DATA PROTECTION IMPACT ASSESSMENT

We have created the below template to help you with your DPIA.

This is only a template and your DPIA is not yet complete. It will not be valid until you have made the suggested edits and you have a copy signed-off by us as completed and approved.

Please follow our colour-coded key below to ensure you add all the extra details which tailor this DPIA to your school's plans.

URGENT: To be completed by the School.

ACTION REQUIRED: Optional wording for the School to include or amend.

OUTSTANDING: We require further information from the provider.

Name of School: BOUNDS GREEN SCHOOL

Assessment Carried Out By: FAYE PAPINI

Reviewed By DPO On: 06/07/2021

1. Name and Aim of Project/Technology/System

Medical Tracker

Medical Tracker is an online software to report first aid incidents, track medications and student care plans. The online forms are built to comply with DFE, OFSTED and RIDDOR guidelines. Medical Tracker allows us to comply with DfE Guidelines to accurately store records, notify parents of incidents and report serious incidents and near misses.

2. Personal Data Used by Project/Technology/System

Sensitive Personal Data will be processed using Medical Tracker. The data will be synched daily from SIMS (the school's Management Information System) into Medical Tracker via Groupcall. There is no manual data entry, the data will be synched so that only relevant and current data is on Medical Tracker.

Medical Tracker synchs with SIMS to extract the following fields

Staff data

- Staff ID
- Staff email
- Title
- Legal forename
- Legal surname
- Staff role
- First Aid qualification – start date & end date
- Email
- Address and telephone number

Pupil

- Legal Surname
- Legal Forename
- DOB
- Current NC Year
- Gender
- Medical Needs
- Medication
- Care plan

Parent/Guardian data

- Parent name
- Parent email
- Parent mobile
- Relationship to pupils (mother/father)

Visitor data (only in the event of accident/incident)

- Name
- Email
- Date of birth
- Nature of incident

All current pupils and staff data will be synched onto Medical Tracker from our MIS system using Groupcall.

Medical Tracker retains leaver information if they have any records associated with their profile however it does not retain parent/carer or address details of students that have left only the basic details and the information within each record. The application works the same for staff or visitor records if they have had a record created against their profile.

3. Purpose of Processing

The data is provided to medical tracker is maintained in order to comply with the public task legal reason for processing. The data comes from our SIMS system, where parents provide information regarding medical conditions for their child/children.

Medical Tracker enables the school to record, track and manage student health.

4. Steps taken to protect data

The personal data shared will include some sensitive data relating to medical needs.

Medical tracker act as the Data Processor. This means that the parties should have a written contract/data sharing agreement in place in accordance with the DPA 2018.

The School as data controller has a duty to ensure that Medical Tracker has adequate security in place. The School as data controller is legally responsible for the processing of data on behalf of the processor. In situations such as data breach it will be the school as data controller who will be responsible.

Steps Taken By Medical Tracker to protect Data

As of the Effective Date of the DP Agreement, when Processing Personal Data on behalf of the school in connection with the Service, Medical Tracker as Data Processor shall implement and maintain the following technical and organisational security measures for the Processing of such Personal Data ("Security Measures"):

• Physical Access Controls: Data Processor shall take reasonable measures to prevent physical access, such as security personnel and secured buildings and factory premises, to prevent unauthorised persons from gaining access to Personal Data, or ensure Third Parties operating data centres on its behalf are adhering to such controls.

• System Access Controls: Data Processor shall take reasonable measures to prevent Personal Data from being used without authorisation. These controls shall vary based on the nature of the Processing undertaken and may include, among other controls: authentication via passwords; two-factor authentication; documented authorisation processes; documented change management processes; and/or, logging of access on several levels.

• Data Access Controls: Data Processor shall take reasonable measures to provide that: Personal Data is accessible and manageable only by properly authorised staff; direct database query access is restricted; application access rights are established and enforced to ensure that persons entitled to use a data processing system only have access to the Personal Data to which they have privilege of access; and, that Personal Data cannot be read, copied, modified or removed without authorisation in the course of Processing. All backups are encrypted before being stored using keys from Amazon Key Management Services (https://aws.amazon.com/kms/). The keys are rotated yearly, and all keys required to decrypt existing backups will be stored until no longer required.

• Transmission Controls: Data Processor shall take reasonable measures to ensure that it is possible to check and establish to which entities the transfer of Personal Data by means of data transmission facilities is envisaged so Data cannot be read, copied, modified or removed without authorisation during electronic transmission or transport.

• Input Controls: Data Processor shall take reasonable measures to provide that it is possible to check and establish whether and by whom Data has been entered into, modified or removed from data processing systems. Data Processor shall take reasonable measures to ensure that (i) the Personal Data source is under the control of the Customer; and (ii) Personal Data integrated into the Service is managed by secured transmission from the Customer.

• Data Backup: Back-ups of the databases in the Service are taken on a regular basis, are secured, and encrypted to ensure that Personal Data is protected against accidental destruction or loss when hosted by Data Processor. The backups are located across 3 London UK data centres and encrypted.

• Data Security: Where appropriate and reasonable, Data Processor should make use of accepted Data Security controls including but not limited to encryption, pseudonymisation and anonymisation.

• Logical Separation: Data from different Data Processor's Customers is logically segregated on Data Processor's systems to ensure that Personal Data that is collected for different purposes may be Processed separately.

• Network Security Controls: Data Processor shall implement appropriate network security controls based on risk assessment as it relates to Data Protection; commonly including Firewalls, Anti-Malware and system logging.

• Security Testing and Assurance: Data processor shall establish mechanisms for testing and assessing the effectiveness of technical or organisational measures used for establishing data security.

The data transferred from SIMS (the school's management information system) contains identifiable information about our pupils, parents and staff. Medical Tracker uses Groupcall to transfer the data from SIMS to Medical Tracker. This is completed by Groupcall providing a read-only API feed that allows the data to be drawn from SIMS to Medical Tracker. Groupcall cannot view or edit the data, the sole purpose is to transfer data.

Medical Tracker has clear data security measures and back up processes.

Steps to be taken By the School To Protect the Data

- Each user's access will be customised to the appropriate level of access (e.g. full admin rights through to read only access).
- Staff will receive training to the level required for their role using the software.
- Only first aiders will have permission to add and edit information on Medical Tracker.
- The school will ensure strict access controls are in place and strong passwords are used and not shared.
- The school will create internal guidance or processes to avoid risks e.g. log out of software once finished/lock PC when leave desk etc.
- We will share the Medical Tracker Privacy notice on our school website.

- Medical Tracker retains data only while we continue to use the software. If we cancel our subscription, we will receive all data within 90 days. This will then be retained by the school in order to adhere to DfE retention guidelines.

5. Impact And Risks

School Assessment of Risk		
	Risk Level	**Comments**
Likelihood of harm to data subject	Unlikely	Secure portal, with limited access only to key staff.
Severity of harm (regardless of likelihood)	Significant	The software harvests a lot of basic and personal information relating to pupils, parents and members of staff
Overall risk (taking into account measures to reduce risk above)	Low	
DPO Assessment of Risk		
Likelihood of harm to data subject	Unlikely	
Severity of harm (regardless of likelihood)	Minimal	
Overall risk (taking into account measures to reduce risk above)	Low	

Compliance Statement

I can confirm that this data protection impact assessment has been completed to the best of my knowledge and that Sound Cloud 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: 

Date: 06/07/2021

DATA PROTECTION IMPACT ASSESSMENT

DPO Statement

I can confirm that I have reviewed the DPIA above and are satisfied that the school have taken appropriate and proportionate steps to protect the data

Signed: Tosin Lawal on behalf of Judicium Consulting Ltd. **Date: 06/07/2021**

Judicium Education
Judicium Consulting Ltd
72 Cannon Street
London EC4N 6AE

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:	
Review to be carried out by:	