Security Policy

We are committed to ensuring that your information is secure. In order to prevent unauthorised access or disclosure, we have put in place suitable physical, electronic and managerial procedures to safeguard and secure the information we collect online. We backup records remotely on secure servers which are managed by us and our service providers in the UK. Personal information that we store or transmit is protected by security and access controls, including username and password authentication, two-factor authentication, and data encryption where appropriate. In relation to online transactions, we partner with quality payment processing providers who implement the highest standards in encryption and data security.

Smart Club Backup & Security

Many of our clubs avail of our secure Online Backup solution. Under this arrangement all of a club's data is backed up securely once every 24 hours to a secure server located in England. We will only request access to this data upon request by the club and this is only likely to happen in the case of any emergency where there is a risk of loss of data on the club's local server.

All communications between Smart Backup Server and your local Server are transported in a 128-bit SSL (Secure Socket Layer) channel. Although all your backup files travel through a public network (internet), potential eavesdroppers have no knowledge of what has been exchanged.

All of your files are first zipped and encrypted with your defined encrypting key before they are sent to Smart Backup server. To everyone but you, your files stored on Smart backup server are no more than random files with random content.

The encrypting key used to encrypt your files resides only on your computer and is known only to Smart Club Solutions, although we can provide this to you if necessary. Currently, the algorithm that we are using to encrypt your files is Advanced Encryption Standard (AES), with 256-bit block ciphers.

Smart Club Cloud Summary

Our Smart Club Cloud enables members to carry out a range of secure financial transactions online. Such transactions are processed by other reputable third party payment processors, so the only sensitive member information actually held in our Cloud is the following: Firstname, Surname, Date of Birth and Email. This information is required to assist login verification and to match transactions with the relevant member in the club database. No bank account or card details are stored in the Cloud. Indeed, such information is only entered and live for the period of the transaction by the payment processor. Our Cloud database is hosted in AWS and has firewall rules that only allow access from our office IP address and the AWS server which hosts the Cloud site and API. All web communication is over https and SQL server communication is done on an encrypted pipe. Personal data is passed to third parties for certain integrations. AWS backs up the Cloud database on a daily basis.

No card details are transported across the web from our server to the payment provider. Instead, we use tokenization which is the process whereby we collect sensitive card or bank account details, or personally identifiable information (PII), directly from our members in a secure manner. We use a client side process executed on the user's machine to perform this process. This ensures that no sensitive card data touches our server, and allows our integration to operate in a PCI-compliant way.

Smart Club Cloud is secured using a 256bit SSL Certificate issued by Certificate Authority (CA) Lets Encrypt. Part of Lets Encrypt's security policy is the need to renew your certificate every 90 days. This limits potential damage from key compromise and mis-issuance.

Smart Club Cloud Security

The SmartClubCloud is a '*Web Application*' which is a web based application hosted and accessed via the internet by users in different locations. Each user is assigned their own '*Session*' during which their information is kept separate from other user sessions. This is how each user does not see each other's information.

The SmartClubCloud uses 2 databases :

Database 1 is the database held on our server to hold usernames and passwords of registered members and is used to authenticate member login requests. Accounts are locked and need to be unlocked by the club after 10 failed login attempts.

Database 2 is the database located within the club itself and is only ever accessed if the member login attempt is successful. The information accessed here is specific to the logged in member only. If the member is paying online for an invoice or topping up their purse, then the SmartClubCloud will access the clubs Payment Processor details to process the funds from the member to the club account. This information is used only for the lifetime of the transaction while the Processor processes the payment. Username and secret are 'Hashed' using a 128 bit encryption algorithm to ensure it is unreadable to the human eye should it be intercepted. This ensures total security.
The only information stored on Database 1 used by Smart Club Cloud are the club name and ID and the member ID together with the members first name, second name and Email address for login and password authentication purposes.

This is by careful design to ensure the members information is not stored in 2 places, namely the club database and the online database used by the Smart Club Cloud. This not only improves security but improves speed and performance by scaling down the amount of space required on our online server as the majority of space is already catered for to hold the members information on the actual club server itself.

When the member logs into the Smart Club Cloud, the application determines firstly if their username and password match the credentials in the '*Online Membership Credentials*' database.

On a successful login, the members details are fetched from the clubs database and stored in the members online '*Session*' as described above. The information in this '*Session*' is only available to the browser on the user's machine for the lifetime of the session.

Sessions are limited to 20 minutes of inactivity unless the member logs out before that time to end their online session, which then disposes of the data held in that session.

Extra Reassurance!

- Member addresses are NOT STORED in the Smart Club Cloud
- Member bank details are NOT STORED in the Smart Club Cloud
- Member bank details are NOT STORED nor ACCESSED in the Smart Club Cloud
- Family member details of members are NOT STORED in the Smart Club Cloud
- Payment Processor username and secret are NOT STORED in the Smart Club Cloud
- With the exception of the club name, all other club details are NOT STORED in the Smart Club Cloud

All payments processing is transferred to our payment processor to be handled entirely through their secure SSL web service and full encryption takes place to securely complete all transactions before the user is returned to their page on the Smart Club Cloud web site.

How does the Smart Club Cloud access the database in my club?

In order for the Smart Club Cloud to pull information from the club database, there are a few things need to be configured initially:

- The club MUST have a static IP address
- The club router must be set up to accept incoming traffic requests from the internet to access the SQL server database.

For this to happen we need to open some ports. The first is port 80 to allow incoming connections from the internet (Smart Club Cloud) and the second is the port which SQL server uses to house the club membership database used by the Smart Club Cloud.

This is where a lot of users ask about the security risk of opening their router to accept internet traffic. There are indeed *potential* scenarios where a would-be hacker could access your router or network so we make some configuration settings to your router, firewall and the SQL server where the database resides. These settings are discussed below.

Smart Club Cloud: Protecting your network

The following steps are taken to prevent potential hackers from gaining access to your router settings and any machines connected to your network.

We turn off router remote access / management

Some routers have this feature built in, others do not. For those routers which have the feature we will disable it. This prevents anyone who does an IP scan on port 80 from entering your IP address and viewing your router login screen.

We request that you change your router username and password

As an extra precaution it is highly advisable to change the username and the password to the router. Routers come with a standard username and password for quick first time setup and the details are normally something like *'Admin'*, *'Admin'*.
With router remote management disabled, you cannot get access to the router logon screen but again this is for extra added security.

We change the default port of SQL Server

The standard port used by SQL Server is 1433. It is very easy for a potential hacker to do an IP scan for all IP addresses with port 1433 open. The hacker would then perform a *'BruteForce'* attack to try a combination of passwords and usernames once they find an IP with port 1433 open.
We will change the port of SQL server on installation to a port of our choice which has no standard application attached to it. This way, should a hacker stumble across your IP address in a scan and if they see port open then they have absolutely no way of knowing this port is a port we have set up for SQL server. They won't even waste their time attempting a brute force attack, they would rather want to confirm an IP with port 1433 and spend the coming days trying to find a way in to that rather than waste time on a port which could be for any one of thousands of applications.

We disable the standard / default system administrator account

Again this is another SQL server default feature where it creates a system administrator account for the user. This account has total access and control over everything in the database and is the most powerful of user types. As extra security, this user is disabled therefore rendering it useless.

Password protected logins for Smart Club Cloud access

The Smart Club Cloud needs to access the club database using the static IP supplied by the club. The username and password to access the SQL database is stored in a file (*not in a database*) within the protected area on the server. This username and password combination consists of a strong makeup of alphanumeric characters and symbols, yet again adding an extra layer of security to the entire setup.