Stanton St Quintin Parish Hall

Charity Reg: 1165682

SSQ Hall Committee Ltd – Cookie Policy

The Privacy and Electronic Communications Regulations (PECR) 2003 requires websites being used within the UK to contain a Cookie Policy.

Legislation relating to cookies can be found in PECR, GDPR and EU Regulation on Privacy and Electronic Communications (commonly known as ePrivacy Regulation).

What are cookies?

Cookies are simple text files that are stored on your computer or mobile device by a website's server. More formally a cookie is known as an HTTP (Hypertext Transfer Protocol) cookie, a web cookie, an internet cookie or a browser cookie. The name 'cookie' is a shorter version of 'magic cookie', which is a term for a packet of data that a computer receives, then sends back without changing or altering it.

Each cookie is unique to your browser and no matter what it's called, it consists of information. When you visit a website, the website server sends a cookie to your computer. Your computer stores it in a file located inside your web browser. This file is often called 'Cookies'.

Information in cookies can vary from your preferred language to your location. Cookies often store your settings for a website. When you return to the site, the browser sends back the cookies that belong to the site. This allows the site to present you with the information customised to fit your needs, containing website preferences previously set up.

Cookies can contain a wide range of information such as a unique identifier, website's domain name and some digits and numbers, it can also (where there are sign-ins and account set up) contain personal data such as your name, home address, email address or phone number.

Why are cookies used on our website?

SSQParishHall.co.uk is hosted on Wix.com platform.

Primarily cookies are used to:

- Sustain or improve the experience of website visitors;
- Monitor and analyse the performance, operation and effectiveness of the platform;
- Ensure the platform is secure and safe to use.

What types of cookies are there?

There are a number of classifications and types of cookies:

Provenance

First-party cookies:

These are directly set by our website when visited by the user. These cookies are used, primarily, for ease of use of the website and convenience of the user.

Third-party cookies:
Third-party cookies are set by those websites or social media sites that are not directly visited by the user. So, these are cookies from sites linked to from the primary site. Currently the only links ssqparishhall.co.uk website has to third-parties are via a button link to Facebook and Google Maps.

Once installed, third-party cookies also track users and save their information for ad targeting and behavioural advertising.

Some browsers are making it more difficult for third-party cookies to be used. Safari and Firefox have blocked third-party cookies. Google Chrome is intending to block third party cookies.

Duration

Session cookies:
Session cookies will expire either immediately after leaving the web browser or within a few seconds of leaving.

An example of session cookies is when using an e-commerce site, the items a user places in a basket will be remembered, because of the session cookies. If session cookies were not in use then basket items would disappear by the time the user got to checkout.

Persistent cookies:
Persistent cookies are stored on a user's device to help remember information, settings or sign-on credentials that a user has previously saved. This enables a faster website experience and creates convenience for the user. These cookies track website visitors as they move around the site, to identify what people like about a website by how long they stay on a page, frequency of visit, etc.

As the name suggests, persistent cookies can stay on the user's browser for a long time. Generally, these cookies are required to have an expiration date (anything between a second to 10 years). According to the ePrivacy Directive persistent cookies should be deleted after 12 months, but this is not always the case.

Purpose

Essential/Strictly necessary cookies:
These cookies are essential for you to browse our website and use any features that we set up.

Preference cookies:
Also knows as functional cookies, these are used to allow a website to remember choices you made in the past, such as language preference, login user name. Not necessary for our website.

Statistics cookies:
Also known as performance cookies and are essential. These cookies collect information about how you use a website, such as which pages you visit, which links you click on. None of this information can be used to identify you. It is all aggregated and is, therefore, anonymised. Their sole purpose is to improve website functions.

Marketing cookies:
These cookies track online activity to help advertisers deliver more relevant advertising or to limit how many times you see an ad. These cookies can share that information with other organisations or advertisers. These are persistent cookies and generally third-party.

Which cookies do we use?

Websites designed using Wix.com hosting and design services use the following cookies as a matter of course:

Cookie Name	Purpose	Duration	Cookie Type
XSRF-Token	Security	Session	Essential
hs	Security	Session	Essential
svSession	User login (*not currently required by users of our website*).	2 years	Essential
SSR-caching	To indicate the system from which the site was rendered	1 minute	Essential
wixCIDX	Monitoring/debugging system	3 months	Essential
wix_browser_sess	Monitoring/debugging system	session	Essential
consent-policy	Used for cookie banner parameters	12 months	Essential
smSession	For logged in site members (*not relevant for website viewers*)	Session	Essential
TS	Security and anti-fraud	Session	Essential
bSession	System effectiveness measurement	30 minutes	Essential
fedops.logger.sessionId	Stability/effectiveness mesurement	12 months	Essential
wixLanguage	To save user language preference (no currently available for viewers).	12 months	Functional

Additional cookies may be used in future, if and when the website incorporates apps or links.

Protecting yourself from cookie fraud

Cookies are not viruses, not even malicious cookies. The plain text nature of cookies means they cannot be executed (i.e. the process of running a computer software program, script or command).

Your antivirus software can do little or nothing to protect against malicious cookies. There are two key things to do to protect yourself against becoming a victim of cookie fraud.

- Keep your browser up to date as many cookie exploits are designed to take advantage of holes in outdated browser security. Most update automatically but some may still require manual update.

- Avoid questionable sites. If you should see a warning either by your browser or by a search engine that a site is potentially malicious, don't proceed to the site unless you wish to risk infiltration by malicious cookies.

Managing cookies on your device

There are a number of websites providing advice on disabling and deleting cookies. A few are listed below.

https://www.allaboutcookies.org/manage-cookies/

https://aboutcookies.org.uk/managing-cookies

Review

This document will be reviewed January 2023.