ParentMail Data protection and GDPR

123Comms Limited, Trading as ParentMail, is a wholly owned subsidiary of IRIS Software Group

Please refer to www.iris.co.uk

V 1.6 June 2018

Contents

1. Introduction

Widely used - ParentMail is currently used by over 5000 school in over 120 Local Authorities and comply fully with all the corresponding Local Authority Security Standards.

Developed with schools - ParentMail has been developed by us in partnership with school staff and leading education professionals. We are an organisation with a strong background in the development and application of software and communications technology to provide solutions in a wide variety of sectors.

MIS integrated - ParentMail is an official technical partner of Capita, the operators of the predominant school administration system Capita Sims. Our relationship with Capita ensures that the ParentMail system is, and will remain, fully compatible with Sims. ParentMail has similar relationships with, and is also fully compatible with, Progresso (Advanced Learning), Scholarpak, CMIS, and all other major MIS and registration systems.

Privacy by design - ParentMail is externally hosted and accessed via secure internet connections. ParentMail is delivered using secure servers operating Secure Sockets Layer (SSL) encryption, using SSL protects data by using Transport Layer Security that encrypts data as it passes between the user and ParentMail. ParentMail also incorporates 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. School and Parent access to ParentMail is only possible via encrypted data connections and access may be require school firewalls to be updated to permit this. Please contact ParentMail support if there are any issues accessing the ParentMail service.

Compliant - ParentMail is registered under the Data Protection Act 1998 (Registration Number: Z8936949) and is also PCI DSS registered for payment card processing, see the following link to validate https://sealserver.trustwave.com/
Data Protection is central to all our operations, and we ensure that all our procedures are robust and comprehensive. For example,
ALL data stored in the ParentMail database is encrypted and NOT stored in a raw visible format.
Strict adherence to the General Data Protection (GDPR) principles are in place across all of our business operations.

Accountable – IRIS Software Groups named Data Protection Officer is Vincenzo Ardilio.

The following guide will answer more specific data protection queries but if you have any additional questions please email them to dataprotection@123comms.com

2. Data Access Policy

Due to changes in legislation made September 2012 at the DBS (Disclosure and Barring Service), ParentMail's business activities no longer meet the revised criteria for regulated activity with regard to access to school data and contact with children & young people.

Details of these changes to the guidelines are available to view at
http://www.gov.uk/government/uploads

However, field-based roles that involve regular visits to schools still qualify for a DBS check and are carried out where applicable.

ParentMail users are divided into two groups, ParentMail Employees and School Users

ParentMail 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 –

Basic level required for general operational use

Intermediate level for escalation

Administrator 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 (sharing of passwords is not permitted for example)
- Similarly, each uses a secure login and password for the ParentMail 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 ParentMail staff accessing the system from outside of the known network are required to pass through two factor authentication (2FA) in order to access the system.

ParentMail Employees - Payments

Payment processing and back office in ParentMail is operated and accessed using a separate distinct web interface that separates access from the communication system. Access to this system is restricted to the payments and escalation/resolution team.

School Users

- As part of the setup process, the system creates a secure password-based user account with unique one-time use registration code
- School users are shown how to create new users as part of the system training and are then responsible for creating and managing their own accounts
- These school user accounts are controlled via the ParentMail user account settings section where schools can choose the areas of the system users have permission to access.
- Users are required to change their passwords regularly, and are reminded to use one that is secure

- Gaining support requires users to pass security screening when making enquiries to the ParentMail Helpdesk – ensuring that information is only passed to appropriate parties
- School Administrators are responsible for the removal of user accounts after staff leave the school.

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
- Able to import data from the schools' Sims or other Management Information database in a secure/encrypted manner.

4. Data stored

ParentMail maintains a database containing the following data:

Student data	Parent Data	Staff data	Catering data	Payment data
Forename Surname UPN (Reference) Year Group Registration Group Gender DOB	Relationship Title Forename Surname Gender* DOB* Email Mobile Address	Title Forename Surname Gender* DOB Email Mobile	Meal purchased Cost Nutritional information Date of purchase FSM entitlement	Amount paid Item purchased Purchase method Sale or Refund Order number Purchaser ID

*Note; These items are scheduled to be removed from our database as there is no longer a reason for us to hold them. This document will be updated once this removal occurs.

The ParentMail system is hosted in a tier 4 data centre located in the UK

5. Data Upload Process

School held parent/pupil data can be uploaded from the school's Management Information System either automatically each night, or manually by a school user depending on the school's requirements. To achieve this data extraction ParentMail uses an in house developed server side piece of software. This data extraction software performs the following tasks;

- Gathers only data required to operate ParentMail from the school MIS system
- Extracted data is then encrypted prior to transmission to the ParentMail system
- Data transmission takes place once both ends of the service (School and ParentMail) have confirmed their identity by sharing login credentials and a unique API key
- Data is then transmitted in an encrypted form

- Once received the data is unencrypted and validated for structure and school ID
- Once validated as the data is queued for import and imported
- Should there be any parental contact changes these are presented to the parent to confirm their acceptance of rejection.

6. Parent data removal

Should it be required, Parent contact details can easily be removed from the ParentMail system via the ParentMail user interface on either the school or parent account.

However, to stop the re-import of contact information the automatic data import function needs to be updated to not re-import parent details into ParentMail. As the Data controller it is the responsibility of the School to manage this process.

For SIMs schools changing the contact priority status to type 9 will ensure that the data is not extracted and subsequently imported into ParentMail.

For other MIS systems please contact the provider directly for their solutions.

7. Data retention and Destruction Policy

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

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, at this point the school account is disabled. This means that 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.

The school is responsible for also responsible for;

- *Disabling and deleting any active ParentMail data extraction software that is running on the MIS system.*
- *Downloading a copy of the full transactional payment history for their records as this will no longer be accessible once the account is closed.*

8. SMS Message Sending Process

School users with appropriate permissions are able to request messages are sent via the ParentMail system. To achieve this the school user selects the pupils/staff they wish to receive the message from the contact book displayed within ParentMail. The message content is then typed into the message sending screen on ParentMail.

At the requested time the message is queued for delivery, here the mobile numbers of parents associated with the chosen pupils are pulled from the database and unencrypted. A list of numbers

to receive the SMS is then sent with the message content to our SMS service provider O2 who send the content to each of the numbers provided.

Our SMS provider then provides a Message ID for each of the messages sent which is later used to track delivery status of each SMS message.

9. Software Renewal Policy

ParentMail utilises different software applications to deliver our online services. In the event that new versions of core software are 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 comprise 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, normally within a 24 hour turn around.

If we highlight any changes that are feature based, that do not affect the day to day running of the system, and we look 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 ParentMail's operations. To ensure our services are as secure as possible we conduct monthly network/server penetration testing of all our systems, these tests are carried out TrustWave our PCI DSS certification partner.

Useful Information;

ParentMail is a trading name of 123Comms Limited

Head office;

Litton House, Saville Road, Peterborough, PE3 7PR

Registered office, IRIS Software Group Limited;

Riding Court House, Datchet, Berkshire SL3 9JT

Data Protection Registration Number – Z8936949
Company Registration Number – 04336436

If you have a more in-depth query that relates to Data Protection, please e-mail our Data Protection Officer at dataprotection@123comms.com