

DATA PROTECTION IMPACT ASSESSMENT (DPIA)

Name of School: Campsbourne School

Assessment Carried Out By: Jonathan Smith (Head Teacher)

Reviewed By DPO On: 15/03/2022

Outstanding Questions and Comments

We will be unable to sign off the DPIA without receiving the response to these questions (which will mean the DPIA will be incomplete). If you are unsure of the answers, we have tried to put best practice guidance in brackets or explaining why we need to know the answer to this question:

1.Name and Aim of Project/Technology/System

Department For Education attendance data collection

Department for Education are seeking more regular data collection from schools in order to combat attendance issues and provide better intervention strategies.

They will be using Wonde to conduct regular data extraction.

2.Personal Data Used by Project/Technology/System

Data Collected Includes: -

Demographic data

- Name
- Date of birth
- Gender
- Ethnicity
- Unique pupil number
- School unique reference number
- Local Authority code
- Attendance sub-codes

Vulnerable children indicators

DATA PROTECTION IMPACT ASSESSMENT (DPIA)

- Looked after children status
- SEN support
- EHC plan
- FSM data
- Pupil premium data
- Children in need and child protection data

Data is collected through Wonde. Wonde will be collecting and using sensitive and personal data for pupils and staff (we can decide to allow this). There is a little flexibility in some of the data required but most of what is asked for is necessary for the system to work.

All the data requested is available on our MIS system and there shouldn't be any new data required.

3. Purpose of Processing

The purposes behind regular attendance data collection is to help shape government response to the pandemic, offer insight into attendance of pupils and allow interventions to take place promptly.

The legal reason for processing this data will predominantly be public task. As special category data is used, the lawful basis is in the substantial public interest specifically for government purposes, equality of opportunity and safeguarding.

4. Steps taken to protect data

DfE's steps to protect data

Department for Education have completed a data protection impact assessment in conjunction with the ICO This is an attachment to this impact assessment.

DfE have a privacy notice to share with parents and pupils. Schools should ensure this is accessible.

Data is held on Microsoft Azure cloud hosting based in the EEA.

Regular reviews will be conducted to determine the ongoing necessary of this programme.

Wonde's steps to protect data:

Wonde stores the School's data within Amazon Web Services (AWS). The Ireland data centres are used to ensure the data stays within the EEA. Wonde is ISO 27001 accredited and has also committed to Cyber Essentials which will follow the ISO 27001 accreditation.

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>.

DATA PROTECTION IMPACT ASSESSMENT **(DPIA)**



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

The School can request Wonde to remove all data related to the School. Wonde will also inform any third party that they will no longer be able to access the School's data through Wonde.

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

Sharing with third parties:

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.

The School can revoke access to a third party with immediate effect. Revoking access to a third party takes place within the Wonde School Portal. The School will be notified when a third party requests access to our data or changes to existing data scopes. The School will be required to approve the scopes before the third party is granted access to the data.

Data is only transferred within the EEA or with third parties with sufficient accreditation.

Data retention

Wonde Ltd will process personal data for as long as required by schools, their approved third parties and any direct services provided to individuals. Wonde will only store the personal data for the retention period in line with the requirements of the GDPR.

Wonde shall within a reasonable period of either a written request from the School, or the termination of this Agreement, delete and procure the deletion of all copies of the School Data

Wonde confirm that, upon request or termination of agreement, they will delete school data. Their data is backed up for a period of 31 days, so Wonde aim for data to be deleted within that timeframe.

School's steps to protect data:

The School ensures that the data which Wonde accesses is pertinent to the programme.

1. Data protection impact assessment in place (both DfE and school have completed a DPIA).
2. All systems have the appropriate technical measures in place (e.g. intrusion, detection, firewalls, monitoring, encryption to ensure that data is protected at all times whether in storage or in transmission)
3. Only authorised members of staff can access the admin side of Wonde.
4. Staff receive training/have awareness on good practice of using Wonde.
5. To update privacy notices with detail on data collection.
6. To share and make accessible the DfE privacy notice and any further literature they provide about the process.
7. Information packs will be available to parents on the process in September 2022.

DATA PROTECTION IMPACT ASSESSMENT **(DPIA)**



5. Impact And Risks

School Assessment of Risk		
	Risk Level	Comments
Likelihood of harm to data subject	Unlikely	
Severity of harm (regardless of likelihood)	Severe	
Overall risk (taking into account measures to reduce risk above)	Low-Medium	
DPO Assessment of Risk		
Likelihood of harm to data subject	Unlikely	
Severity of harm (regardless of likelihood)	Severe	
Overall risk (taking into account measures to reduce risk above)	Low-Medium	No new data collected. Data mostly involves more regular collection of data.

Compliance Statement

I can confirm that this data protection impact assessment has been completed to the best of my knowledge and that the software complies with the data protection principles under the GDPR.

All privacy risks and solutions have been considered and represent a proportionate response to the identified risks to personal data.

Signed: *Jonathan Smith, for and on behalf of Campsbourne School* Date: 15/03/2022

DPO Statement

I confirm that I have reviewed the DPIA above and have made recommendations set out in the comments above which should be accounted for before implementing the above.

Signed: *Patrick Ballantine, for and on behalf of Judicium Education* Date: 15/03/2022

DATA PROTECTION IMPACT ASSESSMENT
(DPIA)

Review

This data protection impact assessment should be reviewed to ensure control measures are working and updated to reflect significant findings or changes.

Date of next review:	Spring 2023
Review to be carried out by:	Jonathan Smith (Head Teacher) and DPO