Kidwizz

Data Protection and GDPR

Contents Page

PAGE 3: INTRODUCTION DATA ACCESS POLICY

PAGE 4 TO 5: DATA ACCESS POLICY, KEY SYSTEM SPECIFICATIONS, DATA STORED, DATA UPLOAD PROCESS and PARENT DATA REMOVAL

PAGE 6: DATA RETENTION AND DESTRUCTION POLICY, PUSH NOTIFICATIONS and SOFTWARE RENEWAL POLICY

PAGE 7: SECURITY AUDITING and USEFUL INFORMATION

1. Introduction

Start Up Company - Kidwizz ltd

Kidwizz complies fully with all the corresponding Local Authority Security Standards.

Developed with schools and parents - Kidwizz has been created by team with over 10 years experience working within schools. It has been designed according to schools and parent/carers needs. We believe we have the strongest knowledge in the industry with regards to, how a school runs on a day to day basis. Our app provides solutions in a wide variety of sectors for both schools and parents.

Privacy by design - Kidwizz is externally hosted and accessed via a secure internet connection. Kidwizz is delivered using a secure servers operating encryption. We protect data by using encrypting data as it passes between the user and Kidwizz. Kidwizz has a rigorous security protocols that restricts access to the logged in area meaning access is only possible by authorised personnel, via a User Name and Password. Schools and Parent/carers access to Kidwizz is only possible via encrypted data connections. We may require school firewalls to be updated to permit this. Please contact your Kidwizz account manager if there are any issues accessing any of the Kidwizz services.

Compliant - Kidwizz is registered under the Data Protection Act 1998 (Registration Number: ZA612764)'

Data Protection is central to all our operations, and we ensure that all our procedures are robust and comprehensive.

For example,

ALL data stored on the Kidwizz database is encrypted and NOT stored in a raw visible format. Strict adherences to the General Data Protection Regulations (GDPR) principles are in place across all of our business operations.

2. Data Access Policy

Kidwizz Employees - General

To maintain a consistent approach, employees are given appropriate access rights based upon their operational requirements.

Three levels of access rights are used:
Level 1: required for general operational use
Level 2: level for escalation
Level 3: level which has full access to the entire database

- All user access is comprehensively logged
- Each user is issued with their own back office and system User ID with appropriate strong passwords
- Employees use these identities and passwords in keeping with security best practice (for example, sharing of passwords is not permitted)
- Similarly, each uses a secure login and password for Kidwizz internal systems and network
- Employees are educated on matters of security and integrity, and the confidentiality of information
- User IDs and passwords are disabled upon any employee leaving the company
- Employees access levels are reviewed on a regularly basis to be appropriate to their role
- Any paper-based sensitive information is disposed of through onsite shredding
- All Laptops and mobile devices used by members of staff use disc/data encryption and have remote wipe facilities enabled where present.
- Any Kidwizz staff accessing the system from outside of the known network are required will be logged at all times.

Kidwizz Employees - Payments

Payment processing and back office in Kidwizz is operated and accessed using a separate distinct web interface that separates access to our data stored. Kidwizz uses Stripe as a payment provider.

School Users

- As part of the setup process, the system creates a secure password for the main admin office. The school is responsible for managing this username and password.
- School users are shown how login in and out and are then responsible for managing the security of that account internally.
- These school user accounts are controlled via the Kidwizz user account settings section. Schools can set their own internal levels of permissions.
- Users are required to change their passwords regularly, and are reminded to use one that is secure. For example using your first name or DOB is not secure.

- Gaining support requires users to pass security screening when making enquiries to the Kidwizz Helpdesk – This ensures that information is only passed to appropriate parties.
- School Administrators are responsible to change password when a removing any staff leavers.

3. Key System Specifications

- Cloud based system that scales ahead of, or with demand
- Secure web based user interface
- Responsive design that scales to the size of the device being used to access
- Free iOS and Android app for parents
- The software is written using a mixture of scalable software technologies

4. Data Stored

Kidwizz maintains a database containing the following data:

Student data	Parent Data	Staff data	Photos and Videos subjected to your school only	Catering data	Payment data

5. Data Upload Process

School held parent/pupil data is uploaded through a CSV file exported via your schools MIS system. Schools can upload or request Kidwizz to upload a CSV to the Admin Dashboard. We will require you to notify us when there are new starters or leavers (parents, staff and children) to update changes. Data will be removed and disposed of by emailing Kidwizz. This request will only be accepted when the main school user sends a written request via email or letter. All changes made via Kidwizz are through CSV files only. We recommend sending this to us via a secure system such as Egress For example: changes to personal address data, changes to leavers or new starters etc.

6. Parent data removal

Should it be required, parent contact details can easily be removed from the Kidwizz platform by emailing your account manager. Schools will be provided with training on how to internally manage this process too.

7. Data retention and Destruction Policy

Kidwizz is committed to the protection of data held whilst customers are accessing the system. All data held in the Kidwizz database is encrypted and not stored in plain text. All communication between the user (school and Parent) and the Kidwizz service is encrypted.

In the event that a customer cancels their agreement, access to their school setup is disabled on contract expiry or on the date requested by the customer. When an account is disabled this means, the account is locked, not accessible and all personal data relating to Parents and pupil will be removed after a 7-day period as will all sent messages/forms etc.

The Company will retain all transactional information for a period of at least 6 years as required by law. This retention period is for the use of the relevant authorities.

8. Push Notifications

School users with appropriate permissions are able to send push notifications. Notifications are sent to parents when a new product is set up by the school user. School users can also send a message to define groups such as whole school, year groups or class group.

9. Software Renewal Policy

Kidwizz utilises different software applications to deliver our online services. In the event that a new version of core software is released, for security, stability or performance reasons, we carry out thorough research and testing to determine if any of the updates could impact any of the components/functions that we use.

Should we highlight any changes that impact security and could impact our services, we aim to have the software updated as soon as possible. As we use managed servers, these updates are carried out by our hosting company and are normally within a 24 hours.

If we highlight any changes that are feature based, that do not affect the day to day running of the system, we will seek to roll these updates out at the next development cycle for web updates. These normally occur during school holidays to reduce impact on the end user.

Hardware updates take the form of total hardware swap out with new equipment minimising the risk of downtime.

10. Security Auditing

Security of personal data is of paramount importance to Kidwizz operations. To ensure our services are as secure as possible we conduct monthly network/server penetration testing of all our systems.

11. Useful Information

Kidwizz Ltd

3rd Floor 207 Regent Street London W1B 3HH

Email: hello@kidwizz.com Website: www.kidwizz.com

Data Protection Registration Number – ZA612764 Company Registration Number – 12052943