

# Data Handling Policy

## **General Data**

Our promise to you is that the information you give us is treated in total confidence and stored in full accordance with the new General Data Protection Regulation (GDPR) which will come into power from the 25<sup>th</sup> May 2018. . It is kept only so we can provide you with the information and services that best match your requirements and preferences. We may conduct data analysis and market research, but we will never sell or pass on your details to any third party for marketing purposes.

## **Online data**

ChildsPlay does not collect any personal information from visitors to its website other than information that is knowingly and voluntarily given. This personal data is stored in-house on our computer systems to enable us to respond to your requests. Anonymous information is collected, such as the number of visitors to the website in a given period, but it is purely statistical and cannot be used to identify an individual user.

ChildsPlay will always endeavour to protect your data from loss, misuse, unauthorized access or disclosure, alteration or destruction. We fully understand the concerns people may have about releasing personal details over the internet. We are committed to investing in technology to provide high security for your information through versign certificates that encrypt all data held on our web sites

## **Customers own data**

ChildsPlay ensures that all data supplied to us for the purpose of support and training will at all times be controlled and protected. The data will at not anytime ever leave us or go off site without customer approval. We endeavor to protect third party data by always uploading and downloading from our secure web site and not through attached emails unless encrypted.

We will always only keep data for the purpose of its intended use i.e. support, by which time we will delete all data supplied. No data is held more than 48 hours.

Customers data that's excepted as critical will be held in an our over night safe if required.

## **Hosted customers data**

All our Customers with hosted ChildsPlay's are on servers, not in our building they are in highly secure buildings in the UK that have 24x7x365 day manned with security staff that work to SIA certification. The buildings meet ISO standards such as ISO 27001 for data centres. They have 24x7x365 day monitoring. With FM200 fires suppression systems in place, with very early smoke detectors by Vesda. Plus UPS and power generators to maintain connectivity 24x7x365 days.

The servers we use are configured to our requirements and only we can access them, no person in the data centres can access our servers. The server IP address are only supplied to our customers that use our servers. With the IP we use Remote Desktop Connections (RDC) to allow our customers access our servers. These Remote Desktop sessions operate over an encrypted channel, preventing anyone from viewing your session by listening on the network giving you

extra protection. These servers have been set to only allow three attempts then they will also reset if left idle for more than 15 mins. Only key staff can change your settings and we will not give any of your staff details or passwords over the phone. We will only allow such information to be sent to you via an email. Please also note it is the responsibility of our clients to ensure the usernames and passwords issued to them are securely used and not passed to any third parties.

ChildsPlay Backups. ChildsPlay creates backups every time it closes, these are then stored on our servers ( backups that are on our servers will be deleted when they are over 6 months old) but it is the responsibility of the customer to download backups to their local computer.

### **Customer data option**

With ChildsPlay you can if you wish send us anonymous data. This is data that has child, parent and address info set to be anonymous, so we only know the child codes not their names etc. when handling your data.

### **Data Records**

We maintain a full list of customers who have access to their hosted data. Which is updated on a very frequent bases. These records are essential for maintaining who has access but also in the event of any kind of disaster. Be it at a customer location or the companies location. We must work towards providing our customers the infrastructure to continue trading no matter what the reason for the disaster. These plans are part of our Company Disaster Recovery Plan Policy.

I hope this help you. If you have any other questions regarding this please email me [ian@childsplaysoftware.co.uk](mailto:ian@childsplaysoftware.co.uk).

Last updated 2/1/2018