School Data & Information Security Overview

Helping schools to securely manage their data

wonde

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 help 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 and how Wonde complies with any applicable laws to facilitate this relationship specifically in relation to its operations in South Africa.

Company overview

Name	Wonde Limited
Company Number	08645640
UK ICO Registration Number	ZA118834
Head Office	Furlong House, 2 Kings Court, Newmarket, CB8 7SG
Website	www.wonde.com

Security Accreditation	ISO27001
	Cyber Essentials Plus

Head of Information Security	Andrew Dool
Data Protection Manager	David King
Data Protection Officer	data@wonde.com

What is Wonde?

Wonde has been designed with data protection and security in mind and is now used by 25,000+ schools and by 400+ Apps.

A school needs total confidence in the security and reliability of their technology. Wonde's innovative platform has been designed and built to integrate seamlessly with the School Management System.

Wonde's intuitive data management system provides schools with a single portal from which they have full visibility and control over the data they share with Apps, whilst maintaining the highest levels of data security and integrity.

Wonde is used by the large majority of Apps to connect and synchronise their platform with the important data within a school's School Management System. These include Apps such as Karri, Allxs and 2Simple.

Wonde is on the UK Government's G-Cloud framework and is a framework supplier for the Crown Commercial Service.

How does Wonde work?

Wonde is a secure platform that sits betweens a school's School Management System and the Apps that a school uses.
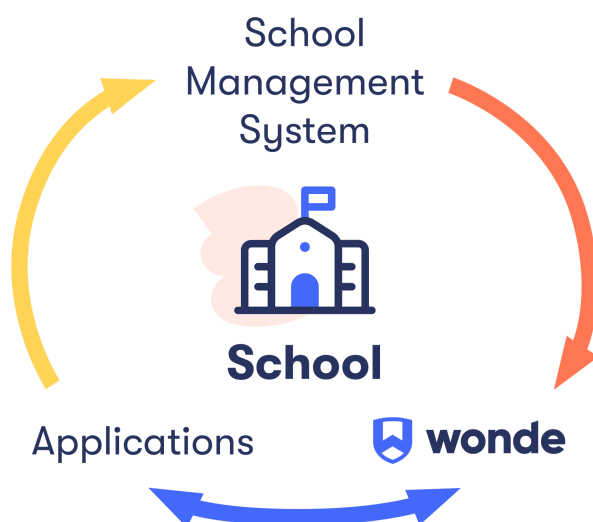
Once Wonde connects with a school's School Management System, Apps can synchronise their systems with the required information all via a simple approval based process with the school in full control of what data is shared with each App.

Wonde is designed to help schools be the masters of their data. 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. Upon connecting to a school's School Management System, Wonde will only extract the data that is requested by Apps used by the school AND ONLY data that is approved by the school.

Throughout the installation of Wonde at a school, Wonde will request access to a range of data sets that are required for the majority of Apps. Wonde cannot extract the data until an App connect has been approved by the school. The school has full control of this process inside the Wonde school portal.

How often does Wonde extract data from the School Management System?

Wonde extracts data from a school's School Management System on a regular basis to ensure Apps engaged by the school have accurate and 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 School Management System. 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 School Management System and reflecting within an App. 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 South Africa to keep school data within its server.

For any data transfers outlined below, Wonde still uses AWS for all of its data storage in the EEA.

AWS is an approved data storage supplier and offers the highest level of security to ensure it is compliant with the data protection laws in both South Africa namely the Protection of Personal Information Act 2013 (**"POPIA"**) and the data protection laws in the United Kingdom such as the UK GDPR and Data Protection Act 2018.

Will any data be transferred outside of South Africa?

Wonde complies with the requirements of POPIA for international transfers. In the event Wonde transfers any school data to third parties providing services to Wonde who are based outside of South Africa such as to the United Kingdom or the EEA without obtaining your specific written consent, Wonde will do so in accordance with the requirements of POPIA. This might also apply in circumstances where the school elects to use an App based outside of South Africa, which it chooses to do so, with or without Wonde.

Such transfers may be to facilitate services supporting Wonde providing IT administration services and hosting services, and parties providing assistance with managing our marketing databases, or to send school data to the Apps.

Whenever Wonde transfers any school data outside of South Africa, Wonde ensures a similar degree of protection is afforded to it by ensuring at least one of the following safeguards is implemented:

(a)   There is adequate legal protection. This means that the recipient of the school data must be subject to a law, binding corporate rules or binding agreement such as a data processing agreement, which provide an adequate level of protection that effectively upholds the principles for reasonable processing, and that include provisions that are substantially similar to the conditions for the lawful processing of personal information and for the further transfer of the school data.

(b)   Wonde believes or reasonably believes that the country that the information is being transferred to has substantially similar privacy obligations and an adequacy decision applies;

(c)   a permitted general situation applies i.e it is necessary for the performance of a contract;

(d)   the data subject consents to the transfer;

(e)   it is in the interests of the data subject i.e. the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the responsible party and a third party; and

(f)   the disclosure is required and is authorised by applicable law.

Where Wonde participates in a valid cross-border transfer mechanism under the applicable laws, Wonde will (and, where appropriate, the school) will ensure that appropriate safeguards are in place to ensure an adequate level of protection with respect to the privacy rights of individuals and compliance with the applicable laws in relation to the personal information.

Schools may seek to engage with Apps outside of South Africa as mentioned above, 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 with the schools approval.

Wonde also seeks to engage its suppliers and software providers to retain any school data within the United Kingdom and 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 as stated above..

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 personnel can access it. Wonde employees are bound by their 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

At no other time can any employee of Wonde access the schools Wonde school portal. This can only be done for support related enquiries and the school has to give Wonde the permission to do so.

Can schools control what data is available to Apps

Yes - Wonde's platform gives schools full visibility and control over the data they share. The 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 sets 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.

Within the Wonde school portal, schools can revoke access to an App with immediate effect. Once revoked, the App will receive no further data from the schools School Management System via Wonde. Please note that 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. Wonde enters into a data processing agreement with a school which sets out Wonde's provisions on security and data retention.

Wonde only maintains the latest up-to-date information from within a school's School Management System. 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).

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 which ensures our internal processes meet the highest standards.

Which data protection laws apply to Wonde?

In South Africa, the principal data protection law is POPIA which sets out the key principles and regimes that govern the handling and use of personal information including the school data.

In the UK, there are two key relevant data protection laws including the UK General Data Protection Regulation (**"UK GDPR"**) and the Data Protection Act 2018 (**"Data Protection Act"**) which apply.

The school has the primary responsibility as the responsible party to determine the basis upon which it collects the school data and the purpose for which it may be used.

Wonde ensures it enters into all appropriate contracts with the relevant parties to facilitate its services and to ensure compliance with POPIA, the UK GDPR and the Data Protection Act.

Is Wonde a responsible party or an operator of the personal information?

Wonde is the operator of the school data and the school is the responsible party.

For the purposes of providing the services through Wonde's technology, to both schools and Apps, Wonde acts as an operator of the school and accordingly enters into a data processing agreement directly with a school to formalise the relationship.

This is in place to protect each school's data and the agreement formally sets out the instructions that Wonde must operate under, to collect and use 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 any applicable data protection agreements with Apps and School Management System providers.

Is Wonde compliant with Popia?

Wonde provides its services in South Africa and as such, its internal processes and procedures are designed to be compliant with Popia.

The school as the responsible party determines what school data is used by Wonde. The data processing agreement governs any such instructions to Wonde.

Wonde will therefore assist the school in ensuring that the data subject's rights under Popia are adhered to such as the right to be notified, the right to request, correct and delete school data.

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

Yes, schools can request Wonde to remove all school data related to their school or for a specific data subject. Wonde will also inform any App that they will no longer be able to access the school's data through Wonde.

This is in accordance with the requirements of Popia.

Can schools request that an individual's data is not extracted from their School Management System?

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 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 all of 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 in place a data breach policy?

Yes - Wonde has in place internal and external procedures and policies to deal with any data breaches or incidents to ensure it complies with any requirements of Popia or UK GDPR.

Where can you find more information on how Wonde helps schools manage their data?

If you have any further questions or require more information, you can reach the data compliance team by emailing data@wonde.com.

Appendix 1: How schools install and connect to application

This document explains the process a school first follows when they choose to configure an integration between one of the third party applications (App) they use and their School Management System through Wonde.

The process consists of two key stages of firstly approving the App, followed by configuring the connection between their School Management System and Wonde.

Once the school's first App has requested to connect to the school, Wonde will verify this contact at the school via a phone call. An email is then sent from Wonde with a secure link for the school to create their admin account.
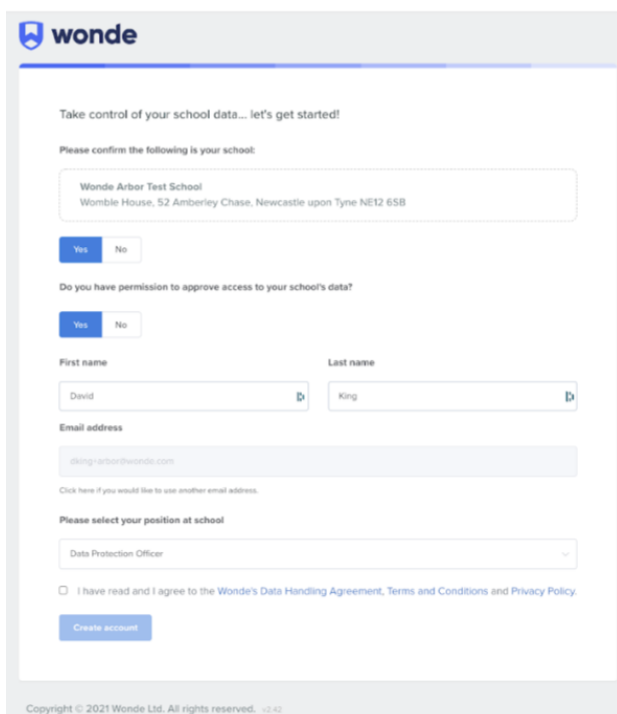
1) Creating your school's Wonde account

Upon receiving the initial email and clicking through to begin creating their account, the first step is to confirm that the user has the authority to approve access to school data stored in the School Management System. If the user doesn't have permission, an additional screen asks for the correct contact details to be added. A new email invite is then sent to the nominated person.
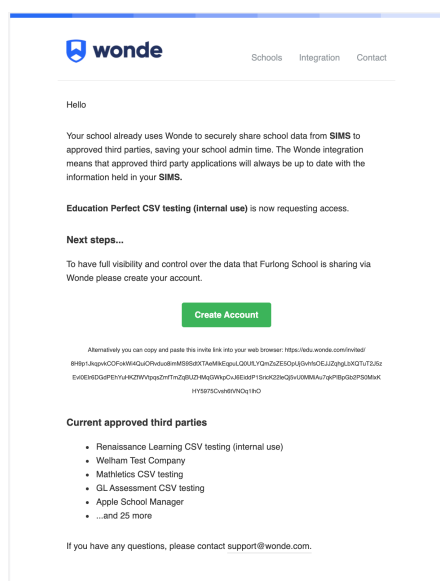
Once the user who has the authority to approve access to school data receives the email invitation (as shown above), they click through to begin their school's

Wonde account creation, filling out the following fields.

Upon clicking 'Create Account', their account becomes active and they will be able to review and approve any requests from third party apps to connect to their school data.

2) Reviewing a request from a third party application

Each time a School Wonde Admin User (Admin) logs into their Wonde portal, they arrive at the Dashboard which displays any new apps that have requested to connect and are therefore 'Pending Approval'.

● The user can now click on the App to review the data the App is requesting be shared with it. This is the same data that the school would previously be sending to it via CSV or manually inputting.

● The user can now see the list of each data set (permissions) that the app has requested to be shared with it in order for it to work most effectively.

● These permissions are either 'Required' or 'Optional'.
○ Required - The basic data that the App requires in order to function.

○ *Optional - The school has the ability to toggle these on/off, potentially having an impact on the functionality of the App. Optional permissions are often used for additional modules that an App has which not all schools use and hence the school can toggle them on/off as needed.*

● *If a group of permissions (e.g. Photo) is selected, such permissions are shown on a granular level to highlight the individual fields.*

Once the user has reviewed the permissions requested by the app, they can choose to either approve or decline the App's access to the requested school data.

3) Approving or Declining a third party application

If the Approve access option is selected, an email approval receipt is sent to all Admins and to the App. This email highlights the name of the App and their permissions, who approved them, their position and the date/time approved.

If in the future the App makes a change to their permissions or requests additional data be shared with them in order perhaps for a new feature to work, the school will be prompted to review and approve any changes before the App can access the new permissions.

If the Decline access option is chosen, the App will receive an email highlighting this, the reason the school declined and therefore the data will not be shared with them. Should the school change their mind at a later stage and wish to approve the connection, the App will have to go through the request process once again.
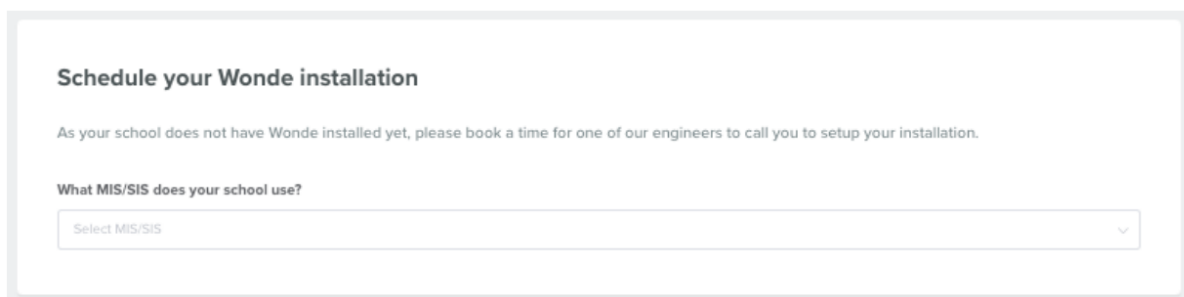
If the App is approved by the school, the school will then further engage with Wonde to configure the integration of Wonde with the school's Management Information System. Once this is complete, Wonde will be able to sync the permissions approved by the school and provide them to the App.

4) Integrating with the School Information System
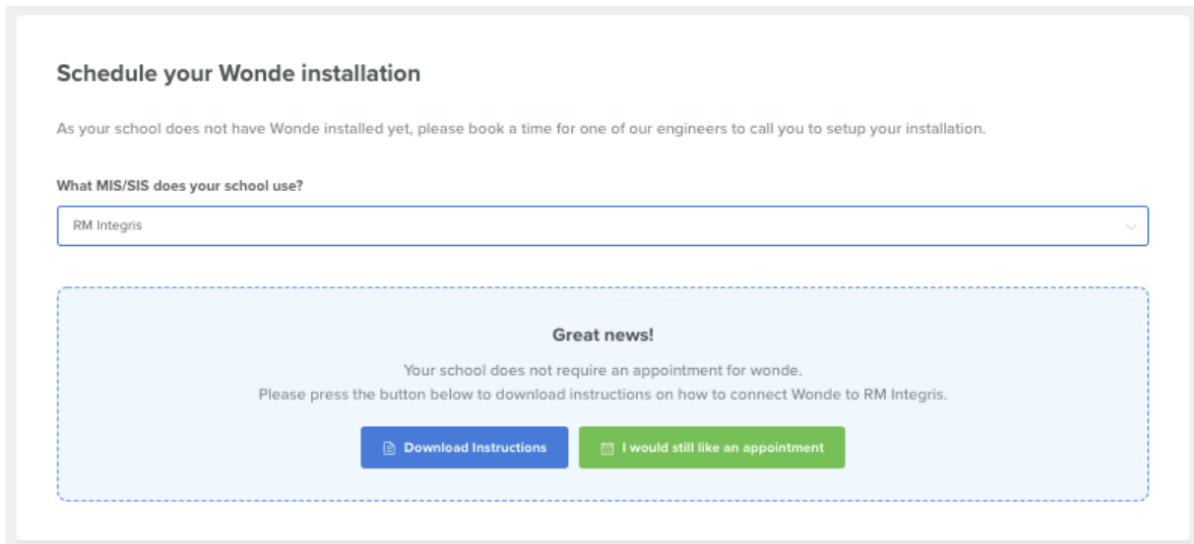
Once an App has been granted access ('Approved access' above), the Admin is taken through to the steps of configuring the connection of their School Management System to Wonde. This is a one time process and only needs to be completed after the first App has been approved by the school.

This can be done by following the simple installation guide or with the help of Wonde's Integrations Team.

a) From the dropdown, select the type of School Management System used by your school:

Schedule your Wonde installation

As your school does not have Wonde installed yet, please book a time for one of our engineers to call you to setup your installation.

What MIS/SIS does your school use?

Select MIS/SIS

b) Depending on the School Management System selected, the following step will either provide the
user with a guide to complete the integration or arrange an appointment.

c) If the user selects the option to schedule an appointment, they simply choose a date/time whereby a Wonde representative will make contact to assist them with the process.

5) Access control

Wonde also provides a school with the ability to control exactly which individuals' data is shared with the App. The 'Access control settings' tab is available in the top right of the page when viewing an app's details.
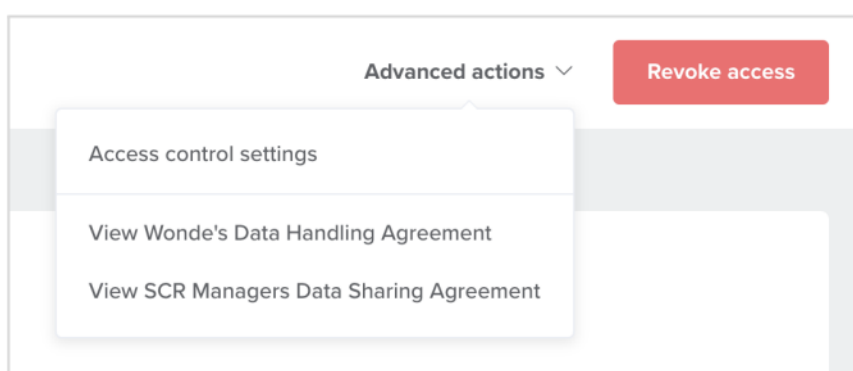
There are three options available:

● First option allows all users associated with the permissions to be accessed.

● Second option is when the school wishes to exclude certain users - The

data associated with any individuals selected will not be passed onto the third party app.

● Third option is when the school wishes to only include a small number of users - Only the data associated with the individuals selected will be passed onto the app. All other users will be excluded.

Questions?

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