GDPR

exa education
Internet & Filtering for Schools

How do Exa Education's services comply with GDPR?

There has been a huge amount of information published about the upcoming implementation of GDPR in May 2018. With such a lot of detail to process and work through, it can be difficult to know exactly what it is you need to do as a school to ensure compliance with the new regulations. This guide details how Exa Education's services comply with GDPR, so you have one less thing to worry about come May!

Connectivity

As a "mere conduit" (as defined "The Electronic Commerce Directive 2000/31/EC") Exa Education is not responsible for any data passing over its network. However, for operational purposes, we sample and log (for a period up to 31 days) a select number of the packets transiting through our network. This equivocates to approximately 1TB of data each month. This is industry practice, and necessary – for example, in the event of a DDOS attack occurring, it enables our engineers to identify where the traffic is originating from through the public IP address associated with the packet, and where it is being sent to. From this information, the attack can be mitigated.

The data collected by these packets may contain personal information in addition to the public IP address, such as a username, if entered into an insecure site. This data will *only* be used for operational matters, and is automatically deleted after the specified time period. The information is stored on servers owned by Exa Education in secure data centres based in the UK. Access to this data is provided over an encrypted channel and can only be accessed by a limited number of authorised Exa Education employees, whose job role explicitly necessitates this access.

Traffic usage volume is also stored for our connectivity products for operational purposes; this does not contain any personal data and therefore does not require compliance with the conditions identified by GDPR.

Email

The data logged by Exa Education's mail servers contains:

- **The time the communication was sent**
- **The public IP address of the server/mail client used to send the email**
- **The email address of the sender and the recipient**
- **The username which authorised the communication**

This data is stored for three months for operational purposes as it enables potential issues to be identified and is line with industry practice. It will only be accessed in the event of a incident, or if a customer requests information on their own communications.

All passwords for users' email accounts are encrypted. However, we periodically perform password strength checks for the security of our customers, during this process the authorised engineer may expose insecure passwords. In the event of this occurring, immediate notification is sent to the user requesting that their weak password is changed within 48 working hours – after which period it will be automatically reset.

The data is stored on servers owned by Exa Education in secure data centres based in the UK. Access to this data is provided over an encrypted channel and can only be accessed by a limited number of authorised Exa Education employees, whose job role explicitly necessitates this access.

SurfProtect Quantum

SurfProtect Quantum collects the following information:

- the address or URL of any web page which a user tries to access
- the words entered into a search engine
- the public IP address that initiates a web request
- when an attempt to access a restricted website or enter a banned search term has been made
- the time an activity occurred

This information is recorded against the username or, if Active Directory integration has not been enacted, only the external IP the incident is associated with. The data currently extracted from your school's AD server as result of enabling AD integration is as follows:

- the full name of each user, all AD usernames and AD groups

In the future, certain features of SurfProtect Quantum may require access to both the AD username *and* password of a user to enact advanced filtering capabilities. Prior to this data being extracted from your school's AD server, your explicit permission will be requested and these features will not be enacted until consent has been provided.

SurfProtect Quantum automatically scans for any changes in your school's AD information every ten minutes. If the data has changed and a user has been added or deleted, for example, a new complete export will be performed and the previous data will be replaced. The data for any users deleted from your school's AD server will not be stored by SurfProtect Quantum and will be entirely erased; although the online activity reports generated on this user up to the point of erasure will be available for the following three months.

The above data is stored by Exa Education in compliance with GDPR under Article 6(1)(b) 'Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject to enter into a contract.' In consenting to the Terms and Conditions presented at the point of order, you enter into a contract which requires Exa Education to process the data stipulated above in order to perform the filtering and reporting function through SurfProtect Quantum; in line with DfE online safety requirements and Prevent duty obligations.

The data stored by SurfProtect Quantum is minimal and only that which is explicitly necessary for the enactment of the filtering and reporting function, as defined above. As a result, SurfProtect Quantum does not record any special categories of personal data (such as genetic data or data revealing a user's religious beliefs) and therefore does not require compliance with conditions for processing under Article 9(2).

As the data controller, Exa Education is responsible for ensuring that the appropriate technical and organisational security measures are implemented to protect the personal data stored by SurfProtect Quantum. All data is therefore stored on servers owned by Exa Education in secure data centres based in the UK. Access to this data is provided over an encrypted channel and can only be accessed by a limited number of authorised Exa Education employees, whose job role explicitly necessitates this access. Data is stored for a duration of three months, or up to the length of the contractual period, after which time it is erased and cannot be retrieved. If data is required to be deleted prior to this, a formal request can be submitted to Exa Education for consideration.

With access to user data requiring careful control, we advise that you restrict access to your SurfProtect Quantum online portal to a limited number of staff with permission to view this information. If you have purchased your SurfProtect Quantum service through an Exa Education Partner, they will also have access to this online portal in order to assist with any support issues you may have. However, if you would like this access to be amended, please do not hesitate to get in touch with our team.