

Exeter College GDPR - IT systems ROPA - 28th November 2018

ID	Category of Personal Data	Source of the data	Why we process this data	How long we keep this data	Our lawful basis for processing	Details relating to lawful basis (where applicable)	special category grounds	special category grounds - details of public interest (where)	criminal conviction grounds	criminal conviction grounds (further information)
1	Name, Contact details and University Card details of Staff and Students. In the case of students we also store course details and current course status. We also store passwords used to access systems which are encrypted.	We obtain this data from University of Oxford. We obtain this data from you.	To grant access to College systems as a necessary part of the management and operation of our systems and controlling who has access to them.	Deleted at the end of the relationship.	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 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.	We hold no special category data.		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. 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 p	Login information and internet usage 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, statutory obligations such as Prevention of Terrorism and duty of care, 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.	We hold no special category data.		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 obtain this data from you. We generate this data about you.	As necessary part of the management and operation of the systems to identify common faults and trend analysis.	We retain this information for 5 years.	Processing is necessary for the purposes of our or someone else's legitimate interests, except where overridden by your data protection rights and freedoms.	The College has a legitimate interest in keeping such records to help it maintain the functioning and security of its systems.				
4	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.	Firewall and Internet traffic records are retained for 1 year. Security incidents are retained for 5 years.	The College has an obligation to record the internet traffic to be able to identify any potential breaches in University or College Acceptable Use Policies.					
5	History of printed documents, such as document name, time/date printed, and charges accrued.	We obtain this data from you by using the service.	Record of printing for charging purposes. College can plan printing requirements.	We retain 1 years worth of print records.	Processing is necessary for the purposes of our or someone else's legitimate interests, except where overridden by your data protection rights and freedoms.					

Exeter College GDPR - IT systems ROPA - 28th November 2018

ID	Category of Personal Data	Source of the data	Why we process this data	How long we keep this data	Our lawful basis for processing	Details relating to lawful basis (where applicable)	special category grounds	special category grounds - details of public interest (where)	criminal conviction grounds	criminal conviction grounds (further information)
6	History of telephone calls.	We obtain this information from you by using the service. We obtain this from the University.	Record of usage needed to maintain the system for billing and administrative purposes.	1000 days of telephone history (calls made and received) is available to the College on request.	Processing is necessary for the purposes of our or someone else's legitimate interests, except where overridden by your data protection rights and freedoms.					