

## **Data Protection**

ParentPay provides online payments, income management and dinner money administration software to schools and local authorities across the UK and to universities globally.

ParentPay has its own Data Protection Act registration and is registered as a Data Processor. ParentPay takes data protection very seriously, indeed Director and Founder, Lynne Taylor, has done extensive work on data protection in schools and has provided consultancy on the issue to schools and LEAs.

The school (and the local authority) will already be registered as a Data Controller. ParentPay provides the software application for the school but does not access or use the data – hence the DPA registration as a data processor. The school is still responsible for managing, maintaining, updating and accessing the data.

ParentPay's commitment to the school to act responsibly as a data processor is covered in the terms and conditions agreed to by the school as part of the set up and application process and is covered in our data protection and privacy policy, see extracts below.

As ParentPay does not access or use the parent/pupil data, then the school is fully able to use ParentPay software without the need to change its DP statement as the purpose for which the data is being used by the school (i.e. the administration of the pupil) has not changed.

The scenario is no different from the school using the Capita SIMS .Net MIS software to manage pupil data, their financial management software, which contains some pupil and payer data, or any other application the school will already be using to administer the pupils while at the school.

If parents decide not to activate their account, or make payments online, that is entirely their decision.

Even data entered by parents when using the online payment system, is NOT owned, used or accessed by ParentPay. We do not own the data entered in the system and will never sell the data, market to the parents or pass the data to third parties. All personal data remains under the full control of the school. For information related to payment card data, see the section below.

These issues have been fully investigated by other local authorities, some of which include Somerset County Council, Cornwall, Staffordshire, Nottinghamshire, Warwickshire, East Riding of Yorkshire, Hertfordshire, London Boroughs of Croydon, Bromley, Sutton, Enfield, Hammersmith and Fulham.

ParentPay is currently used in over 110 different local authorities across the UK. In each and every case, it was agreed that as ParentPay never uses the data in the system and does not access the school's data, then the solution could be launched without parental consent prior to launch – the school remains in control of ALL data used in the ParentPay software.

Croydon Borough Council's Director of Children's Services previously commissioned a complete and thorough independent audit of the entire system, the company and all security, data protection and processes. This audit was conducted by international consultancy firm Deloitte Touche, who gave a positive reference and full support for ParentPay.

ParentPay have also worked on national projects with Becta, the government's lead partner agency responsible for the strategic development and delivery of the government's e-strategy in schools, and provided guidance and advice to the DCSF related to efficiency in school administration.

ParentPay also supplies software solutions to the world's largest foreign exchange company, Travelex, providing international payment solutions for students at Universities in countries around the world.

## **ParentPay Security**

The ParentPay web site is hosted in a secure data-centre which is certified to ISO 27001, the International Standard for Information Security Management. This accreditation is very difficult to achieve and as such provides a high level of certainty and confidence in the resilience, availability and security of the solution.

ISO 27001 is designed to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties.

Administrative access to the website is only possible with two factor authentication (password and certificate) and through encrypted data traffic (VPN).

User web access to the online service is only allowed through 128-bit encrypted HTTPS; the SSL certificate is issued and signed by Verisign.

Usernames and passwords are randomly generated for initial account activation and parents are made to change their password on first login.

Changed passwords are treated as Personal Data under the Data Protection Act and are encrypted in the database. They cannot be viewed by schools or by ParentPay, or recovered from the software – only reset.

No data is ever moved or copied onto, or transported on external disc or other unencrypted media by ParentPay. Data displayed to the parents in their online accounts comes from the schools own MIS systems and is transmitted over a secure encrypted link.

## **Payment Security**

All card transactions are processed through a PCI DSS Level 1 certified payment gateway into the card scheme networks. The Payment Card Industry Data Security Standard is the international standard for card transaction security and ensures that all transactions are processed with the reliability and security expected and fully compliant with all bank and card scheme regulations and requirements.

NO payment card data (card numbers, expiry dates, issue numbers or card security codes) is ever held or maintained within the ParentPay application. ParentPay does not store this data nor can ParentPay or the school ever access this data in ParentPay.

Users are asked to input these for each transaction and only transaction identifiers are stored in the database, which allow for the tracking and auditability of the system, with complete card data integrity being maintained.

All communication within the payment system is strongly encrypted using 2048-bit Public/Private Key encryption with variable 168-bit session keys. This is many more times secure than standard browser SSL security.

## **Data Protection and Privacy Statement Extracts**

### **Privacy Statement**

The [www.parentpay.com](http://www.parentpay.com) and [www.pay24-7.com](http://www.pay24-7.com) websites are owned by ParentPay Limited. ParentPay regards users privacy as important and any personal information given to us will be used in accordance with the UK Data Protection Act of 1998. ParentPay does not store any personal information about individuals who visit this site except where they provide contact information or use one of our online services. Any information provided will only be used for the reasons specified, and it will not be shared with any third party without the users consent, unless required by law.

### **Purpose of Data and Third Party Disclosure**

ParentPay do NOT use personal information for marketing purposes.

ParentPay will retain user information for as long as necessary to fulfil the purpose(s) above, and in accordance with the law.

ParentPay will only disclose user information to other third parties in the following limited circumstances:

- where it is required to do so in order to deliver the service applied for, e.g. to an acquiring bank or card scheme for credit/debit card processing or to another financial institution for the processing or settlement of other payment transactions and instructions.
- where we are legally obliged to do so, e.g. to law enforcement and regulatory authorities
- where there is a duty to disclose in the public interest
- where disclosure is necessary to protect our interest e.g. to prevent or detect crime and fraud
- where you give us permission to do so e.g. on an application form

ParentPay use reputable agents (data processors) to fulfil services on their behalf, e.g. payment service providers and acquiring banks for the authorisation and settlement of credit and debit card transactions. ParentPay will provide information to those agents specifically for use in connection with those services.

The information that ParentPay provide to them will be protected by a confidentiality agreement and will be used solely for the purpose of fulfilling the service. These agents are required to process the information in accordance with the Data Protection Act and ParentPay's specific instructions.