
WONDE

# School Data & GDPR Information

*Updated: 2nd March 2018*

## How long does Wonde retain data for?

Wonde will only access and retain specific data from a school's management information system (MIS) if it is required by a school approved third party. Wonde gives granular control to the school and third parties to ensure only the required data is shared and accessed. The data is frequently updated to ensure that Wonde only retains up-to-date data. If a record is removed from within the MIS it will be removed from Wonde during the next sync.

## Can a school request Wonde removes all data stored for their school?

Yes, schools can request Wonde to remove all data related to their school. Wonde will also inform any third party that they will no longer be able to access the schools data through Wonde.

## Where is the data stored?

Wonde stores school data within Amazon Web Services (AWS). The Ireland data centres are used to ensure the data stays within the EEA.

## Does Wonde hold any independent security accreditation?

Wonde is currently preparing for the ISO 27001 accreditation which this is due for completion in April 2018. Wonde has also committed to Cyber Essentials which will follow the ISO 27001 accreditation

## How is the data secured?

### *Data scopes*

Third parties define the scope of data required for their application within Wonde. These scopes can be defined down to a granular level (i.e. first name) which is approved by the school. An application is not able to access data outside of the agreed scope without further school approval.

***Data encryption***
Data is encrypted during transit and at rest using Amazon Web Service's RDS encryption service and our own SSL certificates. Information on the cyphers used are available with the following tool: https://www.ssllabs.com/ssltest/analyze.html?d=wonde.com&latest

***Access Control***
All database access between Wonde and AWS is protected by a secure password and IP limitations. A strong password policy is always in place. Two factor authentication is required for all accounts that have access to school data or administrational functionality. Staff only have access to the minimum amount of data required to perform their job. All laptops have encrypted hard drives.

## AWS deletions policy

Information relating to the deletions policy for AWS and additional GDPR compliance can be found at https://aws.amazon.com/compliance/gdpr-center/

## What information does Wonde extract?

Wonde will only extract data within the scopes approved by the school. Third parties define the scope of data required for their application within Wonde. These scopes can be defined down to a granular level (i.e. first name) which is approved by the school. An application is not able to access data outside of the agreed scope without further school approval.

## How often does Wonde extract data from the MIS?

Wonde extracts data from a school's MIS on a regular basis. By default updates occur multiple times a day although the schedule can be tailored to the schools requirements.

## Who has access to the data?

Wonde developers and engineers have access to school's data for troubleshooting and issue resolution purposes only. All staff undergo training and follow company policies to ensure the security and confidentiality of school data.

## Does Wonde use any third parties who have access to the data?

Only third parties who have been approved by a school have direct access to data. No other third party are permitted to access the school's data.

## Can schools request an individual's data to not be extracted from their MIS?

Yes, Wonde can block the data any individual who does not want Wonde to store or pass on their data to a third party. The data will be provided to Wonde from the MIS but any data associated with the individual's user ID will immediately ignored and not stored by Wonde.

## Will any data be transferred outside of the EEA?

Data is only transferred within the EEA or with third parties with sufficient accreditation (i.e. Privacy Shield) as in line with requirements under the GDPR.

## Can schools control what data is available to third parties?

***Revoking access***
Schools can revoke access to a third party with immediate effect. Revoking access to a third party takes place within the Wonde School Portal.

***Approving data scopes***
Schools will be notified when a third party requests access to their data or changes to existing data scopes. Schools will be required to approve the scopes before the third party is granted access to the data.

***Optional data scopes***
The third party outlines the data scopes they require as a minimum to run their application. Third parties can also define optional data scopes to access data that adds addition value or functionality to their application. Schools have the ability to approve these optional data scopes during the approval process or at a point the future.

## What software will be installed?

Depended on the school's MIS, and the infrastructure at the school, Wonde may be required to install software that has been accredited by the provider of the MIS.

## Do Wonde undertake DBS checks?

All Wonde staff with access to school data undergo a Disclosure and Barring Service (DBS) check carried out by a certified third party.

## What actions are Wonde taking with regards to the GDPR?

Wonde has reviewed policies, procedures and infrastructure to ensure they are in line with upcoming GDPR. Wonde is also auditing all third party suppliers to ensure compliance.

Wonde is committed to compliance with all relevant EU and Member State laws in respect of personal data, and the protection of the rights and freedoms of individuals whose information we collect and process in accordance with the General Data Protection Regulation (GDPR).

## Additional documentation

Please visit https://www.wonde.com/documents for further information