



## ParentPay Security: An Overview

Privacy - Integrity - Availability

### Data Transmission

#### *Web Users*

The use of any web application – including ParentPay – requires data travelling between a local computer and a web server.

For users of ParentPay, all data that travels between the web server and the client browser, is always encrypted at the highest level in practice today. ParentPay chose Verisign as their Certificate authority. This SSL certificate enables 128 Bit symmetric encryption with 1024 Bit asymmetric encryption for key exchanges.

Broken or misconfigured browsers which do not support SSL will be refused by ParentPay.

#### *Administration*

The web server farm is hosted by the well known and trustworthy organisation NTT/Verio in London. Apart from normal web access, administrators are allowed to access the machines for maintenance work.

If administrators work over the network, they may always and only access any ParentPay server in an encrypted and strongly authenticated manner (VPN: virtual private network).

This assures that any data that travels over the network between the ParentPay servers and any client cannot be introspected or tampered by a third party.

### Data Storage

#### *Persistent data*

The ParentPay web application uses an SQL database to store data permanently. The data is backed up nightly and a redo log is maintained to recover from any disaster, however unlikely such an event may be.

#### *Intermediate storage*

Commonly when browsers access the Internet through a proxy server (web cache) the proxy stores (caches) each and every page, which has been accessed by the browser. In the case of ParentPay the cache cannot store the pages for two reasons:

- 1) The NoCache property is set for all pages in ParentPay since they may display sensitive information. Caches interpret this property and therefore do not save such pages.
- 2) The pages are encrypted and even if the cache did store the page into a file nobody could read it.



## ***Passwords***

All passwords in ParentPay are stored in an encrypted way in the database. Therefore passwords are unreadable even for database administrators.

The exception to this rule are those passwords which have been set up automatically and whose users have not yet logged in. In such cases passwords may be stored unencrypted. As soon as the user logs in they will be forced to change the password thus saving an encrypted version.

There are two alternative ways of encryption. One of it is by symmetric key. This method has the advantage that passwords can be emailed to users.

The other way of encryption is as hashes. Hashed passwords are never recoverable; they can only be reset.

## ***Cookies***

Cookies are employed by ParentPay for the sole purpose of tracking browser sessions. Cookies are not used to encapsulate user information. Cookies are valid only for ParentPay itself and not sent to other servers. Conformant browsers delete any locally stored cookies after the idle timeout which may vary between 30 and 60 minutes.

## **Service Availability**

### ***Hardware***

ParentPay has made great efforts to deploy its software on resilient hardware. Critical parts like hard drives have been laid out redundantly in RAID arrays for fail-proofness.

Most of our server farm is laid out in an n+1 manner i.e. We always have one machine more than the minimum required. Thus being able to compensate a complete outage of any one machine at any time.

### ***Monitoring***

All hardware is constantly monitored electronically by our hosting provider to recognise failure conditions early and to enable precautionary replacement of parts under controlled conditions through the NTT/Verio staff.

Equally the critical software components are constantly monitored for availability and freedom of error.

### ***Network***

The network connectivity of the ParentPay servers is guaranteed by our hosting provider NTT/Verio. All the network equipment of NTT/Verio is laid out in n+1 manner. The network is connected to several internet backbones with automatic failover.



## ***Network Security***

The ParentPay server farm is protected by a sophisticated security environment involving but not limited to:

- 1) Stateful packet inspection firewall (transport and internet layer) disallowing any direct network access to the backend computing environment.
- 2) Application layer filtering.
- 3) Virus screening

## ***Further information***

Further information may be obtained from the ParentPay technical team. Please email [webmaster@parentpay.com](mailto:webmaster@parentpay.com)