# Contents

[Contents 1](#_Toc209777107)

[Introduction 2](#_Toc209777108)

[Terminology and definitions 2](#_Toc209777109)

[Consent for cookies 2](#_Toc209777110)

[Who you need to get consent from 4](#_Toc209777111)

[Exemptions from providing information and obtaining consent 4](#_Toc209777112)

[Providing Privacy Information 4](#_Toc209777113)

[Appendix One – Techniques & other considerations 6](#_Toc209777114)

[Techniques for providing information and seeking consents 6](#_Toc209777115)

[What else do we need to consider 7](#_Toc209777116)

[Appendix Two – Example Cookie Privacy Notice 9](#_Toc209777117)

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Summary of changes** | **Author** |
| V1.0 | January 2021 | Initial | One West |
| V2.0 | January 2022 | Formatting | One West |
| V3.0 | February 2023 | Formatting | One West |
| V4.0 | September 2023 | Full review – reformatted and changes to terminology. | One West |
| V4.1 | October 2023 | Formatting | One West |
| V5.0 | September 2025 | Refreshed content. Addition of example cookie privacy notice. | One West |

# Introduction

When a user accesses a website or webpage, they download a small file onto their computer, smartphone, wearable technology, smart TVs, and other connected devices. This file is called a ‘cookie’. Due to the data that cookies gather they are consider personal identifiers by the Data Protection Act.

There are two distinct types of cookies.

* Essential cookies
* Non-essential cookies

This guide builds on definitions in the Privacy and Electronic Communications Regulations (PECR) and the Information Commissioner’ Office (ICO) [Guidance on the rules on use of cookies and similar technologies](https://ico.org.uk/media/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies-1-0.pdf). The regulations require that unless an exemption applies you must:

* Tell people that cookies are used.
* Explain what the cookies will do and why.
* If a non-essential cookie is used you must get the person’s consent to store a cookie/s on their device.

This guidance goes through the following steps:

* Working out if you need to seek consent for non-essential cookies.
* How to ask for consent.
* What privacy information you need to provide.

# Terminology and definitions

**Essential Cookies** are those required to structure a website for a specific device, remember information you input to enable you to navigate between pages, or connectivity details. These cookies **Do not need consent.** Included in this definition are statistic or analytic cookies used to improve website services, performance or presentation, though they are not essential, they do not require consent.

**Non-Essential Cookies** or cookies that are not strictly necessary are cookies that track users activities for the purposes of advertising, embedding links, or ‘widgets’ which are small applications that appear on webpages. Many of these will be from third parties, but not all, it depends on how you and your webpage developer have set up your webpage. You **must gain consent** for non-essential cookies.

The **subscriber** means the person who pays the bill for the use of a line / network connection while the **user** is the person using the computer or other device to access an online service, in many cases the **subscriber** and the **user** may be the same.

Consent for a cookie should be obtained from the **subscriber** or **user**. But in practice, you may not be able to distinguish between consent provided by the **subscriber** or the **user**. The key issue is that one of the parties must provide valid consent.

# Consent for cookies

You must notify users that cookies are being used whether they are essential or non-essential, however you only need to gain consent for non-essential cookies.

Consent for non-essential cookies must be sought **before** they are installed on a device. You may use a banner or a cookie manager to do this. You should speak to your web developer regarding this if you do not manage your own website. What cookies are used can be easily identified using the software that the website is built with.

When a user first accesses a webpage you must tell them that cookies are being used, a cookie banner is one of the best ways to do this, it will appear usually at the bottom of the screen but can appear anywhere on the screen. You may only use essential cookies, in which case you can simply say that essential cookies are being used and have a clickable option in the banner saying yes I understand and another option linking to your cookie privacy information page.

A typical example where only **essential cookies** are used is below.

|  |
| --- |
| We only use essential cookies on our website. |
| I understand | Further information about the cookies we use |

If you use **non-essential cookies** you will need to have further options but must ensure that the cookies are not installed until the user provides consent. You cannot use pre-ticked boxes except with essential cookies as they do not require consent. An example of this type of banner or cookie manager is below.

|  |
| --- |
| We use essential and non-essential cookies on our website. We ask your consent to enable these cookies. |
| I consent. | I only want the following cookies selected below. | Information about the cookies we use. | Further information about cookies. |
| Essential ⃝ | Analytic ⃝ | Marketing ⃝ | All cookies ⃝ |

The above examples illustrate the two most common types of cookie notification and consent; they may be presented in different ways but will retain the fundamental components.

A cookie manager may be used which will generally have a constant presence on the screen, you may have to pay for a cookie manager as they are generally third party products.

An example of a cookie manager that appears on the screen, the small C at the bottom left hand side will minimise the option box but can be accessed at any time if the user wishes to change their preferences.



# Who you need to get consent from

In practice a user accessing your website will provide consent if necessary, the user could be someone who is just temporarily using the device or they could be the subscriber, it does not really make a difference as long as your non-essential cookies are not automatically enabled, and if necessary you can provide evidence that the user or subscriber provided consent in any case.

In education settings where children may be using devices the use of cookies should be managed through technical controls and predetermined browser settings. In general cookies should be disabled or retained only for the period of use, parents should be told about the use of cookies in the general parent and pupil privacy notice.

Managed devices that are provided by your organisation may be controlled; however, you may decide to leave the decision of consent to the user. Technical settings should be put in place that remove cookies at the end of the period of use or at the end of the day.

# Exemptions from providing information and obtaining consent

|  |  |
| --- | --- |
| **Activity**  | **Likely to meet ‘Strictly Necessary’ exemption**  |
| A cookie used to remember the goods a user wishes to buy when they go to the checkout or add goods to their shopping basket. | ✓ |
| Cookies that are essential to comply with the GDPR’s security principle for an activity the user has requested – for example in connection with online banking services. | ✓ |
| Cookies that help ensure that the content of a page loads quickly and effectively by distributing the workload across numerous computers (this is often referred to as ‘load balancing’ or ‘reverse proxying’)  | ✓ |
| Cookies used for analytics purposes, e.g. to count the number of unique visits to a website  | ✓ |
| First and third-party advertising cookies (including those used for operational purposes related to third-party advertising, such as click fraud detection, research, product improvement, etc.). | 🗶 |
| Cookies used to recognise a user when they return to a website so that the greeting they receive can be tailored | 🗶 |

# Providing Privacy Information

You need to provide information in the form of a privacy notice about cookies in such a way that the user will see it when they first visit your service. If you use a cookie banner as shown earlier at the top of page 3 you will need to create a separate webpage where you will need to outline the cookies used and their function.

Gathering that information can usually be done by your web page development team or company or you can use a simple online cookie auditor application that lists the cookies for you. You may need to expand on the information provided by a cookie audit app but in general they will provide everything that you need, double check the results against the example cookie privacy notice in appendix 2.

An example cookie privacy notice is provided in appendix 2 but it must contain the following information.

* A brief description of what cookies are.
* What cookies are used, broken down into their respective types.
* How to change cookie settings, either through the cookie manager or banner, or through browser settings. These are fairly generic and so the standard text used in the example in appendix 2 can be used.

# Appendix One – Techniques & other considerations

## Techniques for providing information and seeking consents

Various techniques for providing information and seeking consents are discussed below:

### Can we use message boxes and similar techniques?

Message boxes such as banners, pop-ups, message bars, header bars or similar techniques might initially seem an easy option for you to achieve compliance. However, you need to consider their implementation carefully, particularly in respect of the implications for the user experience.

There are challenges with using these techniques. If users do not click on any of the options available and go straight through to another part of your site, and you go ahead and set non-essential cookies on their devices, this would not be valid consent. This is because users who fail to engage with the consent box cannot be said to consent to the setting of these cookies.

### Can we rely on settings-led consent?

Some cookies are deployed when a user makes a choice over a site’s settings. In these cases, consent could be sought as part of the process by which the user confirms what they want to do, or how they want the site to work.

It might be the size of the text a user wants to have displayed, the colour scheme they like or even the 'personalised greeting' they see each time they visit the site. You must take care that any processing of personal data related to the setting of preference cookies or other personalisation features is limited to what is necessary for this purpose.

### Can we rely on feature-led consent?

Your site may include video clips or remember what users have done on previous visits to personalise the content they provide. Some cookies would then be stored if the user chooses a particular feature of your site. However, you still need to provide clear and comprehensive information and obtain consent. Where the feature is provided by a third party, users will need to be made aware of this and be given information on how the third party uses cookies and similar technologies so that the user is able to make an informed choice.

### Can we rely on browser settings and other control mechanisms?

This is where the user or subscriber sets up their browser so that only certain cookies are allowed.

Although European guidelines are no longer relevant to the UK they still provide helpful guidance that you should consider. PECR suggest that browser settings may be one means of obtaining consent if they can be used in a way that allows the subscriber to indicate their agreement to cookies being set. However, you should not assume each visitor to your website can configure their browser settings to correctly reflect their preferences in relation to the setting of cookies.

In future you may well be able to rely on the user’s browser settings as part, or all, of the mechanism for satisfying yourself that you have consent to set cookies. For now, relying solely on browser settings will not be sufficient.

### Can we use ‘terms and conditions’ to gain consent for cookies?

No. Consent must be separate from other matters and cannot be bundled into terms and conditions or privacy notices. The key point is that you should be upfront with your users about your use of cookies.

Any attempt to gain consent that is bundled in terms and conditions will not be compliant.

### Can we use ‘cookie walls’?

A cookie wall – sometimes called a ‘tracking wall’ – requires users to ‘agree’ or ‘accept’ the setting of cookies before they can access an online service’s content. This is also known as the ‘take it or leave it approach’.

In some circumstances, this approach is inappropriate. For example, where the user or subscriber has no genuine choice but to sign up. This is because the UK GDPR says that consent must be freely given.

If your use of a cookie wall is intended to require, or influence, users to agree to their personal data being used by you or any third parties as a condition of accessing your service, then it is unlikely that user consent is considered valid.

However, it should be noted that not all cookie tracking is intrusive or high risk.

Moreover, the UK GDPR is clear that the right to the protection of personal data:

* Is not absolute.
* Should be considered in relation to its function in society.
* Must be balanced against other fundamental rights, including freedom of expression and the freedom to conduct a business.

The key is that users are provided with a genuine free choice. Consent should not be bundled up as a condition of the service unless it is necessary for that service.

### Can we pre-enable any non-essential cookies?

No. Just because users may be unlikely to select a particular non-essential cookie when given the choice, or because the cookie is not privacy intrusive, is not a valid reason to pre-enable it.

Enabling a non-essential cookie without the user taking a positive action before it is set on their device does not represent valid consent. By doing this, you are taking the choice away from the user.

## What else do we need to consider

### What if our use of cookies changes?

If your use of cookies changes significantly, then you will need to consider how this impacts on any consent that you have already gained.

### What about cookies set on websites that we link to?

Your online service / web site may not be the only place where users and subscribers could have cookies set during their interactions with you.

For example, if you also have a presence on social media platforms, then those platforms will set cookies on users’ devices once they visit your pages there, eg after they’ve navigated away from your website. These cookies can be used for different purposes depending on the platform, but common uses are to provide you with statistical information about how users interact with your social network presence.

Although you may not directly control the cookies that the social media platform sets, you do control the fact that you have a presence on that platform and you are also able to determine what types of statistics you want the platform to generate based on user interaction. This means that you are jointly responsible, with the social media platform, for determining the purpose and means of the processing of personal data of any user that visits your presence on that network and, therefore, you are a joint data controller for this activity with the platform.

This remains the case even if the network only provides you with anonymised or aggregated statistical information. To generate that information the platform will process personal data, firstly by recording what visitors do and then by then anonymising that information.

So, you need to ensure that your own privacy notice on your website includes references to any social media presence that you may have, and how individuals are able to control the setting of any non-essential cookies once they visit there, even if these cannot be covered by your site’s consent mechanism.

### What about cookies set on overseas websites?

It is important to note that being based in the UK you are subject to the requirements of PECR even if your website is hosted overseas (eg, using cloud services based in the USA).

### How often should we get consent?

You should ensure that any first-time visitors to your website are provided with clear information about the cookies you use and are given choices and controls about any non-essential ones.

There is a range of reasons why you may need visitors to ‘reconsent’ to cookie settings. Depending on the circumstances you may not need to ask for fresh consent each time someone visits. Several factors may need to be considered, such as frequency of visits or updates of content or functionality.

An example of when you need to obtain fresh consent is when you are setting non-essential cookies from a new third party. This is because the consent that the user previously gave would apply only to those parties that you specified at the original time. When your service sets cookies from a new third-party, you would need to ensure that users consent to this.

### How should we keep records of user preferences?

Some users will visit your website regularly and others will visit rarely, with a spectrum of others in between. You therefore need to decide an appropriate interval between when you require users to select their preference (whether that is consent or rejection) and decide when that preference expires (after which point users are given the option again).

PECR isn’t intended to inconvenience or unduly disrupt the experience of your users. You are not expected to repeatedly require your users to specify their preference as a matter of course, whether that results in consent for non-essential cookies or refusal. These are issues that you will need to determine as the service provider with your web developer.

# Appendix Two – Example Cookie Privacy Notice

**Use of cookies by the school/town council etc**

Cookies are small text files that are placed on your computer by websites that you visit. They are widely used in order to make websites work, or work more efficiently, as well as to provide information to the owners of the site. The table below explains the cookies we use and why.

**Essential cookies**

|  |  |  |
| --- | --- | --- |
| **Name** | **Purpose** | **Expires** |
| CookieControl | This cookie is used to remember your choice about cookies on www.example.com | 90 days |
| language | This cookie is used to remember any selection you have made about language on www.example.com using the language selector, so that the site will be shown in your chosen language when returning to the site.  | 7 days |

**Analytics cookies (optional)**

|  |  |  |
| --- | --- | --- |
| **Name** | **Purpose** | **Expires** |
| Silktide analytics javascript | Silktide analytics javascript is used to collect information about how visitors use our website. We use the information to compile reports and to help us improve the website. We collect information including the number of visitors to the website, where visitors have come to the website from and the pages they visited.The information is collected and processed in a way that does not directly identify anyone. Once the information is collected, the IP address and browser details of a visitor is used to create a 'magic number' that changes every 24 hours. The IP address and specific browser details are immediately forgotten and never stored. | 24 hours |

**Video player cookies (optional)**

Our site contains some video content. If you don't enable video player cookies, video content will appear as standard links, which will take you to YouTube and Vimeo to watch the videos. YouTube and Vimeo may set cookies when you use their sites. Or, if you enable video player cookies, you'll see videos embedded in our pages and YouTube and Vimeo may receive information about the videos you watch for analytics and advertising purposes.

**YouTube embedded player**

|  |  |  |
| --- | --- | --- |
| **Example cookies** | **Purpose** | **Expires** |
| AECAPISIDHSIDNIDSAPISIDSID\*SSIDSOCS\_Secure\* | We embed videos from our official YouTube channel, using YouTube’s privacy-enhanced mode. You can read about YouTube’s privacy-enhanced mode on [YouTube’s embedding videos information page.](https://support.google.com/youtube/answer/171780?hl=en-GB#zippy=%2Cturn-on-privacy-enhanced-mode)If you visit a page containing a YouTube video and are logged in to a YouTube or Google account, Google may use cookies for security purposes, remember your preferences, and receive information about the videos you watch for analytics and advertising purposes cookies and collect data linked to your Google account. For more information, see the [Google Privacy Policy](https://policies.google.com/privacy?gl=GB&hl=en-GB#intro). | Between 180 and 400 days |

**Vimeo embedded player**

|  |  |  |
| --- | --- | --- |
| **Example cookies** | **Purpose** | **Expires** |
| \_cf\*\_ga\*\_gid\_uet\*\_builderSessionidlanguageOptanon\*sd\_client\_idvimeo\*vuid | We embed videos from our official Vimeo channel using Vimeo’s Do Not Track setting. You can read about this on [Vimeo’s embedding videos page](https://help.vimeo.com/hc/en-us/articles/12426260232977-Player-parameters-overview).Vimeo may use cookies to enable the video to play, remember your preferences and maintain the security of its service.If you visit a page containing a Vimeo video and you are logged in to your Vimeo account or if you’ve visited the Vimeo website before the website, Vimeo may use cookies eg to keep you logged in, for analytics and advertising purposes, and collect data linked to your Vimeo account. For more information, see the [Vimeo cookies policy](https://vimeo.com/cookie_policy). | Between 0 and 400 days |

\*indicates various cookies that contain additional letters, numbers or characters in their name.

**Cookies on our careers site**

We use these cookies on the external career site:

* **Session management cookies:** User, device, and session ID cookies along with timestamp cookies for timing out sessions after inactivity. These cookies expire at the end of the session.
* **Routing cookies:** To forward requests for a single session to the same server for consistency of service. These cookies expire at the end of the session.
* **Application:** Security Management (ASM) cookies - To help protect web applications and infrastructure from security attacks. These cookies expire at the end of the session.

|  |  |  |
| --- | --- | --- |
| **Name** | **Purpose** | **Expires** |
| PLAY\_LANG,PLAY\_SESSION,timezoneOffset,wd-browser-id | User, device, and session ID cookies along with timestamp cookies for timing out sessions after inactivity. | When you close your browser |
| TS\*  | Helps prevent cyber attacks on the user’s interactions with the enterprise cloud applications. Verifies that the domain and subdomain cookies sent between the web server and the client aren’t altered. | When you close your browser |
| CALYPSO\_CSRF\_TOKEN | Contains a CSRF token to prevent cross-site request forgery attacks, that is, to prevent a user from carrying out unintended operations on the career site. | When you close your browser |
| Naming convention of WorkdayLB\_\*WorkdayLB\_UICLIENT,WorkdayLB\_SAS | Used to forward requests for a single session to the same server for consistency of service. | When you close your browser |

\*indicates various cookies that contain  additional letters, numbers or symbols in their name.

**How do I change my cookie settings?**

You can change your cookie preferences at any time by state how users can access the banner or manager.

Alternatively, most web browsers allow some control of most cookies through the browser settings. To find out more about cookies, including how to see what cookies have been set, visit [www.aboutcookies.org](http://www.aboutcookies.org/) or [www.allaboutcookies.org](http://www.allaboutcookies.org/).

Find out how to manage cookies on popular browsers:

* [Google Chrome](https://support.google.com/accounts/answer/61416?co=GENIE.Platform%3DDesktop&hl=en)
* [Microsoft Edge](https://privacy.microsoft.com/en-us/windows-10-microsoft-edge-and-privacy)
* [Mozilla Firefox](https://support.mozilla.org/en-US/kb/enable-and-disable-cookies-website-preferences)
* [Microsoft Internet Explorer](https://support.microsoft.com/en-gb/help/17442/windows-internet-explorer-delete-manage-cookies)
* [Opera](https://www.opera.com/help/tutorials/security/privacy/)
* [Apple Safari](https://support.apple.com/en-gb/safari)

To find information relating to other browsers, visit the browser developer's website.

To opt out of being tracked by Google Analytics across all websites, visit <http://tools.google.com/dlpage/gaoptout>.