Keble College GDPR ROPA - IT Functions - v1.4 (July 2020)

Category of personal data	Source of the data	Why we process it	How long we keep this data	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 Grounds	Criminal conviction grounds (further information)
Firewall and security logs and network traffic logs consisting of the date and time, and the source and destination IP addresses of the connection	We generate this data about you	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 | 3 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 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. | |
| Access logs to College webservers or services which do not require explicit login. This includes information on the web page requested, originating IP address and, if provided by the web browser software as part of the standard request mechanism, referrer information on the webpage that delivered you to our page, which may include search terms entered into your browser. Unless you are connecting from inside College, the IP address cannot uniquely identify you unless we request information from the | We generate this data about you | 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 | 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 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. | |

Keble College GDPR ROPA - IT Functions - v1.4 (July 2020)

Category of personal data	Source of the data	Why we process it	How long we keep this data	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 Grounds	Criminal conviction grounds (further information)
Internet provider to follow up on malicious or criminal activity.									
Network or computer misuse incident reports	We generate this data about you We obtain this data from the University of Oxford.	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	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.	
Audit information for computers and networks used by students, staff and visitors, consisting of date and time of login and logout or of network connection and disconnection, username or IP and MAC address	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.	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 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.	
A record of all authorised users of College systems along with the level of access permission users have to those systems. We also store encrypted passwords.	We generate this data about you We obtain this data from the University of Oxford.	As a necessary part of the management and operation of our systems and controlling who has access to them. Encrypted password information is held to enable users to login	As long as users remain active members of college + 6 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	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				

Keble College GDPR ROPA - IT Functions - v1.4 (July 2020)

Category of personal data	Source of the data	Why we process it	How long we keep this data	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 Grounds	Criminal conviction grounds (further information)
		to our systems with their password.		necessary for compliance with a legal obligation	is also necessary to comply with the College's security and accountability obligations under data protection laws.				
Records of which users have printed documents in College and at what time/date and details of charges for the printing.	We generate this data about you	Records of printing are required for billing and for handling queries and problems	3 years, after which time records are stripped of personal data and consolidated into totals.	Processing is necessary for the purposes of our or someone else's legitimate interests, except where overridden by your data protection rights and freedoms;	Keeping such records are necessary for auditing and charging. Once stripped of personal data, records are useful for predicting usage trends and providing the service.				
Network registration data specifying the owner of a computer (identified by MAC address) used on the College network.	We obtain this data from 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.	As long as users remain active members of college + 6 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 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.				
Correspondence relating to support requests for College or University systems, or for support for personally owned equipment, which may include name, email address or telephone number, password to access a local computer and other information provided that is pertinent to the request for support.	We obtain this data from you	In order to deal with the request or to provide support. Contact details are required to get in touch solely for the purposes of handling the request.	3 years. Relevant information arising from solving the support request may be used elsewhere as part of documentation for future issues, but will first be stripped of all personal or identifying information.	Processing is necessary for the purposes of our or someone else's legitimate interests, except where overridden by your data protection rights and freedoms;					