Privacy FAQs

Wonde - Support Document

School data & information security overview

This document is maintained by Wonde's Information Security Compliance team, and reflects the current information security and management procedures, controls, policies and practices across the company. It aims to clarify Wonde's position in the data processing chain and answer frequently asked questions around how schools, Wonde and third party edtech applications (**"Apps"**) interact.

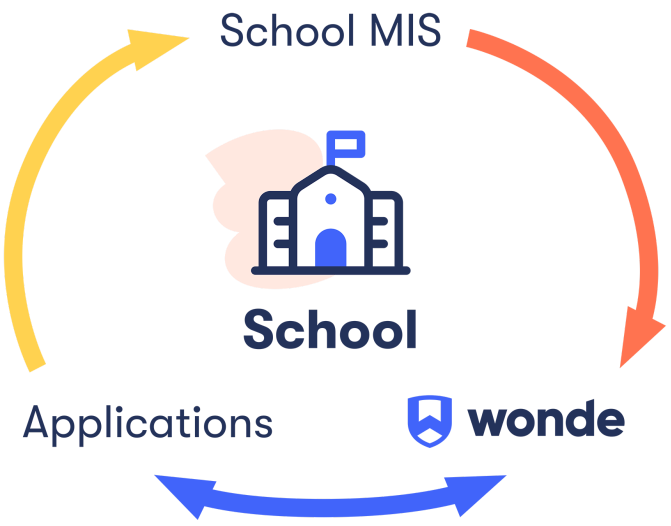
Company overview

Company Name	Wonde Limited
ICO Registration Number	ZB504536

Head of Information Security	Gemma Stannard
Data Protection Manager	David King
Data Protection email	data@wonde.com

How does the Wonde portal work?

The Secure portal sits between your school MIS and the Apps your school use.



Upon connecting to your MIS, Wonde enables Apps to synchronise their systems with the required information via a simple approval process.

All access to data requested by an App must be approved by the school before Wonde can connect and begin synchronising that data. Schools have the power to review, revoke and add data sets to an App, keeping the school in full control of its data at all times ***(See Appendix 1 for more information)***.

What data does Wonde process?

The types of data Wonde processes is dependent on what the school wishes to share with the App (controlled within the Wonde school portal). When connecting to a school MIS, Wonde will only extract relevant data for specific Apps that have been approved by the school.

To enable Wonde to provide an efficient service for schools and apps, we will request access to a range of data sets at the beginning of the connection process. These data sets are identified as being required by the majority of Apps.

Once an App connection has been approved by the school, Wonde will only extract relevant data from the data sets, ensuring the school has full control of what they are sharing.

How often does Wonde extract data from the MIS?

Wonde extracts data from a school's MIS on a regular basis to ensure Apps used by the school have accurate, up to date data with which to provide their service to the school.

For example;
At 09.45am a parent contacts the school office to say they have changed their mobile phone number. The school immediately inputs the new mobile phone number into the MIS. Later that day at 14.30pm the school sends an SMS text message to the same parent. The school would expect the new mobile phone number to be available within the SMS text messaging App used by the school, Wonde's frequent data extractions make this possible.

By default, data updates which overwrite existing data in an App occur multiple times a day, therefore there may be a delay between updating the information in the MIS and reflecting that information within an App. If required, Wonde can adjust the data extraction/update frequency to meet any custom school or App requirements.

Where is the data stored?

Wonde uses Amazon Web Services (AWS). These storage facilities are based in Ireland which keeps all school data within the European Economic Area (EEA).

AWS is a data storage supplier that offers the highest level of security to ensure it is compliant with the UK GDPR and the Data Protection Act 2018. Many government departments now use AWS including HMRC, the DVLA and Ministry of Justice.

Will any data be transferred outside of the EEA?

Wonde complies with all requirements of Data Protection Legislation including international transfers. Schools may seek to engage with Apps outside of the EEA in which case, a circumstance may arise where the school authorises the transfer. Wonde is able to facilitate this on the basis that schools have completed their own due diligence and approval processes.

Wonde seeks to engage our suppliers and software providers to retain any data within the EEA. However, in circumstances where that is not possible or in the absence of any adequacy decision, Wonde ensures that it has safeguards in place in accordance with Data Protection Legislation, which include contractual terms and Standard Contractual Clauses.

Who has access to the school's data?

Wonde employees are not permitted to view school data by default. In situations where it is necessary to access school data on behalf of the school, such as when the team at Wonde are assisting the school to investigate a specific support case, only an approved Wonde technical team member can gain access. Wonde employees are bound by contractual obligations regarding confidentiality and data protection. All staff are DBS checked and follow strict ISO27001 protocols. Wonde has an internal data protection team who regularly review this process

and enforce its data protection policies.

Can schools control what data is available to Apps?

Yes. Wonde's portal gives schools full visibility and control over the data they share. Apps define the data sets required for their App and the school can limit this according to the agreements they enter into with each App.

These data sets can be defined down to a granular level (i.e. first name, last name). Schools can view the data sets an App is requesting access to from within the Wonde school portal.

The data permissions requested by an App are in two different categories:

Required - The bare minimum of data an App requires for a school to use the App.

Optional - Additional data that may add enhanced functionality/features to the App.

On the rare occasion a school wishes to amend the 'Required data', they can do so by contacting Wonde on: support@wonde.com. Wonde will liaise with the App to ensure this doesn't impact the schools use of the App.

Schools are able to control the 'Optional data' requested by Apps from within the Wonde school portal via a simple toggle on/off system.

In addition, schools can revoke access to an App with immediate effect. Once revoked, the App will receive no further data from the schools MIS via Wonde. Please note: revoking access does not force the App to delete the school data previously provided to them. If this is required, the school should make a request directly with the App.

How long does Wonde retain data for?

Wonde will retain school data for the duration for which our services are being utilised by the school. Please see the Data Processing Agreement for further information on data retention.

Wonde only maintains the latest data from within a school's MIS. If a school removes all Apps from the Wonde school portal, and providing the school doesn't reconnect other Apps, Wonde will delete data as per our data retention schedule (available on request).

What software will be installed?

Wonde's software is cloud based and with the schools permission, connects to the schools MIS. There are various methods to connect Wonde depending on the MIS used by each school. This will be confirmed in Wonde's first communication with a school.

Does Wonde undertake DBS checks?

All Wonde employees undergo a Disclosure and Barring Service (DBS) check carried out by a certified third party.

Does Wonde hold any independent security accreditation?

Wonde has the following security accreditation:

ISO27001
Cyber Essential Plus

Data security is at the core of Wonde's business and is led by the internal data compliance and security team, ensuring our internal processes meet the highest standards.

Which data protection laws apply to Wonde?

In the UK, there are two key relevant data protection laws (**"Data Protection Laws"**) including the UK General Data Protection Regulation (**"UK GDPR"**) and the Data Protection Act 2018 (**"DPA 2018"**) which sets out key principles and regimes to govern the protection of personal data.

Wonde's privacy notice sets out the lawful basis upon which it processes any personal data in the provision of our services.

Wonde ensures it enters into all appropriate contracts with the relevant

parties to facilitate its services and to ensure compliance with the data protection legislation, including the UK GDPR and the DPA 2018.

A school has the primary responsibility - as the data controller - to determine the basis upon which it collects the school data and the purpose for which it may be used.

Is Wonde a data processor or a data controller?

Wonde is a data processor of a school.
The school is a data controller.

For the purpose of providing our services through our technology, to both schools and Apps, Wonde acts as a direct processor of the school and accordingly, enters into a data processing agreement directly with a school. This is in place to protect each schools data and the agreement formally sets out the instructions that Wonde must operate under, to process the school data for the school's benefit and to facilitate the transfer of school data to the Apps.

Wonde also enters into commercial and data protection agreements with Apps and MIS providers.

Does a school have a data processing agreement with Wonde?

Yes, to use Wondes services a school approves the Wonde Data Processing Agreement (DPA) which can be found here:

https://www.wonde.com/wp-content/uploads/Data-Processing-Agreement-Wonde.pdf

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

Yes., Schools can request Wonde removes all school data related to their school. Wonde will also inform any App that they will no longer be able to access the school's data through Wonde.

Can schools request that an individual's data is not extracted from their MIS?

Yes. Wonde can stop the data of any individual who does not want Wonde to store or pass on their data to an App. Schools can manage this process within the Wonde School Portal.

How does Wonde secure school data?

- All data shared between the school and Wonde is encrypted during transit and at rest. Wonde uses the AWS RDS encryption service and its own SSL certificates, an analysis can be found here.
- Access to school data is protected by active access rights management, adopting the principle of least privilege, secure passwords and IP limitations.
- Two factor authentication is required for all accounts that have access to school data or administrational functionality.
- Monthly penetration testing is completed on Wonde's systems, an internal review process is completed to act on any feedback provided.
- Wonde operates a suite of physical security measures within our offices.
- All devices used by staff are fully encrypted and utilise the most up to date anti-virus software and hard drive encryptions to protect them.
- Wonde performs regular disaster recovery and business continuity testing

Does Wonde have a data breach policy?

Yes. Wonde has internal and external procedures and policies in place to deal with any data breaches or incidents.

Questions?

If you have any questions or would like further information please contact: support@wonde.com.