# Contents

[Contents 1](#_Toc148095494)

[Introduction 2](#_Toc148095495)

[Purpose 2](#_Toc148095496)

[Terminology and definitions 2](#_Toc148095497)

[Consent for cookies 3](#_Toc148095498)

[Who you need to get consent from 4](#_Toc148095499)

[Exemptions from providing information and obtaining consent 4](#_Toc148095500)

[Practical advice for compliance 6](#_Toc148095501)

[How to request consent for cookies 6](#_Toc148095502)

[Providing information and seeking consent 7](#_Toc148095503)

[Appendix One – Techniques & other considerations 8](#_Toc148095504)

[Techniques for providing information and seeking consents 8](#_Toc148095505)

[What else do we need to consider 9](#_Toc148095506)

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Summary of changes** | **Author** |
| V1.0 | January 2021 | Initial | One West |
| V2.0 | January 2022 |  | One West |
| V3.0  | February 2023  |  | One West |
| V4.0 | September 2023 |  | One West |

# Introduction

When a user accesses a website or webpage, they download a small text file onto their ‘terminal device’ (computer or smartphone). This file is called a ‘cookie’. A cookie helps that website remember information about someone’s visit, which can both make it easier to visit the site again and make the site more useful to them. Cookies are used in numerous ways, such as:

* Remembering what is in a basket when shopping for goods online.
* Supporting users to log in to a website.
* Analysing traffic to a website.
* Tracking users' browsing behaviour.

The UK GDPR classifies cookies as a type of ‘online identifier’, meaning that in certain circumstances they will be personal data. Hence, it is important your organisation complies with legislation governing use of 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). Although the PECR are EU regulations they still apply alongside UK GDPR. Broadly, the regulations require that (unless an exemption applies) you must:

* Tell people that cookies are used.
* Explain what the cookies will do and why.
* Get the person’s consent to store a cookie/s on their device.

Crucially, this guide relates to both your presence on the Internet that can be accessed by the public, as well as your responsibilities toward your staff using Internet services as part of their work.

# Purpose

The purpose of this guide is to outline the need for being compliant with legislation covering use of cookies and similar technologies, describe how to conduct a cookie audit and then describe ideal and best practices related to using cookies.

Assuming you do not develop your own website, this guide should help inform your work with the service providers you work with and with your website developer.

# Terminology and definitions

Before considering compliance with regulations covering use of cookies, it is worth understanding what is meant by key terms, **‘subscriber** or **user**’ and ‘**terminal** **equipment**’. Cookie rules apply to the **terminal equipment** of the **subscriber** or **user**.

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. For example, when an individual uses their broadband connection to access a website on their computer or mobile device, that person would be the *user* as well as the *subscriber* if they pay for the connection. Although, if a family member visits a subscriber’s home and uses the internet connection to access your service from their own device, they would be the **user**.

Crucially, PECR states that 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.

**Terminal equipment** refers to the device a cookie is placed on. Typically, this is a computer or mobile device, but may be other equipment such as wearable technology, smart TVs, and other connected devices.

The ICO describes cookies as:

* **Session cookies** or **persistent** **cookies**.
* **First-party and** **third-party** **cookies**.

**Session cookies** allow websites to recognise and link the actions of a user during a browsing session. These are often used to remember what a user has put in their shopping basket.

**Persistent cookies** are stored on a user’s device in-between sessions. They can allow the preferences or actions of the user across a site (or across different websites) to be remembered.

**First-party cookies** are set directly by the website the user is visiting, ie the URL displayed in the browser's address bar. **Third-party cookies** are set by a domain other than the one a user is visiting. This often occurs when a website incorporates elements from other sites, such as images, social media plugins or advertising.

Importantly PECR also apply to any **similar technologies** – such as Local Shared Objects (sometimes called Flash cookies) – and can also cover other types of technology, including applications on smartphones, tablets, smart TVs or other devices.

# Consent for cookies

In broad terms, PECR requires that users or subscribers to websites consent to cookies being placed or used on their device although there is no definition of what consent means. Hence, it is worth following the UK GDPR general definition of consent[[1]](#footnote-1) that states:

‘Consent’ of the data subject means any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

The UK GDPR goes further and says that[[2]](#footnote-2):

* You must be able to demonstrate that you have valid consent.
* Consent requests must be ‘clearly distinguishable from other matters’ – ie, they must not be bundled as part of terms and conditions.
* Consent requests must be in an intelligible and easily accessible form, using clear and plain language.
* There must be a mechanism to allow the individual to withdraw their consent at any time.

Crucially, the UK GDPR bans pre-ticked boxes[[3]](#footnote-3) – silence or inactivity does not constitute consent.

Hence, in respect of cookies, this means:

* The user must take a clear and positive action to give their consent to non-essential cookies – continuing to use your website does not constitute valid consent.
* You must clearly inform users about what your cookies are and what they do before they consent to them being set.
* If you use any third-party cookies, you must clearly and specifically name who the third parties are and explain what they will do with the information.
* You cannot use any pre-ticked boxes (or equivalents such as ‘on’ sliders) for non-essential cookies.
* You must give users controls over any non-essential cookies, and still allow users access to your website if they don’t consent to these cookies.
* You must ensure that any non-essential cookies are not placed on your landing page (and similarly that any non-essential scripts or other technologies do not run until the user has given their consent).

Unfortunately, the ICO’s description of obtaining cookies is not entirely clear. Hence, it is important to note that the PECR do not distinguish between cookies used for analytics activities and those used for other purposes. Analytics cookies do not fall within the ‘strictly necessary’ exemption. This means you need to tell people about analytics cookies and gain consent for their use.

At times it may be worth you considering you collect personal data and whether you could use anonymised data instead, in order to comply with the data protection principles (which require personal data to be adequate, relevant and not excessive). This is likely to be relevant where you are not using the data to provide a service to the user – for example, if you are simply counting visitors to a website.

Nevertheless, you should be aware that the creation of anonymous information may involve processing of personal data – for example, to generate aggregate statistics based on user interaction. This processing would therefore be covered by the GDPR.

# Who you need to get consent from

PECR does not specify whether the user or subscriber’s wishes should take precedence if individuals have different preferences in respect of the setting of cookies. Other references in PECR to a subscriber’s ability to make decisions in this area, such as around browser settings, might suggest the subscriber’s preferences take priority, although in some circumstances this will not always be the case.

Hence in a working environment, where an employer (the subscriber) provides an employee (the user) with a device at work, along with access to certain services to carry out a particular task. Completing the task effectively depends on using a service that uses cookies, and a device that accepts them. In this case it is reasonable for the employer’s wishes to take precedence.

There are other sections of PECR, concerning browser settings, where the subscriber clearly can decide on behalf of any user. However, there will also be circumstances where a user’s wishes should take precedence.

In a domestic context there will usually be one subscriber (the person in the household paying the bill) and potentially several other users. If a user complained that your website was setting cookies without their consent, you could demonstrate compliance with PECR if you could show that consent had previously been obtained from the subscriber.

**In practice, the key to resolving problems is to ensure information about cookies and mechanisms for making choices are as easily accessible as possible to all users.**

# Exemptions from providing information and obtaining consent

There are two exemptions to providing information and obtaining consent. They are:

* A cookie is for the sole purpose of carrying out the transmission of a communication over an electronic communications network.
* A cookie is strictly necessary to provide an ‘information society service’ (eg a service over the internet) requested by the subscriber or user. Note a cookie must be essential to fulfil a request – cookies that are helpful or convenient but not essential, or that are only essential for your own purposes, will still require consent.

This means you are unlikely to need consent for:

* Cookies used to remember the goods a user wishes to buy when they add goods to their online basket or proceed to the checkout on an internet shopping website.
* Session cookies providing security that is essential to comply with data protection security requirements for an online service the user has requested – eg online banking services.
* Load-balancing cookies that ensure the content of your page loads quickly and effectively by distributing the workload across several computers.

**However, it is still good practice to provide users with information about these cookies, even if you do not need consent.**

At this stage it is worth considering what Information Society Services (ISSs) are. ISSs are defined as:

‘Any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services. (This may include entertainment, storage solutions or educational services)[[4]](#footnote-4)

What is unclear in this definition is to what extent providing information via a website constitutes an ISS. In many cases information provided is not done so in exchange for remuneration, hence is it right to assume that an informative website, such as a ‘gov.uk’ website or news website is providing services as an ISS?

To help understanding here are several examples of where the ‘strictly necessary’ exemption may or may not apply:

|  |  |
| --- | --- |
| **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, eg 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 | 🗶 |

# Practical advice for compliance

Crucially, the ICO provides as much flexibility as possible for you to design solutions that meet your business needs and provide users with the choices they require. The ICO takes a risk-based approach to enforcement in this area, taking into account the level of intrusion, the efforts made to provide clear information and get consent, and then any consumer (data subject - subscriber or user) concern.

If you are unsure whether your organisation currently complies with the rules relating to cookies it is worth taking the following steps:

* Check what type of cookies and similar technologies your organisation uses and how you use them.
* Assess how intrusive your use of cookies is.
* Where you need consent decide what solution to obtain consent will be best in your circumstances.

In terms of your website, you will need to determine the purpose for the cookies you use. A cookie audit will help by:

* Identifying those cookies operating on or through your website. A combination of browser-based tools and a review of server-side code would help with this.
* Identify the type of cookie – session or persistent.
* Define the purpose(s) of each of the cookies you use (or intend to use).
* Confirm whether cookies are linked to other information held about users – such as usernames – and whether use of cookies also involves (or will involve) processing other personal data.
* Identify what data each cookie holds or otherwise processes.
* Distinguish between which cookies are strictly necessary and which ones are not (and would therefore require clear and comprehensive information and consent)
* Ensure that your consent mechanism enables users to control the setting of all non-essential cookies.
* Determine the lifespans of any persistent cookies and whether these durations are justifiable for the stated purpose.
* Determine whether each cookie is a first or third-party cookie, and if it is a third-party cookie who sets it.
* Check that your privacy information provides accurate and clear information about each cookie.
* Confirm what information you share with third parties, and what users are told about this.
* Document your findings and follow-up actions and build in an appropriate review period.

Having conducted a cookie audit what constitutes ‘strictly necessary’ (hence exempt from seeking consent) will to some degree be determined by the purpose of the site.

For example, a site that sells products will mean that a cookie that remembers the content of the previous page would be strictly necessary if its inclusion meant that every time the user navigated away from the shopping basket, it would reset the contents. While a website that uses an online assessment form may need a certain cookie that looks at the user’s system to work out how best to layout the form, for an information and guidance site with a separate login section the website designer might consider the security compliance cookie as strictly necessary.

**Regardless, your website should clearly explain what cookies are used and what they do.**

# How to request consent for cookies

How you request consent for cookies will depend initially on what the cookies are doing and, to some extent, on the relationship you have with your users. When considering how to provide information about cookies and how to request consent there are different techniques for drawing users’ attention to information and the choices available to them. You may also find it helpful to look at the methods other online services already use. Importantly, you need to ensure any consent mechanism you put in place allows users to have control over all the cookies your website sets, not just your own.

For example, if you want to set third-party content such as tracking pixels and beacons from social networks, you must ensure users are given information about these and appropriate controls to signify whether they consent. Admittedly, this can be challenging as not all consent mechanisms presently enable users to disable cookies from third parties directly. However, designing and implementing a consent mechanism that works only for some cookies would not be compliant with PECR, as the user is not provided with any control over these cookies – they must visit different websites and take different actions to disable them.

Ultimately, you determine what cookies are set on your website, and in particular, the number and type of third-party cookies. One consideration before incorporating a third-party cookie should be whether your consent mechanism allows the user to control whether the cookie is set or not.

Hence it is recommended that you work closely with the company / organisation you have contracted to develop and maintain your website to decide what cookies are appropriate for you and agree what methods you use to provide information and seek consent.

# Providing information and seeking consent

You need to provide information about cookies in such a way that the user will see it when they first visit your service. This is usually done within the cookie consent mechanism itself.

You should also provide more detailed information about cookies in a privacy or cookie policy accessed through a link within the consent mechanism and at the top or bottom of your website. Hence, you should consider how the design of your online service impacts on the visibility of the link to your policy.

For example, a link at the bottom of a concise webpage which has no content “below the fold[[5]](#footnote-5)” will be much more visible and accessible than a link in the footer of a dense webpage of 10,000 words. In this case, a link in the header may be more appropriate.

Other ways of increasing the prominence of cookie information include:

* Formatting – this might include using a different colour of font. The key is whether the link to this important information is distinguishable from ‘normal text’ and other links.
* Positioning – simply moving the link from the footer of the page to somewhere more likely to get attention is an easy but effective thing to try.
* Wording – Making the hyperlink more than simply ‘privacy policy’ would help. This could involve ‘signposting through some explanatory text, such as ‘Find out more about how our site works and how we put you in control.’)

You also need to ensure the information is clear so that your users understand it. Consider tailoring the language to your audience, and not using lengthy and overly complex terminology.

The rules are no different if children access your online service. You will need to provide clear and comprehensive information about your use of cookies and ensure you have consent for any that are not strictly necessary. However, if children are likely to access your service you will need to ensure that both the information you provide and the consent mechanism you use are appropriate for children.

# 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 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.

1. Article 4(11) of the UK GDPR [↑](#footnote-ref-1)
2. Article 7 of the UK GDPR [↑](#footnote-ref-2)
3. Recital 32 of the UK GDPR [↑](#footnote-ref-3)
4. Article 2(a) of the E-Commerce Directive and Article 1(2) of the Technical Standards and Regulation Directive (98/34/EC)/(98/48/EC) [↑](#footnote-ref-4)
5. Anything that isn’t visible immediately and requires scrolling is considered below the fold. [↑](#footnote-ref-5)