Data Protection Impact Assessment (DPIA)

Last Updated: 09 June, 2020

1

About Operoo

Operoo is an online and mobile platform for Forms, Medical Records and Field Trip Management.

Operoo is designed with privacy and security as our highest priority. We apply stringent processes to keep data safe through design, development, testing, and day-to-day operations.

The purpose of this document is to help customers and prospects understand how Operoo keeps data private and secure. Plus, you'll find the answers you need to complete your own **Data Protection Impact Assessment (DPIA)**.

Table of Contents

- The GDPR has arrived (page 4-6)
- Why process personal information in Operoo? (page 7-9)
- Does my organisation need a DPIA? (page 10)
- Key questions to help you understand and demonstrate GDPR compliance (page 11)
    1. What personal data may be collected? (page 12-13)
    2. What consent is recorded? (page 14-15)
    3. Does any personal data flow anywhere else? (page 16-18)
    4. Who has access to personal information? (page 19-23)
    5. How does Operoo keep personal data secure? (page 24-31)
    6. What is the data retention period? (page 32-33)
    7. How is personal data securely deleted? (page 34-36)
    8. What policies and procedures are required? (page 37-39)
- Learn More (page 39-44)

The GDPR has arrived

The **General Data Protection Regulation (GDPR)** was introduced to give EU citizens / residents more control over their personal data held by organisations.

The GDPR applies to any organisation that does business in the EU, including schools, academies and other educational establishments, clubs, and businesses (and their supplying software companies such as Operoo).

The GDPR gives citizens *more* control over Personal Data held by organisations

The underlying aim of the regulation is to strengthen the privacy and rights of data subjects by ensuring that organisations:

- Inform what personal data is collected, and how it is used.
- Have appropriate consent to collect personal data.
- Process personal data in a lawful, fair and transparent way.
- Collect and use minimum data needed.
- Take steps to ensure data is accurate and up-to-date.
- Only keep personal data for as long as needed.
- Take reasonable measures to keep data secure.

Who does the GDPR apply to?

Data Controller

Operoo Customers act as the controller for any personal data they collect (e.g. school, club, business).

Data Processor

Operoo is the Data Processor and processes personal data on behalf of the Data Controller.

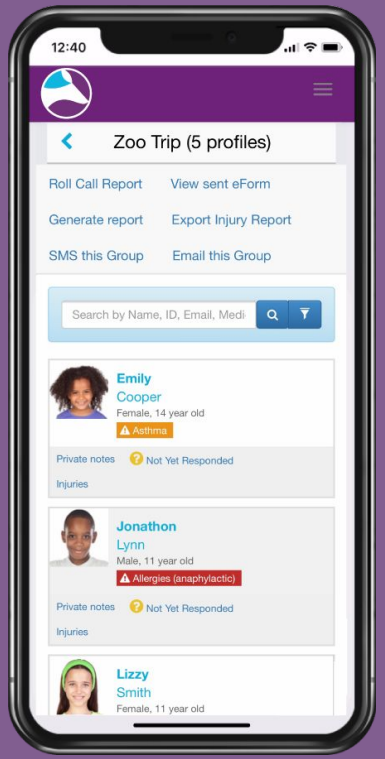
Data Subject

Individuals whose personal data Is being processed (e.g. students, parents, staff).

Why Process Personal Information in Operoo?

Schools, clubs and other groups with a duty of care are required to keep relevant personal information about the members in their charge. This includes medical conditions and consent information. Operoo helps customers:

- Eliminate the time and hassle of collecting paper forms and consent from parents or guardians.
- Keep emergency contacts, medical conditions and personalised action plans up-to-date.
- Provide Authorised Supervisors with instant access to emergency information (even offline), so they know exactly what to do, who to call, and what to tell paramedics in an emergency.



12 reasons to go paperless

Collect forms faster

Forms sent directly to parents who can respond in minutes.

Save money

Paper, toner, printers, stamps, envelopes, and distribution.

Save time

Automated reminders chase parents for missing information.

No crumpled or lost forms

Easier to read and file. Lost forms are a GDPR data breach.

No messy handwriting

More accurate information reduces chances of errors.

No manual data entry

Empower your team to do more valuable work.

No more carrying copies

Give staff instant access on mobile devices, even offline.

More secure access

Restrict access with account and password protection.

Reduce risk

Know exactly what to do and who to call in an emergency.

More useful

Log incidents, mark roll and send group messages to parents.

Remove staff access

No forms taken home by staff and no shredding paperwork.

Easier to audit

Everything is tracked and instantly available to audit.

Does my organisation need a DPIA?

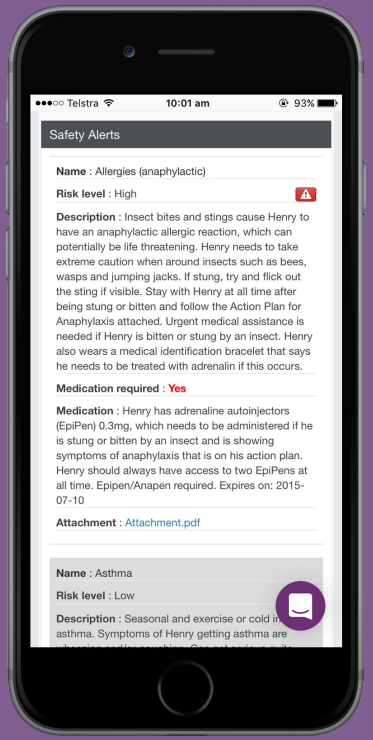
A **Data Protection Impact Assessment (DPIA)** is a privacy-related impact assessment. It's objective is to identify and analyse how data privacy might be affected by certain actions or activities.

Under the GDPR, a DPIA is required in the following cases:

- Profiling of personal information
- Systematic monitoring on a large scale
- Processing sensitive data on a large scale

Organisations use Operoo to process sensitive personal data (including health information) about Operoo Users and the people they are legally responsible for.

Therefore, **a DPIA is recommended**.



IS YOUR SCHOOL

GDPR READY?

#8 KEY QUESTIONS

To help you understand and demonstrate GDPR compliance with Operoo

1

What Personal Data may be collected?

DATA CATEGORIES

Operoo is a Data Processor that may store Personal Information, including *Special Category* Health Information, on behalf of organisations (the Data Controller). Types of information that may be stored include:

PERSONAL INFORMATION

Required to create Care Profiles and collect information which helps authorised staff identify students, and know who to call in an emergency.

- Name & Username
- Date of Birth / Age
- Personal Email
- Telephone
- Address (residential, business, postal)
- Photograph or video footage
- IP Address & Location
- Family Details (members / relationships)
- Emergency Contacts
- Responses to eForms
- Consent with Digital Signature

*User Controlled

HEALTH INFORMATION

"Special Category" data to help authorised staff know what to do in an emergency.

- Medical Conditions
- Medications
- Disabilities
- Emergency Information
- Personalised Care Instructions (including asthma and allergy Action Plans)

*User Controlled

NON-PERSONAL DATA

Required to deliver, maintain and improve services.

- Usage Data (action, page, timestamp, etc)
- Pixel Tags (to track if mail opened)
- Cookies (to provide a basic service including Live Chat & Secure Sign-In)

OTHER INFORMATION

- Information requested in eForms designed by Data Controller
- Other information added by Users
- User correspondence

Learn More: www.Operoo.com/privacy

#2

When Is Consent Recorded?

Collecting Consent

Operoo is designed for organisations to collect electronic medical and consent forms from members (or their parents if the member is under legal adult age).

When Users sign up to Operoo, they are required to consent to our Terms of Service and Privacy Policy. This is recorded.

Users are also required to give consent before sharing any information with Organisations or other Individuals. This includes providing consent for every eForm response (including Excursion Forms and the Medical Form which both require a digital signature).

#3

Does any Personal Data flow anywhere else?

The flow of personal data depends on your Operoo set-up.

If your organisation uses Operoo as a stand-alone system, then Personal Data should not flow into other systems.

Most Operoo customers use other systems that contain Member information (e.g. Management Information Systems such as SIMS). In this case, organisations can sync data from other systems into Operoo via manual bulk import, pre-built integrations (read only), or the Operoo API.

Because Operoo proactively sends Automated Reminders to confirm data is still accurate and up-to-date, many organisations use Operoo to update their Management Information Systems.

Admins can sync data from Operoo back into their other systems via bulk export, pre-built integrations (read/write), and the Operoo API.

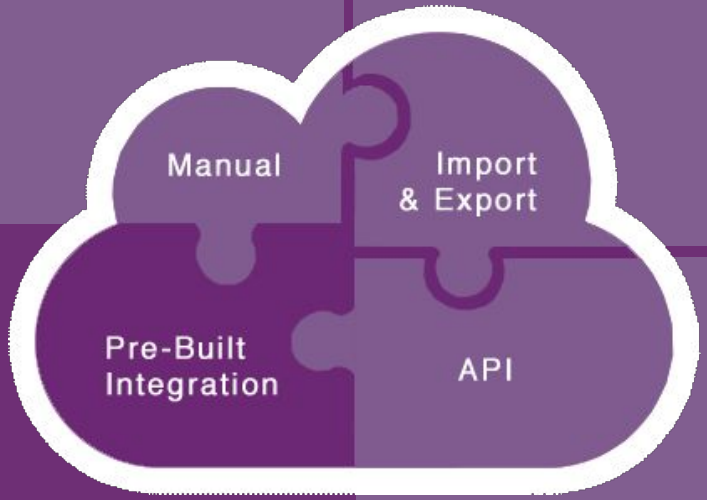
Manual Entry

Manually add the Member Name (e.g. Student, Staff), and a contact email for the person responsible for that Member.

Import & Export

Import bulk Members and Groups via a spreadsheet (duplications avoided).

Export Member profiles, injury reports, roll call data and eForm responses.



Pre-Built Integrations

Read-Only Integrations keep Operoo in sync with your administration systems.

Read/Write Integrations write back data collected by Operoo into your administration system.

Operoo API

Developers can build custom integrations to update other systems, manipulate data and functions using the Operoo API.

4

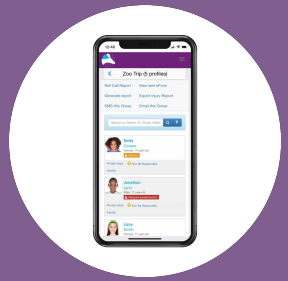
Who has access to Personal Information?

User Controlled

Operoo Users are responsible for adding, sharing and updating all personal information. Users can always see and edit which information is stored, and which organisations have access to their data. Users can revoke access (remove permission) at any time.

Operoo Admins

Admins can request Member (Operoo User) information via eForms. Access is granted if the member responds to an eForm. Admins can organise members in groups, and grant / remove Emergency Member Access to Authorised Supervisors.



Authorised Supervisors

Authorised Supervisors are granted Emergency Member Access to Member's Medical Profiles, which include Offline Access. Authorised Supervisors can also mark the roll, log notes and injuries, and send group messages.

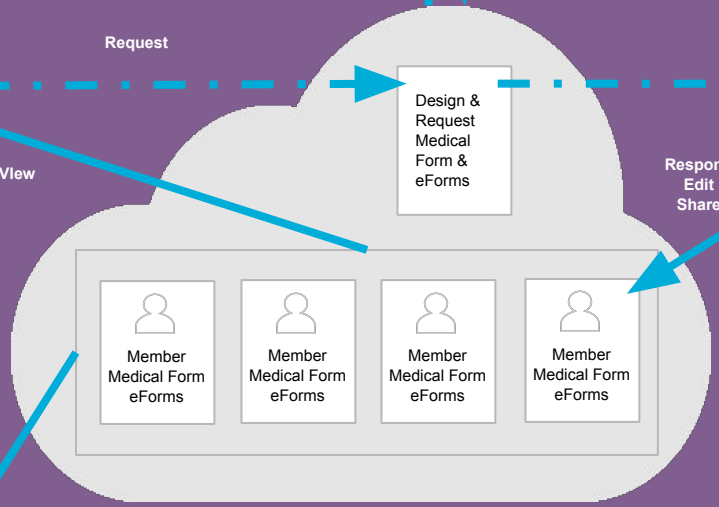
Access to Personal Information

SYNC (optional)

Sync data to your Management Admin System (e.g. SIMS) via import / export, API or Pre-Built Integration (1-way or 2-way).

ADMIN
(customer organisation)

- Invite Members
- Organise Members into Groups
- Request Medical Forms
- Design and send eForms
- Run reports
- Synchronise to other systems
- Authorise Supervisor Access



USER
(parent, staff, adult)

- Create Care Profile (Medical Form)

  May include emergency contacts, medical conditions, medications, and personalised action plans.

- Share Care Profile (Medical Form)
- Respond to eForms
- Delete Account

AUTHORISED SUPERVISOR

- Emergency Member Access
- Excursion Roll Call
- Log Notes and Injuries
- Group messaging
- Secure Offline Access

Operoo Group Edition

School Controlled Medical Data and User accounts

Student Contacts

Parent/Guardians can login to their Operoo student contact accounts to view and update the personal information in the Student Medical Record.

Parents/Guardians can also respond to eforms and can provide consent by responding to eforms.

Operoo Admins

Admins can view and update Student Medical Records as well as give parents/guardians privileges to do so. Admins will manage who has access to the personal information to any number of parents/guardians via Operoo student contact accounts. Admins can remove or grant access to any contact at any time. Admins can organise student members into groups, and grant / remove Emergency Member Access to Authorised Supervisors

Authorised Supervisors

Authorised Supervisors are granted Emergency Member Access to Student Medical Records , which include Offline Access. Authorised Supervisors can also mark the roll, log notes and injuries, and send group messages.

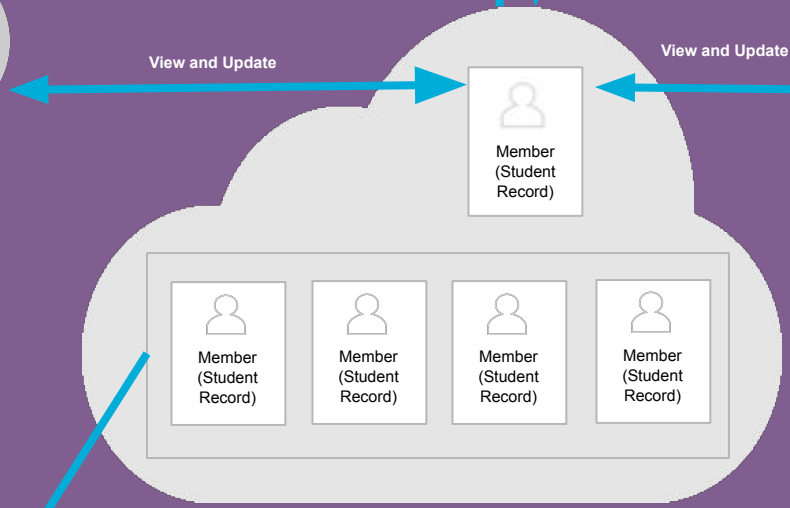
Access to Personal Information

SYNC (optional)

Sync data to your Management Admin System (e.g. SIMS) via import / export, API or Pre-Built Integration (1-way or 2-way).

ADMIN
(customer organisation)

- Create and manage Student Contact Accounts, Staff accounts and Student accounts.
- Organise student members into Groups
- Request verification for Student Record
- Design and send eForms
- Run reports
- Synchronise to other systems
- Authorise Supervisor Access



USER

Parent/Guardian

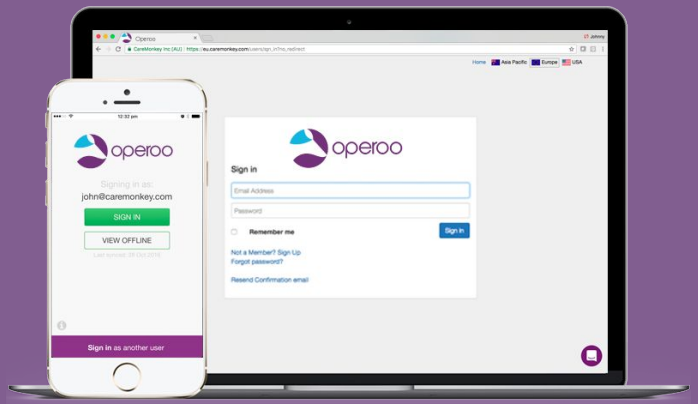
- View / Update Student Record
  May include emergency contacts, medical conditions, medications, and personalised action plans.
- Respond to eForms

AUTHORISED SUPERVISOR

- Emergency Member Access
- Excursion Roll Call
- Log Notes and Injuries
- Group messaging
- Secure Offline Access

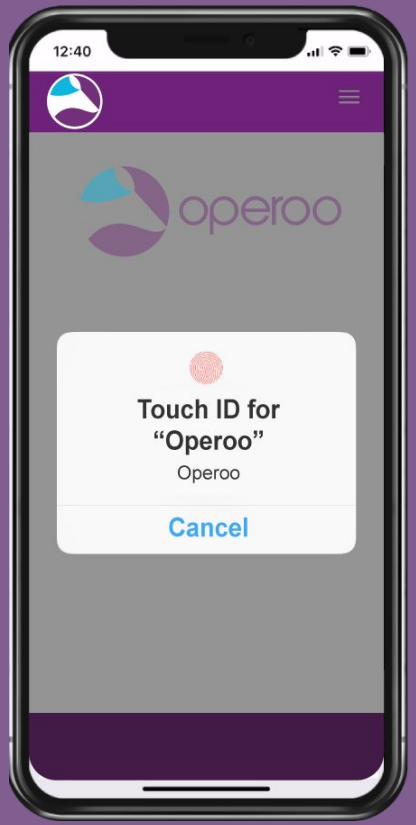
5

How does Operoo keep Personal Data secure?



Account and Password Protection

Operoo restricts access to Users with valid Operoo accounts only.
For Community Edition, users create their own Operoo accounts and give access to the organisations or individuals they choose to share information with.
For Group Edition, organisations such as schools create and manage their Operoo user accounts for parents/guardians, staff and students and can set permissions as to the type of access allowed.
Personal Data is always password protected, utilizing strong password policy and non-reversible hashing for storage of the password. Operoo will always notify Users by email when their account has been accessed from a new device.



Mobile Data Protection

Operoo is often used by Teachers and other Authorised Supervisors on Excursions to ensure they know exactly what to do, who to call, and what to tell paramedics in an emergency.

Access via the Operoo Mobile App requires an additional layer of security, requiring a Pin, Fingerprint or Facial ID.

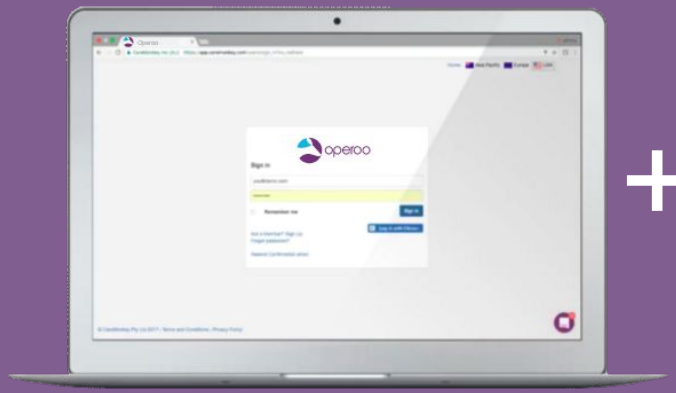
Two-Step Verification

Two-Step Verification (a.k.a Two-Factor Authentication) is an extra layer of security that helps prevent anyone who might have seen, or guessed your password, from accessing your account. When Two-Step Verification is enabled, nobody can Sign In on a new device or browser without the verification code, and the User will be notified by SMS if they try.

Two-Step Verification is an optional security layer. Operoo recommends that our customers mandate Two-Step Verification for Admin and Authorised Supervisors who may access personal data.

Sign In

new device or browser



+

SMS

verification code

Data Encryption

Operoo data is always encrypted at rest, and in transit. Security layers include strong cryptographic implementations, such as 256-bit encryption, and 128-bit data encrypted SSL systems use Advanced Encryption Standards.

Network Monitoring

Operoo's network is designed with security in mind. This includes intrusion detection, firewalls and active monitoring systems. The security sub-layer is capable of detecting anomalies within the system to proactively prevent malicious activities and alert our security staff.

Operoo regularly conducts penetration and threat modeling to ensure our network is properly secure and up-to-date.

Learn More: www.operoo.com/security-practices

Infrastructure

Operoo's physical infrastructure is hosted and managed within Amazon's secure data centers, utilizing Amazon Web Services (AWS) technology. AWS provides a highly reliable, scalable and secure infrastructure platform.

User data is stored on servers in your region, and will never be stored outside of that region. Data for EU residents is stored in Ireland (Dublin).

Mobile Data Security

The Operoo App stores data in an encrypted format to give authorised Users access to emergency information, even when offline.

All data transfer is handled over SSL secure connections. Operoo uses an "Extended Validation" SSL site certificate so Users can be sure they are talking to Operoo when accessing data.

Data that is stored on a device automatically expires and is deleted from local storage after a set period of time, unless the Authorised Supervisor re-synchronises with the server.

Data that is no longer authorised is automatically deleted from local storage.

Privacy Protection by Design and Default

Privacy Settings at highest level

By default, no other User or Organisation can see any information about Data Subjects added into Operoo by Users. Users must deliberately Share a profile (Community Edition) or submit an eForm to an organisation before that organisation can see any information.

Operoo Privacy Policy

“Operoo will NEVER share your data to anyone without your consent.”

Learn More: www.operoo.com/privacy

Citizen’s Control Personal Data

Community Edition: is designed to make Users responsible for adding, sharing and updating personal information. Users can always see and edit information that is stored. Users can see which organisations have access to their Operoo data, and revoke access (remove permission) at any time.

Group Edition: is specifically designed for schools. The medical information is stored in a Student Record. This data belongs to the school and cannot be shared with other schools, organisations using Operoo. The school determines who has access to the student record and can set permission to either “No Permission” or "View and Update" to any number of parents/guardians via student contact accounts. The school can remove or grant access to any contact at any time and give multiple contacts simultaneous access.

Data Breach

In the event of a suspected data breach, Operoo has a Critical Incident Response Team (which includes our Data Protection Officer, Developers, and Senior Management). Operoo has a Data Breach Policy Notification and Incident Response Plan in line with GDPR Articles 33 and 34.

Learn More: www.operoo.com/data-breach-policy

6

What is the data retention period?

Data Retention Schedule

Personal data should only be kept for as long as is needed, and your Education Authority will have clear guidelines on how long data should be kept.

Data Retention Guidelines may vary between countries and local authorities. However, data stored in Operoo is typically required to be kept until the pupil turns 25 years old.

Record Description	Retention Period
Attendance Registers	Date of Register + 7 years
Student Medical Record	DOB of the pupil + 25 years
Trip Records	Date of Trip + 2 years (longer if incident)
Letters Authorising Absence	Date of Absence + 2 years
Accident / Incident Reporting	DOB of the pupil + 25 years (keep all records of pupil)
Risk Assessments	7 years from completion of project, incident, event or activity

*Example Only: Please check the Data Retention Period for your organisation

#7

How is Personal Data securely deleted?

Permanently Delete Data

Operoo allows the Data Controller to archive and / or permanently delete personal data, including Member's medical profile or student record and eForm responses.

Archiving hides the information away from the Admin view (into the Operoo Archives), while Permanently Deleting Data is final, and can never be recovered.

Data should be Permanently Deleted when:

- No longer required (see your data retention schedule)
- There is a successful Request for Erasure.

Request to Erasure

The GDPR (article 17) grants Data Subjects the Right to Erasure, sometimes referred to as the “Right to be Forgotten”.

Individuals can make this request verbally or in writing, and the Data Controller has one month to respond.

If there are no grounds to refuse the request, the Data Controller must delete any personal data about the Data Subject without undue delay.

Right to Refuse

The Right to Erasure is not absolute, and only applies under certain circumstances. The Data Controller has a Right to Refuse the request when required:

- Complying with a legal obligation.
- For performance for an official authority.
- For the establishment, exercise or defense of legal claims.

It is the responsibility of the Data Controller to know how long data is required to be kept for compliance or legal reasons. If there is a reason above to refuse the request, you will need to cite a reason in your response to the Request to Erasure.

8

What Policies and Procedures are required?

Data Protection Officer (DPO)

Your organisation will need a designated DPO, who is responsible for overseeing your data protection strategy, implementation and monitoring.

Your DPO must be an expert in data protection, adequately resourced to make changes, and report to the highest management level.

Any DPO who has questions related to Operoo security should contact security@Operoo.com.

We're happy to help.

Policies and Mandatory GDPR Records

To demonstrate GDPR compliance, your DPO will need to review and update the following school policies.

The information contained in this document should help you complete and update any policies and registers related to Operoo.

- Data Protection Impact Assessment (DPIA) (Article 35)
- Data Protection Policy (Article 24)
- Privacy Notice (Article 12, 13 & 14)
- Employee Privacy Notice (Article 12, 13 & 14)
- Data Retention Policy (Article 5, 13, 17 & 30)
- Data Retention Schedule (Article 30)
- Data Subject Consent Form (Article 6, 7, & 9)
- Parental Consent Form (Article 8)
- Supplier Data Processing Agreement (Article 28, 32 & 82)
- Inventory of Processing Activities (Article 30)
- Data Breach Response and Notification Procedure (Article 4, 33 & 34)
- Data Breach Register (Article 33)
- Data Breach Notification Form to the Supervisory Authority (Article 33)
- Data Breach Notification Form to Data Subjects (Article 34)

Example DPIA

To demonstrate GDPR compliance, your organisation needs to complete a DPIA for Operoo. This should be straight-forward because all the answers are contained in this document. Your organisation should already have a DPIA template for you to work with (below is an example). Remember, you will need to complete this table for each type of Personal Data you collect in Operoo.

Description of Personal Data Collected by Organisation	What is the Data used for?	How does the school collect the Data?	When is consent recorded?	Where is the record stored?	Is the data transferred to any other systems? If yes, describe.	What is the retention period?
Medical Profile including: Emergency Contact Name and Phone Number, Student Medical Conditions, Medications, Personalised Action Plan.	Required to provide duty of care in case of an emergency. To be available at school, and taken on all excursions.	Online Form via Operoo	Consent obtained as part of the completed form (with parent signature).	Data is collected in Operoo, and synced to the school's database (e.g. SIMS).	Data originates in Operoo servers based in Ireland, and is synced to the School on-premise Database (e.g. SIMS).	This data will be retained for the student DOB of the child + 25 years.

Table continued...

Who has access to the Data?	Who is accountable for the Data?	Who is the Data shared with?	How is the Data shared?	Actions taken to mitigate security risks?	How is data securely deleted / destroyed?
Users (e.g. parents), Operoo Admins and Authorised Supervisors (e.g. Headteacher, Admin Assistant, Staff).	School Data Protection Officer	The Authorised Supervisors for excursions.	The school has the authority to grant secure online / offline access to Authorised Supervisors via the Operoo app.	E.g. Access to Operoo is password protected, with Two-Step Verification to ensure access is on an authorised device.	Access permissions removed at end of excursion. Data to be deleted at the end of retention period.

LEARN MORE

At Operoo, we have updated our Terms and Policies to reflect GDPR requirements. To read these in detail, please visit:

Our GDPR Commitment
www.operoo.com/gdpr

Terms of Service
www.operoo.com/terms-of-service

Privacy Policy
www.operoo.com/privacy

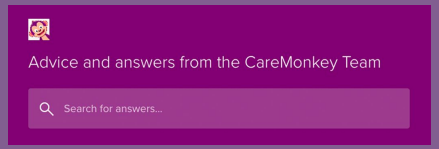
Data Breach Policy
www.operoo.com/data-breach-policy

Cookies Policy
www.operoo.com/cookies-policy

Security Practices
www.operoo.com/security-practices

Still need help?

We're here to provide you what you need via:



SUPPORT FORUM
support.operoo.com

LIVE CHAT
In-App

EMAIL
support@operoo.com

CALL SUPPORT
Australia: +61 3 8566 7727
New Zealand: +64 9 888 0592
United Kingdom: +44 808 164 1031
United States: + 1 424 219 7150

Create Any Form. Ask Any Question.

Operoo is a smarter way to collect forms, and can replace any paper form sent home to parents. Best of all, automated reminders chase up missing information so you don't have to. Check out some of the forms our customers send to make life easier for parents.

Medical Profile Form
Emergency & medical contacts, medical conditions and action plans

Camping Consent Form

Consent to play Sport

Field Trip Consent Form

Policy Agreements
e.g ICT Acceptable Usage Agreement

Media Consent Form
Permission for publication, photos, & filming students.

Collect Payments
Field trips, uniforms, enrollment, dinners, etc

Parent Teacher Interview Bookings

Student Enrollment

Questionnaires
Feedback forms, surveys, quiz, etc.

Student Absentee Form

Request Volunteers
Confirm have valid working with children background checks.

Eliminate staff paperwork too

Operoo gives staff everything they need at their fingertips, including self-service forms with approval workflows.

Field Trip Approval Form

Submit excursion request forms to be approved or rejected.

Employee Onboarding

Contact information, teacher registration, tax file number, bank account details, superannuation, first aid training, etc

Staff Policy Agreements

e.g Visitor handling, acceptable behaviour, password management

Background Checks

Working With Children checks, DBS checks, screening checks.

Leave Request Forms

Vacation, Sick Leave, Carers Leave, etc.

Professional Development Requests

Staff training, conferences, networking events, etc

Injury / Incident Reports

Log incidents as they happen.

Private Notes

Add notes with attachments about students

Private Notes

Disciplinary Reports

Keep notes of which students misbehave and issue detention.

Staff Training Quiz

Quiz staff on school policies to be sure they understand.

Equipment Purchase Request

Request approval for sports equipment, books, devices, etc.

Expense Claim Form

Submit work expense with photo of receipt.

operoo

Consent Forms
Medical Records
Online Payments
Incident Reporting
Mobile Offline Access
Field Trip Management
Staff Forms and Approvals

www.operoo.com