

This privacy notice applies to users of Pembroke College IT systems, email and telephones/mobile devices

A summary of what this notice explains

Pembroke College is committed to protecting the privacy and security of personal data.

This notice applies to users of Pembroke College IT systems, email and telephones/mobile devices. It will apply to anyone allowed to use such systems, including our staff and students. There are separate privacy notices covering the other aspects of processing of staff, student and others' data, including users of the College website, which are available below.

This notice explains what personal data Pembroke College holds about you, how we use it internally, how we share it, how long we keep it and what your legal rights are in relation to it.

For the parts of your personal data that you supply to us to us, this notice also explains the basis on which you are required or requested to provide the information. For the parts of your personal data that we generate about you, or that we receive from others, it explains the source of the data.

What is your personal data and how does the law regulate our use of it?

“Personal data” is information relating to you as a living, identifiable individual. We refer to this as “your data”.

“Processing” your data includes various operations that may be carried out on your data, including collecting, recording, organising, using, disclosing, storing and deleting it.

Data protection law requires us:

- To process your data in a lawful, fair and transparent way;
- To only collect your data for explicit and legitimate purposes;
- To only collect data that is relevant, and limited to the purpose(s) we have told you about;
- To ensure that your data is accurate and up to date;
- To ensure that your data is only kept as long as necessary for the purpose(s) we have told you about;
- To ensure that appropriate security measures are used to protect your data.

Pembroke College's Contact Details

If you need to contact us about your data, please contact:

Jeremy Bennett, Bursar, Pembroke College, Oxford, OX1 1DW

DPO@pmb.ox.ac.uk

Data that you provide to us and the possible consequences of you not providing it

In most cases the data you provide will be a necessary requirement of using the relevant system (for example, you will need a password to access Pembroke College IT systems). If you do not provide such data you will not be able to use the system, and depending on circumstances this may become a disciplinary matter that could lead to the termination of your contract with us whether you are an employee, or a student.

Other sources of your data

Apart from the data that you provide to us, we may also process data about you from a range of sources. These include:

- The University of Oxford, which operates a number of systems that Colleges have access to, including **Email Services**.
- Information that we generate in the course of operating the College's IT systems, or which we obtain from third party suppliers, for example telephone records provided by suppliers of telephone systems.

The lawful basis on which we process your data

The law requires that we provide you with information about the lawful basis on which we process your personal data, and for what purposes.

Most commonly, we will process your data on the following lawful grounds:

- Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.
- Where it is necessary to perform the contract we have entered into with you;
- Where necessary to comply with a legal obligation;

We may also use your data, typically in an emergency, where this is necessary to protect your vital interests, or someone else's vital interests.

How we apply further protection in the case of “Special Categories” of personal data

"Special categories" of particularly sensitive personal data require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal data.

The Special Categories of personal data consist of data revealing:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership.

They also consist of the processing of:

- genetic data;
- biometric data for the purpose of uniquely identifying someone;
- data concerning health;
- data concerning someone's sex life or sexual orientation.

We may process special categories of personal data in the following circumstances:

- With your explicit written consent; or
- Where it is necessary in the substantial public interest, in particular:
 - is necessary for the purposes of the prevention or detection of an unlawful act, must be carried out without the consent of the data subject so as not to prejudice those purposes; or
 - for equal opportunities monitoring;
- Where the processing is necessary for archiving purposes in the public interest, or for scientific or historical research purposes, or statistical purposes, subject to further safeguards for your fundamental rights and interests specified in law.

We have in place an appropriate policy document and/or other safeguards which we are required by law to maintain when processing such data.

Less commonly, we may process this type of data where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the data public.

Criminal convictions and allegations of criminal activity

Further legal controls apply to data relating to criminal convictions and allegations of criminal activity. We may process such data on the same grounds as those identified for “special categories” referred to above.

Details of our processing activities, including our lawful basis for processing

We have prepared a detailed table setting out the processing activities that we undertake, the source of the data, the reasons why we process it, how long we keep it and the lawful basis we rely on.

The table includes detailed information about how and why we process various categories of data, and the related lawful basis. It includes monitoring that may occur of use of telephone and IT services, including, subject to certain safeguards, email content, internet use and/or telephone records for the purpose of ensuring that such services are not used for unlawful purposes, or otherwise breach the Pembroke College’s/ University’s IT/telephone regulations/policy <https://intranet.pmb.ox.ac.uk/it-information/network-access> . Safeguards are set out in our Security Policy: <https://intranet.pmb.ox.ac.uk/it-information/network-access> to ensure that an individual’s privacy is respected appropriately. The lawful basis for such processing is that the Pembroke College has a legitimate interest in maintaining the integrity of its systems, to investigate misuse and in taking action to prevent misuse recurring.

How we share your data

We will not sell your data to third parties. We will only share it with third parties if we are allowed or required to do so by law. This includes for example where we decide to report alleged criminal misconduct to the police.

All our third party service providers are required to take appropriate security measures to protect your personal information in line with our policies, and are only permitted to process your personal data for specific purposes in accordance with our instructions. We do not allow our third party providers to use your personal data for their own purposes.

More information on the categories of recipients of your data is set out in a table below.

Sharing your data outside the European Union

The law provides various further safeguards where data is transferred outside of the EU.

When you are resident outside the EU in a country where there is no “adequacy decision” by the European Commission, and an alternative safeguard is not available, we may still transfer data to you which is necessary for performance of your contract with us (if you are a staff member or student).

Otherwise, we will not transfer your data outside the European Union without first notifying you of our intentions and of the safeguards that apply to your data.

Automated decision-making

We do not envisage that any decisions will be taken about you based solely on automated means, however we will notify you in writing if this position changes.

How long we keep your data

The detailed table of processing activities explains how long we will keep your data.

If there are legal proceedings, a regulatory, disciplinary or criminal investigation, suspected criminal activity, or relevant requests under data protection or freedom of information legislation, it may be necessary for us to suspend the deletion of data until the proceedings, investigation or request have been fully disposed of.

Please note that we may keep anonymised statistical data indefinitely, but you cannot be identified from such data.

Your legal rights over your data

Subject to certain conditions set out in UK data protection law, you have:

- The **right to request access** to a copy of your data, as well as to be informed of various information about how your data is being used;
- The **right to have any inaccuracies in your data corrected**, which may include the right to have any incomplete data completed;
- The **right to have your personal data erased** in certain circumstances;
- The **right to have the processing of your data suspended**, for example if you want us to establish the accuracy of the data we are processing.
- The right to receive a **copy of data you have provided to us**, and have that transmitted to another data controller (for example, another University or College).
- The **right to object to any direct marketing** (for example, email marketing or phone calls) by us, and to require us to stop such marketing.

- The **right to object to the processing of your information** if we are relying on a “legitimate interest” for the processing or where the processing is necessary for the performance of a task carried out in the public interest. The lawful basis for any particular processing activity we carry out is set out in our detailed table of processing activities [LINK].
- The **right to object to any automated decision-making** about you which produces legal effects or otherwise significantly affects you.
- Where the lawful basis for processing your data is **consent**, you have the **right to withdraw your consent at any time**. When you tell us you wish to exercise your right, we will stop further processing of such data. This will not affect the validity of any lawful processing of your data up until the time when you withdrew your consent. You may withdraw your consent by contacting **Jeremy Bennett, Bursar, Pembroke College, Oxford, OX1 1DW** DPO@pmb.ox.ac.uk
- Further guidance on your rights is available from the Information Commissioner’s Office (<https://ico.org.uk/>). You may also wish to contact the Pembroke College’s Data Protection Officer if you are considering how or whether to exercise your rights.

You have the right to complain to the UK’s supervisory office for data protection, the Information Commissioner’s Office if you believe that your data has been processed unlawfully.

Future changes to this privacy notice, and previous versions

We may need to update this notice from time to time, for example if the law or regulatory requirements change, if technology changes, if the Pembroke College or the University makes changes to its procedures, or to make Pembroke College’s operations and procedures more efficient. If the change is material, we will give you not less than two months’ notice of the change so that you can decide whether to exercise your rights, if appropriate, before the change comes into effect. We will notify you of the change by **our website**.

Version control: V.1.0 (May 2018)

Project - IT Functions, including users of College email and tele

ID.	Category of personal data	Source of the data	Why we process it	How long we keep this	Our lawful basis for processing	Details relating to lawful basis (where applicable)	Special category grounds	Special category- details of public interest etc (where appropriate)	Criminal conviction/criminal allegation grounds	Criminal conviction/criminal allegation grounds (further information)
1	Firewall, security and PC misuse incident log files consisting of the date and time of incident, which user (name and/or user name), details of the incident and any consequential action taken.	We generate this data about you	In the course of maintaining the College's networks, protecting their integrity, investigating computer misuse and to minimise the risk of misuse recurring. Such records might also be used for disciplinary purposes where staff or students have breached College policies.	6 years from the date we learn of the incident.	Processing is necessary for the purposes of our or someone else's legitimate interests, except where overridden by your data protection rights and freedoms; Processing is necessary for compliance with a legal obligation	The College has a legitimate interest in maintaining the integrity of its systems, to investigate misuse and taking action to prevent misuse recurring. Keeping such records is also necessary to comply with the College's security and accountability obligations under data protection laws.			The processing is necessary for purposes of the prevention or detection of an unlawful act and must be carried out without the consent of the data subject, so as not to prejudice those purposes.	
2	Login information for students, staff, fellows and visitors consisting of time, date and duration of login, username and name of person logging in, their university card number, IP and MAC addresses associated with login, records of which users have printed documents and at what time/date, details of any charges for printing. We also hold records of the level of access permission users have to the system and which areas (e.g. staff, student, visitor, administrator). We also hold encrypted / obfuscated password information and records of internet usage (including records of sites visited, time and date of visit).	We obtain this data from you We generate this data about you	As a necessary part of the management and operation of our systems and controlling who has access to them. In cases of misconduct or copyright abuse such records might also be used as part of any investigation or staff/student disciplinary action. Records of internet usage are required to assist with troubleshooting and determining which users are affected by a security incident. They are also required to monitor and/or prevent: -malicious network traffic -suspected access of illegal materials, alleged copyright infringement and/or violations of University or College IT or disciplinary regulations Encrypted password information is held to enable users to login to our systems with their password.	Login information and internet use logs are retained for 12 months. Password and access level information is retained for as long as you are entitled to use our systems (e.g. whilst you are a student or staff member).	Processing is necessary for the purposes of our or someone else's legitimate interests, except where overridden by your data protection rights and freedoms. Processing is necessary for compliance with a legal obligation. In the case of staff and students, processing is necessary for performance of our contract with you.	The College has legitimate interest in keeping records of who has accessed its systems, websites visited and activity to assist with IT security and in taking disciplinary action under its contracts with staff or students if appropriate. Keeping such records and monitoring activity is also necessary to comply with the College's security and accountability obligations under data protection laws.			The processing is necessary for purposes of the prevention or detection of an unlawful act and must be carried out without the consent of the data subject, so as not to prejudice those purposes.	
3	IT support logs and records consisting of user names/contact information, dates and times of requests/problems, details of requests and details of steps taken and resolution of requests.	We generate this data about you	In the normal course of operating and maintaining our systems	IT support logs are retained for 12 months.	Processing is necessary for the purposes of our or someone else's legitimate interests, except where overridden by your data protection rights and freedoms; Processing is necessary for compliance with a legal obligation;	The College has a legitimate interest in keeping such records to help it maintain the functioning and security of its systems. Keeping such records is also necessary to comply with the College's security and accountability obligations under data protection laws.				
4	Records of telephone calls made and received (records of numbers called to/from, duration of calls).	We obtain this data from you	The data is provided to us by providers of telephone services (mobile and landline) to the College. We use this data to ensure we have been invoiced correctly by the provider, and to check that College provided telephones are being used in accordance with College policy.	Records are retained for 12 months.	Processing is necessary for the purposes of our or someone else's legitimate interests, except where overridden by your data protection rights and freedoms	We have a legitimate interest in the proper and efficient administration of College telephones and in ensuring they are being used correctly.	N/A		N/A	