DATA PROTECTION IMPACT ASSESSMENT (DPIA)

Name of School: Bounds Green School

Assessment Carried Out By: Faye Papini

Reviewed By DPO On: 03-09-2021

1.Name and Aim of Project/Technology/System

Operoo (CareMonkey)

https://www.operoo.com/

The system will be used for new Nursery and Reception admissions on an annual basis. The school is not using the other aspects/modules within Operoo at this time.

2.Personal Data Used by Project/Technology/System

Operoo collects the data that the school share with them directly (or through the MIS system).

Staff

- Full Name
- School Email Address

Students

- Full Name
- DOB

Parents

- Full name
- Email Address

Accounts will be generated using pupil basic details and parent email. Parents/carers then have to opt into using the system. Only data entered by the parent/carer will be imported into SIMS from the online form.

3.Purpose of Processing

The school is processing this data as there is an obligation to contact parents

The legal basis for processing this information is a mixture of public task (the school are performing their duty as a school) and consent – as parents will be required to opt in to use the system.

DATA PROTECTION IMPACT ASSESSMENT (DPIA)

4.Steps taken to protect data

Steps Taken by Operoo

- Operoo is designed for Adult Users to share electronic admission form and any relevant medical and consent forms with other Organisations on behalf of themselves, or for Individuals they are responsible for (e.g. their child).
- The Emails they send (like most emails) are sent encrypted, however they are stored on third party systems (e.g. email clients such as gmail/outlook) as clear text. For this reason, emails they send never contain any confidential information such as medical information or contact details.
- Limit access to Personal Information about you to employees who we believe reasonably need to come into contact with that information to provide Services to you or in order to do their jobs.
- Operoo uses SSL encryption to store and transfer Personal Information. Despite this, the security of online transactions and the security of communications sent by electronic means or by post cannot be guaranteed.
- Your account is always password protected, and we utilize strong password policy and non-reversible hashing for storage of the password.
- Additional security option to enable Two-Step Verification, (also know as Two-Factor Authentication) which prevents anyone from accessing individuals account without possessing the physical device.
- The security sub-layer is capable of detecting any anomaly within the system to proactively prevent malicious activities and alert their security staff.
- Operoo will always notify individuals by email when your account has been accessed from a new device.
- Operoo uses military level security – the highest standards in Internet and data security.
- Data is always encrypted at rest and in transit.
- Our security layers include strong cryptographic implementations (such as 256 bit encryption, 256 bit data encrypted TLS systems using Advanced Encryption Standards) and defensive-in-depth network protection (with multiple firewalls and active monitoring systems).
- Operoo has an ongoing security and compliance program that includes penetration testing, vulnerability testing and code reviews by independent third parties.
- Operoo's network is designed with security in mind. This includes intrusion detection firewalls and monitoring.
- The Company regularly conducts penetration and threat modelling to ensure our network is properly secure and up-to-date.
- The Company backs up the school's data in the same region every hour.
- Operoo's physical infrastructure is hosted and managed within Amazon's secure data centers, utilising the redundant services of Amazon AWS. AWS provides a highly reliable, scalable and secure infrastructure platform designed to tolerate system or hardware failures with minimal impact.
- The Operoo System consists of various service components that are all load balanced across multiple redundant instances. This ensures that any single hardware or data centre failure does not impact the delivery of their services. In addition, by hosting their servers in the AWS data centers, they take advantage of Amazon's redundant power, environment and internet connectivity systems.
- Operoo databases are provisioned using Amazon's RDS service which gives us the ability to do point-in-time recovery. The Company periodically tests its Disaster Recovery Plan by practicing starting new instances and restoring databases within the AWS infrastructure. Any hidden unknown dependencies during these tests are identified and logged for remediation.
- The Company's business continuity plan also takes into account the continued operation of the head office in Melbourne Australia and the availability and backup of key staff required for continued delivery of our service.

- AWS computing environments are continuously audited, with certifications from accreditation bodies across geographies and verticals including ISO 27001, FedRAMP, DoD CSM, and PCI DSS.
- AWS is fully compliant with applicable EU data protection laws, and the AWS Data Processing Agreement incorporates the model clauses. This means that users wishing to transfer personal data from the European Economic Area (EEA) to other countries can do so knowing that their content in AWS will be given the same high level of protection it receives in the EEA.
- Data is stored on servers in that region, and will never be stored outside of that region. For citizens (data subjects) in the EU, data is stored in Ireland (Dublin).

Mobile Data Security

- The Operoo App is registered on a device using a unique username and password. Second Factor code/fingerprint is then required to access data.
- Data is only accessible by authorised users with that unique username and password.
- All data transfer is handled over SSL secure connections. Operoo uses an "Extended Validation" SSL site certificate so that users can be sure they are talking to Operoo when accessing the data.
- When the Operoo App is accessed on a mobile device or tablet, the data is stored in an encrypted format to give authorised users access to emergency information, even when they are offline or outside mobile range.

<u>Steps taken by the School</u>

- Authorised users who can send communications have received training on its use
- To implement complex passwords to access the App and encourage parents to also adopt a complex password.
- Each user at the school has its own username and password and there are different levels of access (depending on job role).
- To retain data in line with the School's data retention policy.
- Awareness on use of Operoo
- Data will be treated with the strictest confidence.
- School will be sharing Parents' contact details (email addresses and mobile phone numbers). These are considered medium risk details as the user has the protection of choosing to reject or block unwanted contact.
- The system will be used for admissions in Nursery and Reception classes.

<u>Retention</u>

- Users can permanently delete their Operoo Account (including all Care Profile information) at anytime.
- If a User chooses to permanently delete their account, Operoo will make the User aware of which Organisations have stored shared information, and provide contact details of the Organisation for the User to direct requests for erasure.
- Data that is stored on devices automatically expires and is deleted from local storage after a set period of time, unless authorized users re-synchronise with the server.
- Data that is no longer authorised is automatically deleted from local storage.
-

<u>Data Shared with Third Parties</u>

- Operoo does use other third-party systems to run the business and communicate with Users, Customers and Prospects. They ensure any third-party products do not store any private medical information in any system outside Operoo. These service providers may be located in the United States of America, and include:
    - Zoho – Operoo integrates with Zoho to support Users with Live Chat.
    - Customer Relationship Management (CRM) – To manage our leads and customer database (separate to User data).
    - Marketing Automation Platform – To send marketing promotions.
    - Accounting Software – To process account payments.
    - Google Analytics – To analyse web traffic.

- Google Cloud Translation – To perform language translations.
- Email – To send or reply to emails from a User, Customer or Prospect.

5.Impact And Risks

School Assessment of Risk		
	Risk Level	**Comments**
Likelihood of harm to data subject	Unlikely/Possible/ Likely	Unlikely
Severity of harm (regardless of likelihood)	Minimal/Significant /Severe	
Overall risk (taking into account measures to reduce risk above)	Low/Medium/High	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: 03/09/2021**

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: Jessica Gant on behalf of Judicium Education **Date: 03-09-2021**

DATA PROTECTION IMPACT ASSESSMENT (DPIA)

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