, if there is a legitimate and proportionate requirement to provide personal data to the police for an investigation to prevent or detect crime, there would be no need for the College to warn the employee being investigated about this.

In addition, for the use of personal data to be fair and lawful, the College must comply with at least one of the following conditions when processing personal data:

- the individual to whom the personal data relates has consented expressly to the processing after having been suitably informed of the purposes of processing;

- the processing is necessary for the performance of a contract between the College and the individual e.g. the employment or student contract;

- the processing is necessary to comply with a legal obligation placed on the College e.g.

to comply with a court order; or

- the processing is necessary in order to pursue a legitimate interest of the College (or the person to whom the personal data is to be disclosed) provided such use is proportionate and on balance, not unfair to the individual.

If you want to make a new use of any personal data held by or to be collected by the College, you must not do so unless that new use satisfies one of the lawful reasons for processing and it is described in the relevant privacy notice provided to the affected individuals (see below). For example, if someone provides their details as part of a job application, you may not be able to start sending them marketing emails, unless that is covered in an appropriate notice and, in all likelihood, consent from that individual.

What is a Privacy Notice?

Before the College collects and uses any personal data about an individual, the College must make sure the individual knows that the College is responsible for its personal data and compliance with data protection laws and what the College intends to do with that personal data. It needs to provide the individual with a range of information to try to ensure proposed personal data use is reasonably expected and fair. So that it can prove this information has been provided to an individual (in case of complaint or regulatory investigation), the College will provide the necessary information in a written notice, or electronic notice as appropriate.

You should therefore check whether there is an applicable notice which covers the intended processing by the College. The College's template privacy notice is attached at Appendix 1.

Even after fair notice has been provided, the College cannot make any use it wants of personal data. All the other rules explained in this policy still have to be complied with e.g. the information collected must not be excessive. Simply because a person has consented to giving you their information does not override that restriction. Similarly, personal data must not be used in a way which would infringe other laws e.g. in breach of anti-discrimination laws.

It is the College's policy however to seek express consent from individual data subjects for its processing of sensitive personal data. If an individual raises any objections to any intended processing of personal data, the College will consider any such objections but reserves the right to process personal data in order to carry out its functions as permitted by law.

Therefore all prospective members and staff will be asked to sign a consent form/privacy notice when an offer of employment or a course place is made regarding particular types of information which the College may in due course hold/process about them.

If you have any questions about drafting privacy notices and/or the College's template privacy policy, please contact the DPO.

Sensitive Personal Data

The College may from time to time process "sensitive personal data" relating to members of the College Community. "Sensitive personal data" is information as to a data subject's racial or ethnic origin, political opinions, religious beliefs or beliefs of a similar nature, trade union membership, physical or mental health or condition, sexual life, criminal offences or alleged offences, and information relating to any proceedings for offences committed or allegedly committed by the data subject, including the outcome of those proceedings.

Sensitive personal data should not be collected or used unless essential. Extra care must be taken with it (in addition to the normal rules for personal data) because of the greater potential for damage or distress, so it must also be kept more securely. You should refer to the College's IT Policy for further information on how data should be kept securely.

In addition to having a lawful reason for processing personal data as mentioned above another condition must be met to process sensitive personal data and normally the individual's, explicit consent to use of any sensitive personal data must be obtained in advance.

- The College does not wish to collect and use sensitive personal data unless essential and unavoidable and:

- the individual concerned agrees in writing that the College may do so, on the basis of a full understanding of why the College is collecting the details;

- to meet its obligations or exercise its rights under employment related laws e.g. to pay governmental sickness pay or comply with health and safety laws; or

- the use is exceptional, such as where the processing is necessary to protect the vital interests (i.e. matter of life or death) of the individual concerned.

Members of staff should note that the "legitimate interest" criteria described above for normal personal data is not on its own sufficient to allow lawful use of sensitive personal data.

Currently, the College envisages the need to process sensitive personal data of a type specified in Schedule 4 to this policy, for the purposes specified.

Proportionate use of personal data?

The College is responsible for ensuring that personal data collected is proportionate to need for the relevant purpose for which it is collected i.e. adequate but not excessive for that purpose. For example, if you will never telephone someone at home, you do not need their home telephone number.

In addition, Members of the College Community must take care to record and input personal data (and especially sensitive personal data) accurately. Some personal data may change from time to time (such as addresses and contact details, bank accounts and the place of employment). It is important to keep current records up to date. There can be serious consequences for affected individuals, the College and you if personal data is incorrect.

Members of the College Community who use the College computer facilities must not, unless on a need to know basis as required to perform their professional obligations to the College, process personal data about others. To do so is a disciplinary offence.

In addition, members of the College Community must not, without the prior written authorisation of the DPO:

- develop a new computer system for processing personal data;
- use an existing computer system for processing personal data for a different purpose;
- create a new manual filing system containing personal data;
- use an existing manual filing system containing personal data for a different purpose.

The above does not apply to databases which are maintained by individuals within the College Community for their private domestic use, i.e. private address books. Individuals, however, should consider if their private use falls within the scope of the DPA.

If you notice that you have access to more personal data than is normal or needed, please inform the DPO with details immediately.

Data retention: How long should I keep Personal Data?

The College cannot keep or retain personal data forever. Please refer to Schedule 3 for more information regarding data retention.

What rights do data subjects have?

Individuals have certain rights under the DPA in relation to their personal data that is being

held about them either in an "automatically process-able form" (mainly computer records) or in "relevant filing systems" (i.e. structured files that enable personal data relating to a particular individual to be readily accessible) by the College:

- the right to access personal data held about themselves;
- the right to prevent processing of personal data for direct marketing and purposes and in some other situations;
- the right to have personal data corrected;
- the right in some cases to compensation for any damage/distress suffered from breach of data protection law; and
- the right to be informed of automated decision making about them.

Should you receive a request from a data subject to correct their details, or to stop certain uses of their personal data (an objection), you must inform the DPO promptly and follow their instructions.

The College is not always obliged to correct personal data where requested by the data subject and may be entitled simply to record the request, noting that the College has not accepted the correction is needed e.g. when an individual tries to change the record of a disputed conversation at a meeting, as opposed to updating their address.

Individuals are allowed to withdraw their consent to the College's use of their personal data at any time. If a data subject contacts you to withdraw their consent, inform the DPO promptly and where possible, stop using / processing that personal data as requested until you have received guidance from the DPO as to the necessary steps to be taken.

If you receive a request to stop sending direct marketing materials, you should cease sending further direct marketing communications to that individual pending guidance from the DPO. This guidance may include adding that person's name to a marketing suppression list rather than simply deleting their details entirely from the relevant database.

Right to Access Personal Data

A data subject can also ask a data controller about the personal data it holds about them: what is held, what purposes it is used for, the sources from which it was obtained and with whom it is shared. The data subject is also entitled to a copy of their own personal data. The request

must be in writing and is called a subject access request or SAR.

An individual who wishes to exercise his/her right of access may complete the College "Access to Personal Data" form, which is available from the Domestic Bursar's office and send it to the DPO. However, a request made outside of this form may still be a valid request and should be provided to the DPO immediately. You should not refuse to deal with a request that is made on account of the applicant not using the College's Access to Personal Data form.

If you receive such a subject access request, there are special legal rules which must be followed as part of this process. Please pass the request to the DPO immediately and follow their instructions. You must not deal with such subject access requests yourself. Great care is needed to avoid being tricked into disclosing personal data to those who are not entitled to it, especially by telephone. Normally, only the data subject is entitled to their own personal data and nobody else. Special care is needed if dealing with those who are under 18 years of age or vulnerable in some way. Please liaise with the DPO for more details if required.

The College may make a charge of £10 (or other such charge as is permitted from time to time under UK law) on each occasion that access is requested and this fee should accompany the Access to Personal Data form (or other format of subject access request). In accordance with the DPA, the College may refuse repeated requests where a reasonable period has not elapsed between requests.

The College should respond to the request for access to personal data within 40 calendar days of the request or payment of the fee, whichever is the later.

You should also be aware of the Freedom of Information Act 2000 and the Environmental Information Regulations 2004, which give individuals the right to request information (including environmental information, as applicable) held by a public authority, which in certain circumstances may not be held on computer or in a relevant filing system.

Data Security and Disclosure

Members of the College Community are responsible for ensuring that:

- any personal data which they hold is kept securely; and
- any personal data is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party.

Unauthorised disclosure is a disciplinary matter and may be considered gross misconduct.

If in any doubt, consult the DPO.

In addition to the requirements of the DPA the confidentiality of information about individuals must be respected.

For further information regarding the College's expectations in terms of data security, please refer to the College's IT Policy, available from the College's external website.

Where a member of the College Community suspects that a security breach has occurred or may occur, they should act in compliance with the College's IT policy.

Can I disclose personal data to third parties?

A disclosure of personal data is a form of processing. That means that the rules described above for fair and lawful use have to be satisfied. You must not disclose personal data to a third party outside the College unless there is a lawful reason to do so **and** it would be fair to do so (unless agreed with the DPO in advance).

It is more difficult for the College to disclose personal data to another data controller than to a data processor of the College. Provided the privacy notice refers to relevant disclosures to service providers and the disclosure is necessary and proportionate to the relevant service being provided, it is likely to be lawful to disclose the personal data to a data processor. The DPO will be happy to discuss this with you.

If you receive a request for information about an individual from the government, police or other similar bodies or from journalists or other investigators, you should pass that request immediately to the DPO to be dealt with. Where the College voluntarily discloses personal data, it does so at its own risk and must only do so if the disclosure will comply with DPA. The burden is on the College to determine whether disclosure as requested is lawful. Unjustified or excessive disclosure, however well-meaning and however seemingly authoritative the request, risks placing the College in breach of the DPA.

The College may use third parties to provide services to it - for example, running its IT systems or to run a marketing campaign. Where such third parties use the College's personal data on its behalf, special rules apply. The College must have in place a written contract with that third party which contains specific limitations on what they can do with the personal data and imposes appropriate security obligations upon them. Please contact the DPO who will be able to provide you with the appropriate wording to include. You must not contract with such a third party without this wording being included.

Disclosure Outside of the EEA

The College may, from time to time, desire to transfer personal data to countries or territories outside the EEA. Under UK law there are restrictions on transferring personal data to outside the EEA. These controls are to make sure the personal data remains as safe as it

would in the EEA (and so affected data subjects retain similar protection and rights as they have in the EEA) even when their personal data is transferred outside the EEA.

A transfer includes where, for example where you log in to the College network from outside the EEA.

The fact that there will be transfers of personal data to other countries, especially to outside the EEA, should be clearly set out in the privacy notices described above so that they are expected by the individual data subjects.

Transfers within the EEA are considered safe by the DPA in the EEA, as are transfers from the EU to certain other approved countries e.g. Switzerland. An up to date list of 'safe' countries can be obtained from the DPO. Transfers from the EEA to any other outside country are not safe and will not be lawful without additional steps.

The DPO will be able to discuss such steps with you, if you need more information.

If an individual raises an objection to such transfers then you should notify the DPO. Although the College may be satisfied that the country or territory in question ensures an adequate level of protection for the rights and freedoms of data subjects, the transfer must also be fair and lawful and withdrawal of consent may prevent the transfer from being lawful (particularly if it relates to sensitive personal data).

You must comply with any request by an individual not to receive direct marketing (where it is addressed to them) or their choice not to receive marketing by a particular method (for example, post, telephone, e-mail or text messaging). Data controllers also have legal obligations with regard to the storage of information on or access to information on a user's device (for example, a user's computer, Smartphone, tablet etc.) through the use of cookies or similar technologies on the College's website. These obligations must be considered, as the College may need to obtain consent for the use of particular cookies and provide certain information to the users regarding the use of cookies. You must liaise with the DPO about any proposed use of cookies and follow their instructions.

Please consider the College's IT Policy in respect of the College's rights to monitor, inspect, copy, retain, review and intercept, all e-mail, voicemail, telephone conversations and other electronic and non-electronic communications created using or transmitted over the College's voice or data networks or equipment or devices.

Complaints Procedure

Data subjects wishing to lodge a complaint with regard to the College's handling of data/alleged unauthorised disclosure/disagreement with information held, should do so in writing to the DPO. The DPO will seek to resolve the issue to the satisfaction of the data subject. Should the DPO be unable to resolve the matter the data subject may ask that the complaint be referred to the Governing Body. The data subject may also complain to the ICO.

Schedule 1

"Data Holder Contacts"

The College DPO may from time to time designate "Data Holder Contacts" for particular types of data within the College whose responsibilities will include:

- informing the DPO of proposed processing of personal data within the College that may need to be notified to the ICO;

- providing personal data on a particular subject to the DPO in response to a subject access request when requested to do so by the DPO; and

- maintaining the security of, and access to, personal data within their areas, in accordance with the College's IT Policy (available from HR and on the College's external website).

Although Data Holder Contacts may be designated, College Community members, the DPO and the Data Holder Contacts are still expected to comply with their obligations under the College's policies, including the Data Protection Policy and the IT Policy and liaise with the DPO and Data Holder Contacts, as applicable.

The Master- in respect of personnel files for senior officers. Files are maintained on senior College Officers' appointments and employment. The Master may authorise requests for access by others.

The Estates Bursar - in respect of the BUPA medical scheme; housing loans; stipends; other loans, grants and allowances; College tenants, employees.

Files are maintained on the Fellows' medical scheme; Fellows' stipends, staff salaries, USS and OSPS records of current and former Fellows; housing loans; batells and any other loans grants and allowances and College tenants and may be consulted by the Estates Bursar, the Accountant, The Assistant Accountant and the Estates Bursar's secretary. The Estates Bursar and Accountant may authorise requests for access by others. The files are to be kept in locked filing cabinets within the Estates Bursary and the Treasury and these offices are to be locked at all times when not occupied, as per the College's Data Protection and IT Policies.

The Domestic Bursar – in respect of staff personnel matters, applications for staff posts, financial and accommodation matters.

Personnel files are maintained in respect of College staff. Application forms are to be retained

for a limited period (in accordance with this policy, including all Schedules) for subsequent monitoring/follow-up of the selection process.

Personnel files may be consulted on a day-to-day basis by the Domestic Bursar, the Operations Manager and the Domestic Bursary administrative assistant. All other requests for access to personnel files must be authorised by the Domestic Bursar. In accordance with the College's Data Protection and IT Policies, personnel files are to be stored in a locked cabinet in the Domestic Bursary. The office is to be locked whenever unoccupied.

The Senior Tutor – in respect of Tutorial files and files on members of the Teaching Staff.

Tutorial files are maintained in respect of students' academic progress and welfare, awards of scholarships and prizes, loans and grants. Medical notes are also maintained for Health & Safety reasons, to assist in meeting the needs of students with disabilities, or for reasons connected with absences from College, poor performance, applications to the University or to charities etc. Tutorial files may be consulted on a day-to-day basis by the Senior Tutor, the Academic Services Manager, the Academic Registrar and the Admissions Manager. All other requests for access to a tutorial file must be authorised by the Senior Tutor. In accordance with the College's Data Protection and IT Policies, tutorial files are to be kept in a locked filing cabinet in the offices of the Senior Tutor and the office is to be locked whenever it is unoccupied.

Files on members of the Academic Staff are maintained and consulted only by the Senior Tutor. Requests for access to these files can be authorised only by the Senior Tutor. In accordance with the College's Data Protection and IT Policies, files are to be kept in a locked filing cabinet in the Senior Tutor's office, which is to be locked when unoccupied.

The Admissions Manager – in respect of admissions candidates.

Admissions files are maintained to assess candidates for admissions. For successful candidates some of the admissions documentation is included in a tutorial file, for unsuccessful candidates the admissions documentation is archived for subsequent research into the admissions process.

Prior to and following admissions the files may be consulted on a day-to-day basis by the Admissions Manager and Senior Tutor. During the admissions process, admissions files may be consulted by the Senior Tutor, Admissions Manager and those interviewing candidates for admission. In accordance with the College's Data Protection and IT Policies, active files are to be stored in a locked filing cabinet in the Academic Office, which is to be locked whenever it is unoccupied.

In accordance with the College's Data Protection and IT Policies, all archived tutorial and

admissions files are to be kept in a locked storeroom and access authorised by the Senior Tutor, the Academic Services Manager or Admissions Manager.

The Dean – in respect of student files on non-academic discipline
Files are maintained in respect of non-academic disciplinary matters, both within the College and within the University. The Dean's files may be consulted on a day to day basis by the Dean and the Welfare Registrar. All other requests for access must be authorised by the Dean. In accordance with the College's Data Protection and IT Policies, files are stored in a locked filing cabinet in the Welfare Registrar's office, which is to be locked whenever it is unoccupied.

Welfare Fellow – in respect of student files on welfare and personnel files for welfare staff.
Files are maintained in respect of students' health and welfare. The Welfare Fellow's files may be consulted on a day to day basis by the Welfare Fellow and the Disability and Welfare Administrator. All other requests for access must be authorised by the Welfare Fellow. In accordance with the College's Data Protection and IT Policies, files are kept in a locked filing cabinet in the Student Welfare office.

Separate files on students' health are maintained by the College Nurse. The storage and processing of these files are covered by the Data Protection Policy of the University of Oxford Occupational Health Service. The room is locked whenever unoccupied.

The I.T. Manager – computer files and databases containing personal information in respect of members of the College Community.

The files/information may be consulted on a day-to-day basis by the I.T. Manager and I.T. Officers. All other requests for access to files/information must be authorised by the I.T. Fellow or the I.T. Manager.

The computer and database systems shall be dealt with in accordance with the College's Data Protection and IT Policies.

College Databases

The College holds data on current members and former members of the College Community and candidates for admission. The databases used in the College are the Accurate Solutions Financial System, The Oxford Student Systems database, ADSS, ADMIT, the University College current members' database and the Raiser's Edge database. Their use is for the effective administration of the College.

Access to the data held on the College Databases is restricted according to the need of the various users, as is the ability to enter data. In addition to names, year and tutorial side the

information to which they have access is:

- Admissions. The Senior Tutor, The Academic Services Manager, the Dean of Graduates, the Admissions Manager and their administrative assistants have access to all the data held on candidates for admission.

  Those interviewing candidates have access to data on candidates in those subjects for which they have responsibility. The Welfare Registrar has access to data for candidates who have disclosed a disability.
- Academic Administration. The Senior Tutor, student members, Academic Services Manager, IT Manager and their administrative assistants have access to all the data held on the University College Current Members' database. This includes additional data created locally on the University College Current Members' System. Other departments (Lodge, Domestic Bursary, Library, Works Department, Treasury, Master's Office) have access to limited access to the University College Current Members' System.
- Financial Administration. The College Accountant, the Domestic Bursar and their administrative assistants have access to the Accurate Solutions database.
- Alumni Relations and Development. The Development Director, the Master, the Major Gifts Manager, the Annual Fund Manager and their administrative assistants have access to the Raiser's Edge Database.

Schedule 2

Specific examples of data processing by the College

Data Processed for Research Purposes

Personal data held by the College may be processed for research purposes, including statistical or historical purposes. Personal data must not be used in this way if such processing is to support measures or decisions with respect to the individual data subject(s) and that would, or would be likely to, cause substantial damage or substantial distress to the individual data subject(s). Accordingly, it is the College's policy for prior written approval to be obtained from the College Data Protection Officer ("DPO") for any research involving personal data held by the College. Personal data used for research purposes must not be published or disclosed in any way in which the individual data subject can be identified.

CCTV

The College operates a number of CCTV cameras in order to assist with security for members of the College Community and in respect of College property. Any queries regarding the operation of the CCTV system should be addressed to the Domestic Bursar. Requests for access by individuals to personal data held on the CCTV system should be dealt with in accordance with this Data Protection Policy. Ideally, requests should include details of the relevant camera, location, time and date.

E-mail

It is permissible and appropriate for the College to keep records of internal communications which are relevant to an individual's continuing relationship with the College, whether as a Fellow, member of staff or student, including information concerning performance and conduct issues, provided such records comply with the data protection principles and the College's Data Protection Policy.

It is recognised that e-mail is used for such communications and that such e-mails should form part of the College's records. It goes beyond the scope of this policy document to address the appropriate use of e-mail in the proper functioning of the College, and the limitations and legal implications with this mode of communication. Please therefore refer to the College's IT Policy for such detail. However, in particular all members of the College Community need to be aware that:

- the DPA applies to e-mails containing personal data about individuals that are sent or

received by members of the College Community (other than for their own private purposes as opposed to College purposes).

- subject to certain exceptions, individual subjects will be entitled to make a data subject access request and have access to e-mails that concern personal data concerning them, providing that the individual subject can provide sufficient information for the College to locate the personal data in the e-mails; and

- the DPA applies to all e-mails from and to members of the College Community that are sent and received for College purposes, whether or not the e-mails are sent through the College e-mail system or on an individual's own e-mail account.

Alumni Relations and Development

Manual and computer files are maintained in respect of current and past Fellows and alumni for alumni relations and development purposes. All such information is to be dealt with in accordance with the College's Data Protection and IT Policies. The Development Office staff may consult the manual and computer-based files on a day to day basis but requests by others to have access to these files must be authorised by the Development Director, after consultation with the DPO.

Data will be used by the College for a full range of alumni activities, including the sending of College publications, notification of alumni activities and fund raising initiatives.

The consent of individual's will be sought to disclosure of their contact details before they are made available to other current and old members of the College, recognised alumni societies, to sports and other clubs associated with the College and to any agents contracted by the College for particular alumni-related activities. The following classes of information will be included in the College alumni computer database:

- Name and address

- Academic achievements and establishments

- Career details

- Family information

- Donations to the College

Some personal data may also he held/processed in an anonymous form for statistical records and research purposes.

Schedule 3

Retention of Data – College Archives

Some records have to be retained for minimum periods by law (such as records on payments to employees and their taxation). Other records should be kept for a specific amount of time to protect the College from normal business risks, e.g., legal proceedings for breach of contract. Personal data can only be retained for as long as reasonably necessary for the purposes for which it was obtained.

The individual files relating to Fellows and students of the College are the basis of the alumni records and detailed historical archives of the College and are retained indefinitely for reference and research purposes. At some point after a member leaves the College his or her files will be transferred to the College's archives. The timing of such transfer will differ between the various Data Holder Contacts, depending on a number of factors. Until such transfer, files/information may be consulted on a day-to-day basis in accordance with the procedures set down for the individual Data Holder Contacts and thereafter by them or the College Archivist or, for alumni purposes, by the Editor of the Annual Record and the Development Director. All other requests for access to any archived file must be authorised by the Archivist, after consultation with the Data Protection Officer with respect to Bursary/Academic Office files and the Senior Tutor for former tutorial files.

All data about College staff is to be kept for at least the minimum specified by legislation after they cease to be employed by the College, see Retention of Records chart below.

In respect of personal and academic references, these should be held for a reasonable length of time. While personal and academic references may become 'stale', some data e.g transcripts of student marks, may be required throughout the student's future career. Upon the death of the data subject, data relating to him/her ceases to be personal data. However, confidentiality obligations will be owed to the deceased's personal representatives.

The College retains an archive of miscellaneous written records/lists in respect of its members, staff and candidates for reference and research purposes, including tutorial reports, academic records, Senior Tutor's records and correspondence. The confidentiality of these records will be respected.
Permission to access archived records must be obtained from the DPO.

University College Oxford Retention of Records Containing Personal Data

Type of Record	Retention Period	Reason for Period
Personnel Files including training records and notes of disciplinary and grievance hearings.	6 years from the end of employment by the College.	Time limit for litigation
Applications forms/interview notes	6 months from the date of the interviews, unless clearly communicated to the candidate to keep CVs for longer.	Time limit on litigation
Facts relating to redundancies	6 years from the date of redundancy.	Time limit on litigation.
Income tax and NI contributions, including correspondence with tax office	At least 3 years after the end of the financial year to which the records relate.	Income Tax Regulations 2003
Statutory Maternity Pay records and calculations	At least 3 years after the end of the tax year to which the records relate.	Statutory Maternity pay (General) regulations 1986
Statutory Sick Pay records and calculations	At least 3 years after the end of the financial year to which the records relate.	Statutory Sick Pay (General) Regulations 1982
Wages and salary records	Until 5th anniversary of 31 January following year of assessment.	Taxes management Act 1970
Accident books, records and reports of accidents	3 years after the date of the last entry.	Social Security (Claims and Payments) regulations 1979; RIDDOR 2013
Health Records	During employment and for as long as reasonably necessary under the Data Protection Act 1998.	Management of Health and Safety at Work Regulations 1999
Health Records where reason for termination of employment is connected with health, including stress related illness	3 years	Limitation period for personal injury claims

Medical records kept by reason of the Control of Substances Hazardous to Health Regulations 2002	40 years	Control of Substances Hazardous to Health Regulations 2002
Student Records, including academic achievements and conduct	6 years from the date that the student leaves the College, in case of litigation for negligence.	Limitation period for litigation

Schedule 4

Categories of personal data, purposes of processing, sources and recipients of personal data

Applicants and employees

Data:	Name; address; telephone or mobile number; date of birth; employee ID; details of salary; benefits; remuneration and compensation including pension information; performance ratings and related information; job title, details of spouse/partner and dependents; hire date and references received; full time or part time status; employment history; qualifications and skills (professional and academic); financial details; national insurance number and statements of opinion or intention; financial details. Information necessary for legal compliance, including where relevant, religious beliefs, trade union membership and details of race/ethnic origin or nationality; criminal convictions or alleged offences (or related proceedings); Absence records including holiday records and where necessary details of illness for sickness absence.
Main purposes:	Applications administration; staff administration, management and administration of salary and pension administration and other benefits; performance review, training and other HR functions related to employment; planning and administration of the College; career development; training records and requirements; meeting the needs of members of the College Community with disabilities; disciplinary matters; personal development records; the College's legitimate business processes and activities; compliance with legal, regulatory and other good governance obligations (e.g. Health & Safety record); communications/mailings; references; fund raising by the College and the University; provision of healthcare; dietary requirements and research and statistical publications.

Main sources and disclosures:	Applications forms; data subject, family; local authority (and other governmental bodies); examinations results; scholarships; Student Loans Company; University of Oxford; College Staff and Committees; other Oxford Colleges; other Universities; schools; examination boards; other educational institutions; employers; family; College Nurse; other College staff; University of Oxford; General Practitioners; other medical practitioners; police (and other authorities) legal representatives; Court services; research and statistical publications; websites.

Members

Data:	Name; address; telephone or mobile number; date of birth; student ID; financial details; sponsorship details; performance ratings and related information; details of spouse/partner, guardians and dependents; admission date and references received; academic qualifications and skills; national insurance number and statements of opinion or intention; academic record; qualifications and skills; and student record. Information necessary for legal compliance, including where relevant, religious beliefs, trade union membership and details of race/ethnic origin or nationality; criminal convictions or alleged offences (or related proceedings); Medical records, including absence records and dietary needs.
Main purposes:	Student administration, to assess applications from candidates for admission and assist in the admissions process; accommodation issues; to process proper and up to date records of academic progress; fees and charges administration/collection; student welfare; provision of healthcare; dietary requirements; accommodation issues; meeting the needs of members of the College Community with disabilities; disciplinary matters; the College's legitimate business processes and activities; compliance with legal, regulatory and other good governance obligations (e.g. Health & Safety record); communications/mailings; references; fund raising by the College and the University; research and statistical publications.

Main sources and disclosures:	Applications forms; data subject, family; local authority (and other governmental bodies); examinations results; scholarships; Student Loans Company; University of Oxford; College Staff and Committees; other Oxford Colleges; other Universities; schools; examination boards; other educational institutions; employers; admissions officers; family; College Nurse; Senior Tutor; other College staff; University of Oxford; General Practitioners; other medical practitioners; police (and other authorities) legal representatives; Court services; research and statistical publications; data subject; websites.

In all circumstances, where sensitive personal data is processed, the College should try to seek the explicit consent of the College Community member in question (unless one of the limited exemptions provided in the Data Protection Act 1998 applies (such as to perform a legal duty regarding employees or to protect the data subject's or a third party's vital interests)).

For more information regarding the College's data processing, please speak to the College's Data Protection Officer and/or refer to the College's notification with the Information Commissioner's Office, available at www.ico.org.uk.

Appendix 1

University College, Oxford
Applicants, Employee and Members Data Privacy Notice

1. The purpose of this Notice

To assist the College in complying with its legal obligations under the Data Protection Act 1998, we have set out below how the College will process personal information we collect about you.

In addition to the functions described in this notice, the College may also maintain other policies from time to time, dealing with specific areas of your employment or education at the College, such as our IT Policy, Data Protection Policy, Student Handbook and/or Employee Handbook. These policies are available on request and will be notified to you where necessary to comply with relevant data privacy laws.

2. What personal information is collected?

The College collects various "**personal data**" about you in the performance of HR and student services related functions which are explained in more detail in **Schedule A**. Personal data is information which can identify you as a living individual, including where used in conjunction with other information. Common examples of personal data which may be collected and used by the College in its day to day business activities are set out in **Schedule A**.

The information set out in **Schedule A** will be collected primarily from you as information voluntarily provided to us, but we may also collect it where lawful to do so from other sources, e.g. third party parties you interact with, family members, other colleagues, government, tax or law enforcement agencies, reference and vetting service providers and other third parties. We may also collect personal information about and from your use of information systems, equipment and other assets and facilities made available to you for the performance of your work and/or studies.

3. How will my personal data be collected and used?

The College primarily collects personal data about you to the extent necessary to establish and manage our relationship with you as an employee or member and to perform any related functions, as well as to comply with applicable laws. Consequently, the College may process your personal data for reasons set out in **Schedule A**.

The list in **Schedule A** is not intended to be exhaustive and may be updated from time to time as business needs and legal requirements dictate. Some of the personal data that the College maintains will be kept in paper files, while other personal data will be included in computerised files and electronic databases.

4. Who will see my personal information?

Your personal data will be made available for the purposes mentioned in Schedule A and only to responsible management, human resources, accounting, audit, compliance, information technology and other corporate staff who properly need to know these details for their functions within the College. Further information is set out in Schedule A regarding third parties who may hold and maintain your personal data provided to them by the College.

The College will not sell your personal data to any third party other than as part of any restructuring of the College.

5. Will my personal data be transferred abroad?

UK data protection law permits the export of personal data subject to the provision of adequate levels of protection for the processing of such personal data.

Recipients of your personal data may not be located within the European Economic Area ("EEA") but instead located in countries which do not have equivalent protection to that within the EEA. Steps will be taken to protect your personal information in that instance consistent with applicable law.

6. Your right to review and amend personal data

You have the right to review your personal data and have certain inaccurate information about you corrected. If you wish to do so, or to notify the College of a change in your details, please contact HR or student support services as the case may be.

If you have a question about the use of your personal data, or wish to file a complaint about it, please contact the College's Data Protection Officer (the Master) ivor.crewe@univ.ox.ac.uk or line manager in the first instance.

Further details of the College's data protection/notification with the Information Commissioner's Office can be obtained from the College's Data Protection Officer or www.ico.org.uk.

Consent

As some of the proposed processing of your personal data includes the processing of sensitive personal data and/or the transfer of your personal data to other third parties as outlined above, we would appreciate you confirming that you have read the above notice and agree to the proposed use of your personal and sensitive personal data.

By signing this form you are giving your consent to the processing of your personal and sensitive personal data by the College as set out in this notice and in the relevant Schedules to this notice.

Name …… (Please print)

Signed ……..

Date …….

Schedule A to Appendix 1

Appendix 2

UNIVERSITY COLLEGE, OXFORD
Access to Personal Data Request Form

If you wish to make a "data subject access request" pursuant to the Data Protection Act 1998 ("the Act"), you should do the following:

1 Fill in all the relevant sections on the attached form;

2 Hand or send in this form to University College, Oxford, OX1 4BH, marked for the attention of the College's Data Protection Officer, the Master, together with:

a. an administration fee of £10 (this can be, for example, in the form of a personal cheque, banker's draft, building society cheque or postal order; please do not send cash through the post); and

b. a copy of proof of identification in addition to a copy of your student identification where applicable. Acceptable proofs of personal identification include a copy of your driving licence; a copy of your birth certificate or a copy of your passport with the relevant pages showing your name, the passport number and photograph.

The Data Protection Officer will issue a letter of acknowledgement on receiving your request and will begin to process the request as soon as adequate information has been provided by you in order to identify the personal data required, there is acceptable proof of your identification and the College has received the administration fee from cleared funds where appropriate.

The College requires proof of identification because it has a legal duty to ensure that personal data is only disclosed to those entitled to have access, usually only the data subjects themselves. Failure to provide adequate information to facilitate a data subject access request search and/or failure to provide acceptable proof of identification and/or failure to pay the administration fee will result in a delay to the processing of your application.

The College reserves the right to refuse to deal with requests that are identical or similar to requests you have made previously unless a reasonable interval has elapsed between these requests.

Certain information may be exempt from your right of subject access under the Act, in particular, the College may be unable to provide information that contains data about or identifies third parties.

UNIVERSITY COLLEGE, OXFORD
Access to Personal Data Request Form

I would like copies of personal data held about me, in so far as the information is governed by the Data Protection Act 1998, in the categories set out in this form:

Family name:		First name(s):	
Date of birth: *(optional)*		Student number (USN) (if applicable)	

Term time or permanent address or address during vacations: *(optional, but will help us to locate the information you are requesting)*	
Postal and/or e-mail address to which you would like us to send our response:	
Department and course currently enrolled on or department where employed: *(optional, but will help us to locate the information you are requesting)*	

Type/Source of Record	**Please tick as appropriate**
Student records - admissions	
Student records – tutorial	
Student records - disciplinary	
Student records – academic staff's records (please specify)	
Computing records	
Library records	
Financial records	
Personnel records	
Medical records	
Other – please specify	

Signed by the data subject ……Dated …….

College use only:

Date form received …….

Adequate personal identification: ……

Administration fee ……..

Adequate identification of data:

Signed …… Date ……..