What are cookies and how do we use them?

Cookies are text files containing small amounts of information, which your computer or mobile device downloads when you visit a website. When you return to websites - or visit websites that use the same cookies - they recognise these cookies and therefore your browsing device. Cookies can also help ensure marketing you see online is more relevant to you and your interests. You can learn about the cookies we use and how to manage them below.

Most browsers automatically accept cookies, but you can usually refuse or selectively accept cookies, by adjusting the preferences in your browser. If you turn cookies off, there may be some features of our site that will not be available to you and some web pages may not display properly.

Cookies may be either "session" or "persistent." A session cookie expires (i.e., is deleted) when you close your browser. A persistent cookie remains until it expires, or you delete the cookies via your browser settings. Expiration dates are set in the cookies themselves and may vary in length, depending on the purpose of the cookie.

You can find more information about managing cookies at All About Cookies.org and in the section at the end of this policy.

What cookies do we use?

Bluesource uses cookies to enhance your browsing experience, improve website performance, deliver personalized content, and ensure critical website functionalities. Below, we outline the types of cookies we use, their purposes, and their lifespans.

We are also committed to securing your data and ensuring that all cookies are managed in accordance with industry best practices and regulatory standards.

Strictly Necessary Cookies

The following strictly necessary cookies are essential for the website to function properly. They cannot be disabled as they ensure the core functionalities of the site, such as navigation, access to secure areas, and protection against security threats such as clickjacking:

Cookie Subgroup	Cookies	Usage Description	Lifespan
bluesource.co.uk	secure-frame-token	Protects against clickjacking by enforcing secure iframe behavior.	Session

Performance Cookies

The following performance cookies collect information about how visitors use our site to help us improve its functionality and performance:

Cookie Subgroup	Cookies	Usage Description	Lifespan
DoubleClick.net	IDE	Used by Google DoubleClick to register and report website user actions after ad interaction.	13 months
Google Analytics	_ga, _gid	Used to distinguish users and collect site usage statistics.	_ga: 2 years, _gid: 24 hours
Google Maps	NID	Used by Google Maps to remember user preferences and zoom level.	6 months
HubSpot	__hssc, __hssrc, __hstc, hubspotutk	Used to track sessions and identify visitors.	13 months
LinkedIn	bcookie, li_gc, lidc	Used by LinkedIn for tracking embedded services and consent preferences.	2 years
Twitter	personalization_id	Used by Twitter to track user preferences and behavior for embedded content.	2 years
Vimeo	vuid	Used by Vimeo player to track video usage analytics.	2 years

Advertising Cookies

The following advertising cookies are used to deliver ads relevant to you and measure the effectiveness of Bluesource's marketing campaigns:

Cookie Subgroup	Cookies	Usage Description	Lifespan
DoubleClick.net	IDE	Tracks ad performance and user interactions after exposure.	13 months

Functional Cookies

The following functional cookies enable enhanced functionality and personalization on our website, such as remembering your preferences:

Cookie Subgroup	Cookies	Usage Description	Lifespan
bluesource.co.uk	messagesUtk, hs-messages-is-open	Supports live chat functionality and session continuity.	13 months / 30 minutes

How we protect your cookie data

Bluesource takes data protection very seriously and is both ISO27001 and Cyber Essentials certified, protecting cookie data in the following ways:

- All cookies are transmitted over HTTPS connections only.
- We apply the Secure, HttpOnly, and SameSite attributes where appropriate to protect against unauthorized access or use.
- Clickjacking protection is enforced through modern browser security headers (Content-Security-Policy and X-Frame-Options).
- Third-party scripts are reviewed and monitored to prevent unauthorized cookie tracking.
- Our HubSpot CMS is configured with security best practices, including access control, web application firewall (WAF) protection, and malware scanning.
- Website forms are protected with anti-CSRF tokens and validation measures to prevent misuse of cookies in submissions.

Managing Cookies

You can control cookie preferences through your browser settings or use the cookie management tool on our website. Disabling certain cookies may affect your browsing experience.

For more information, visit our Privacy and Governance page: https://bluesource.co.uk/privacy-and-governance

For assistance, contact us at info@bluesource.co.uk.