**Shape

Description automatically generated with medium confidenceCookie Policy**

**Document Control**

**A. Confidentiality Notice**

This document and the information contained therein is the property of Arch Health CIC.

This document contains information that is privileged, confidential or otherwise protected from disclosure. It must not be used by, or its contents reproduced or otherwise copied or disclosed without the prior consent in writing from Arch Health CIC.

**B. Document Details**

| **Document Title** | Cookie Policy |
| --- | --- |
| **Classification:** | Data Security & Protection |
| **Organisation:** | Arch Health CIC |
| **Owner and Role:** | Gary Bishop, CEO & SIRO |
| **Contributor and Role:** | Jennie Worthley, Practice Manager & IG Lead |
| **Full Policy Reviewed:** | 20.10.21 |
| **Full Policy Renewal Due:** | May 2024 |

**C. Document Revision and Approval History**

| **Version:** | **Date:** | **Version Edited By:** | **Version Approved By:** | **Comments** |
| --- | --- | --- | --- | --- |
| 1.1 | 20.10.21 | FP | GB | New Policy in line with new website launch |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# 1. Introduction

## Policy statement

The purpose of this policy is to outline Arch Health CIC’s considerations for the use of cookies in relation to visitors to the organisation’s website. This policy will further detail what cookies are and how they operate, plus information, the requirement to audit and what consent or compliance is required.

## Status

Arch Health CIC aims to design and implement policies and procedures that meet the diverse needs of our service and workforce, ensuring that none are placed at a disadvantage over others, in accordance with the [Equality Act 2010](https://www.legislation.gov.uk/ukpga/2010/15/contents/enacted). Consideration has been given to the impact this policy might have with regard to the individual protected characteristics of those to whom it applies.

This document and any procedures contained within it are non-contractual and may be modified or withdrawn at any time. For the avoidance of doubt, it does not form part of a contract of employment.

## Training and support

Arch Health CIC will provide guidance and support to help those to whom it applies to understand their rights and responsibilities under this policy. Additional support will be provided to managers and supervisors to enable them to deal more effectively with matters arising from this policy.

# Scope

## Who it applies to

This document applies to all staff at Arch Health CIC. Other individuals performing functions in relation to the organisation, such as agency workers, locums and contractors, are encouraged to use it.

Furthermore, it also applies to employees who may or may not be employed by the organisation but who are working under the Additional Roles Reimbursement Scheme (ARRS)[[1]](#footnote-0) in England.

## Why and how it applies to them

This document has been produced to provide staff at Arch Health CIC with an overview as to what cookies are and the need to maintain compliance with regard to the Data Protection Act 2018 and specifically the Privacy and Electronic Communications Regulations (PECR) EC Directives 2003.

# Definition of terms

## Cookie

Cookies are usually small text files, given ID tags, which are stored on a computer's browser directory or programme data subfolders.

Cookies are created when a user visits a website that uses cookies to keep track of their movements within the site, help users to resume where they left off, remember their registered login, theme selection, preferences and other customisation functions.

Further detailed information can be found at <https://allaboutcookies.org/cookies/>.

## Data analytics[[2]](#footnote-1)

Data analytics is the science of analysing raw data in order to make conclusions about that information. Data analytics can reveal trends and metrics that would otherwise be lost in the mass of information.

This information can then be used to optimise processes to increase the overall efficiency of a business or system.

## Privacy and Electronic Communications Regulations (PECR)[[3]](#footnote-2)

The Privacy and Electronic Communications Regulations (PECR) EC Directives 2003 cover the use of cookies for accessing and storing information on a user’s equipment or mobile device.

Further information on the PECR can be found at [Section 6.1](#_heading=h.147n2zr).

## Data Protection Act 2018[[4]](#footnote-3)

The Data Protection Act 2018 (DPA 2018) is a complete data protection system covering general data, law enforcement data and national security data.

## General Data Protection Regulation (GDPR)[[5]](#footnote-4)

The EU General Data Protection Regulation (GDPR herein) is to be read in conjunction with the DPA 2018. The GDPR applies to all EU member states and Arch Health CIC must be able to demonstrate compliance at all times. Further reading can be found within the GDPR Policy.

## Information Commissioner’s Office (ICO)

The ICO is the UK’s independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The ICO covers a number of legislations including the PECR.

Further reading on what the ICO does can be found [here](https://ico.org.uk/about-the-ico/what-we-do/).

# Understanding cookies

## How do cookies benefit the user?

Some cookies are used to remember searches or other aspects such as choosing a language, expanding and collapsing sections of tables of contents or dismissing notification banners.

Other cookies help to define what areas of the website are used. Any data captured will be anonymous and is used in an aggregated way meaning that cookies are collated to scrutinise overall trends in browsing behaviour.

## Are cookies safe?

Staff, patients and other visitors to the Arch Healthcare website may be aware that most websites use cookies.

All users should be reassured that cookies on the Arch Healthcare website, as for others, will not cause any harm to a device, nor do they advise who the user is or divulge any personal details about the user. The data they help to collect is anonymous. At Arch Health CIC, we do not use cookies to collect any data that could be used to personally identify any user.

## How are cookies turned off?

Most modern browsers will offer different ways to configure how they handle cookies and can vary from only allowing cookies from websites that a user trusts to the user blocking all cookies by default.

Steps for controlling users’ settings can vary for each browser. The following links are the official instructions for the most common browsers:

* [Google Chrome](https://support.google.com/chrome/answer/95647?hl=en)
* [Mozilla Firefox](https://support.mozilla.org/en-US/kb/enable-and-disable-cookies-website-preferences?redirectlocale=en-US&redirectslug=Enabling+and+disabling+cookies)
* [Apple Safari](https://help.apple.com/safari/mac/9.0/#/sfri11471)
* [Internet Explorer](https://support.microsoft.com/en-us/help/17442/windows-internet-explorer-delete-manage-cookies)
* [iOS Safari](https://support.apple.com/en-gb/HT201265)
* [Google Android](https://support.google.com/chrome/answer/114662?hl=en-GB&visit_id=637079494936234672-2171410805&rd=1)

For more advice on managing cookies, refer to the [All About Cookies](https://www.allaboutcookies.org/manage-cookies/) website.

# Types of cookies

There are many types of cookies and the following information has been obtained from both <https://aboutcookies.org.uk/cookie-types> and a useful page from <https://www.ageuk.org.uk/help/cookies/>.

It should be noted that this list is not exhaustive and some of the cookies below may be known by different names.

## Session cookie

A session cookie for a website only exists whilst the user is reading or navigating the website. When the user closes their web browser, these cookies are usually removed.

## Persistent cookie

A persistent cookie for a website exists on a user’s computer until a set future date, e.g. the cookie expiry date could be set as one year, and each time a website is accessed over this period the website could access the cookie.

## HttpOnly cookie

An HttpOnly cookie can only be used via HTTP[[6]](#footnote-5) or HTTPS[[7]](#footnote-6) and therefore cannot be accessed by JavaScript. This reduces the threat of session cookie theft via cross site scripting (XSS).

## Secure cookie

A secure cookie can only be used via HTTPS. This ensures the cookie data is encrypted, reducing the exposure to cookie theft via eavesdropping.

## First and third-party cookie

First-party cookies are cookies set with the same domain (or its subdomain) as per the user’s browser's address bar. Third-party cookies are cookies set with domains different from the one shown on that address bar.

The web pages on the first domain may feature content from a third-party domain, e.g. a ‘pop-up’ advert. Privacy setting options in most modern browsers allow the blocking of third-party tracking cookies.

## Strictly necessary cookies

Strictly necessary cookies are essential to make a website work and enable features that users have specifically asked for. Without the use of cookies, these features of the website could not operate or some features may not be accessible.

## Performance cookies

Performance cookies collect anonymous information about users for the purpose of assessing the performance of a website. Common uses include well-known web analytics tools such as Google Analytics.

## Analytics cookies

These are used so that online services can collect information about how people access them, e.g. the number of users on a website, how long they visit.

This is also known as *‘*web audience measurement’ and is often completed in the background.

## Functional cookies

These are cookies that automatically remember choices that users have previously made in order to improve their experience next time they visit a website. An example is where users select their preferred settings and layout.

## Targeting or advertising cookies

These cookies are similar to performance cookies in that they collect information about users’ behaviour and the information is used at ‘individual user level’ to advertise products and services to users on the basis of the behavioural information collected.

Examples include Instagram or Facebook as they use these cookies as a sharing process between the site and the user’s online feeds.

# Legislation

## Legal requirement

The overarching legislation is the Privacy and Electronic Communications Regulations (PECR). This covers the use of cookies for accessing and storing information on a user’s equipment or mobile device.

PECR sits alongside the Data Protection Act (2018) and the GDPR and is explained by the ICO as follows:

*‘Essentially, if you are operating an online service, then the easiest way to look at the two laws is:*

* *If your online service stores information, or accesses information stored, on user devices then you should ensure that you comply with PECR first, including the requirements to provide information and obtain consent; and*
* *The GDPR applies to any processing of personal data outside of this storage or access.’*

[Regulation 6](https://www.legislation.gov.uk/uksi/2003/2426/regulation/6/made) of the PECR that details the confidentiality of communications decrees that users must provide clear and comprehensive information about the purposes of the storage of, or access to, that information and is given the opportunity to refuse the storage of or access to that information.

Further reading surrounding this legislation can be found at:

<https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/>

<https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/how-do-the-cookie-rules-relate-to-the-gdpr/>

# Compliance

## Organisation requirement

See extract from the ICO:

*“To comply with the information requirements of PECR, you need to make sure users will see clear information about cookies. In any case, doing so will increase levels of user awareness and control, and also assist in gaining valid consent”.*

Therefore, when accessing the website, Arch Health CIC has considered and complied with the ICO requirements to ensure that the following information is immediately obvious to the user:

* The location of the Cookie Policy is considered
* People are informed that the website uses cookies
* What the cookies are doing and why is explained
* The person’s consent to store a cookie on their device is obtained
* The fact that there is a separate Cookie Policy rather just use a section of the wider privacy policy is detailed
* Access to this Cookie Policy is provided and it will be accessible via a link within the consent mechanism. This is located at the top of the Arch Healthcare website.

## Location of the cookie policy

To ensure that users are aware that the Arch Healthcare website uses cookies and their subsequent information, the ICO advise as to the importance of the location of this within the website.

The ICO states:

*“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”*

As such, the Arch Healthcare website considers the following:

1. Formatting

The size of the link has been changed or a different font has been used to ensure that the link is distinguishable from *“normal text”* and other links.

1. Positioning

The link from the footer of the page has been moved to a more prominent area to enhance the visual impact.

1. Wording

The wording of the link has been considered to ensure it is more explanatory and Arch Health CIC has titled this ‘Cookie Policy’ opposed to *“Privacy Policy”* which is less obvious to the user.

## Cookie consent

To be compliant with cookies, valid consent needs to be specific, informed and freely given allowing the reader to fully understand that they are giving consent and this should be confirmed by requesting a positive action, such as by ticking a box or selecting a link.

Consent must be separate from other matters and cannot be bundled into terms and conditions or privacy notices.

Care should be taken when collecting sensitive personal details, including health data, and at Arch Health CIC we ensure that any privacy intrusive cookies have clear and specific consent. To ensure consent is freely given, users should have the options to enable or disable non-essential cookies and this should be made easy to carry out.

Further information on cookie consent can be sought within the main ICO document as detailed in <https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/>

## Data analytics

At Arch Health CIC our website uses analytics to monitor activity and we use Google Analytics.

These analytics collect information such as how many people visit the website, what pages they visit and how long they spend on them and how long they stay on the site for but do not allow any third party to use or share any data about a user.

By using cookies, data analysts understand how people browse and can help Arch Health CIC to identify areas that need to be improved, fix problems or better support users in finding the information they need during future visits.

More information can be found here: <https://developers.google.com/analytics/devguides/collection/analyticsjs/cookie-usage>

## Children and cookies

There are no additional rules surrounding children accessing online services and as at Section 7.3, Arch Health CIC has clear and comprehensive information about the use of cookies including consent.

At Arch Health CIC we may have children accessing services via the website so we will ensure that both the information provided and the consent mechanism we use are appropriate for children.

The ICO’s code of practice on age appropriate design has also been considered.

## Third-party cookies

Where Arch Health CIC has allowed third-parties to set cookies on its website, such as content from an advertising network or a streaming video service, both websites have a responsibility for ensuring users are clearly informed about their cookies and are required to obtain consent to ensure that the appropriate information is provided.

## Analytics cookies

In addition to that detailed at [Section 5.8](#_heading=h.3as4poj), there are first-party and third-party analytics cookies. Consent is ordinarily only necessary for first-party analytics cookies.

However, if Arch Health CIC processes personal data through the use of a third-party analytics service, the organisation will need to consider all data protection requirements. Measures will need to be established to highlight the use of analytics cookies and to obtain agreement to set these cookies.

## Cookie exemptions

There are exemptions to consent under PECR. These relate to the purpose for which the organisation stores information, or gains access to information stored, on user devices. Arch Health CIC will be clear with users about these purposes when providing information and requesting consent.

The exemptions in PECR relate to the purpose for which Arch Health CIC stores information, or gains access to information stored, on user devices. Arch Health CIC is required to be clear with users about these purposes when providing information and requesting consent.

The following list is not exhaustive, simply an overview of how PECR’s exemptions work for the different types of cookies and is based on a number of common purposes Arch Health CIC may use cookies for:

| **Activity** | **Likely to meet an exemption?** |
| --- | --- |
| User input | Yes, depending on purpose limitation |
| Authentication | Yes, depending on purpose limitation <https://wordpress.org/support/article/cookies/> |
| Security | Yes, depending on purpose limitation |
| Streaming content | Yes, depending on purpose limitation |
| Network management | Yes, depending on purpose limitation |
| User preference | Yes, depending on purpose limitation |
| Social media plugins | Consent required |
| Social media tracking | Consent required |
| Online advertising | Consent required |
| Cross-device tracking | Consent required |
| Analytics | Consent required |

Detailed information can be sought from the ICO’s [How do we comply with the cookie rules](https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/how-do-we-comply-with-the-cookie-rules/#comply18) document.

## Opting out

Most web browsers automatically accept cookies.

The user can decline accepting cookies and/or choose at any time to reject, block or delete cookies currently stored on their device. Users can find out how to do this for their particular browser by clicking “help” on the browser's menu or by visiting: [www.allaboutcookies.org](https://www.allaboutcookies.org/).

Details on how to opt out can be sought for both [Windows](https://support.microsoft.com/en-us/help/17442/windows-internet-explorer-delete-manage-cookies) or [iOS](https://support.apple.com/en-gb/guide/safari/sfri11471/mac) products, although the user should be advised that should they choose to block cookies they may not be able to access certain features of the Arch Healthcare website.

For mobile phones, information on how to reject or delete cookies on the browser can be sought in the user device manual.

## Withdrawal of consent

Once consent has been obtained, users or subscribers are able to withdraw consent at any time and there should be an option on the consent mechanism to allow users to withdraw their consent with the same ease that they gave it

As failure in meeting this will not be compliant with the GDPR’s consent, Arch Health CIC will provide information about how consent can be withdrawn, and how cookies that have already been set can be removed, within privacy or cookie policies.

The consequences of withdrawing consent will also be made clear, including the impact on the functionality of the website.

## How often is consent required?

Arch Health CIC will ensure that any first-time users to the website are provided with clear information about the cookies that are used and are given choices and controls about any that are non-essential.

All visitors may be required to ‘re-consent’ to cookie settings. However, this is dependent on the circumstances. Several factors will be involved, such as frequency of visits or updates of content or functionality.

Fresh consent would also be required when setting non-essential cookies from a new third party. The consent request needs to be specific and not include ambiguous or unclear references to ‘partners’ or ‘third parties.’ This would invalidate the consent as the user is not fully informed.

## Duration of cookie on device

The duration of the cookie will depend on the purpose of it.

Arch Health CIC ensures that the use of cookies is both limited to what is necessary to achieve the purpose and proportionate in relation to the intended outcome

## Cookie audit

Arch Health CIC will conduct a cookie audit and consider the following as detailed within the ICO guidance:

1. For cookies that are already present, identify those that are operating on or through the website, using a combination of browser-based tools and server-side code reviews
2. Confirm the purpose(s) of each of the cookies that is used (or intended to be used)
3. Confirm whether cookies are linked to other information held about users, such as user names, and whether the use of cookies also involves (or will involve) processing personal data
4. Identify what data each cookie holds or otherwise processes
5. Confirm the type of cookie, such as session or persistent
6. Distinguish between which cookies are strictly necessary
7. Ensure that the consent mechanism enables users to control the setting of all non-essential cookies
8. Determine the lifespans of any persistent cookies and whether these durations are justifiable for the stated purpose
9. Determine whether each cookie is a first or third-party cookie and, if it is a third-party cookie, who is setting it
10. Double check that the privacy information provides accurate and clear information about each cookie
11. Confirm what information is being shared with third parties and what users are told about this
12. Document findings and follow-up actions and build in an appropriate review period
13. The ICO advise that, during any audit, an opportunistic ‘clean up’ of existing web pages is undertaken to stop the use of any cookies that are unnecessary or those which have been superseded as the site has evolved.
14. The usage of any third-party content is likely to change over time so it is good practice to undertake regular reviews of cookie usage, as well as any third-party services the website includes that may set cookies.
15. Upon completion of any audit, the next consideration is the best methods for providing information and requesting consent

Re-audit is essential and at Arch Health CIC this will be conducted annually.

## Social media platforms

As Arch Health CIC uses social media platforms, it should also be noted that those platforms will also set cookies on users’ devices once they visit those pages.

Arch Health CIC will ensure that the privacy notice on the website includes references to our social media sites and how individuals are able to control the setting of any non-essential cookies once they visit that site.

## Non-compliance

In cases where organisations refuse or fail to comply voluntarily, the ICO has a range of options available for taking formal action when this is necessary.

Whilst GDPR gives the ICO enhanced powers, the enforcement regime for PECR remains that which was in effect under the previous Data Protection Act, that is, except where personal data is processed.

Where formal action is considered, for example, an organisation refuses to take steps to comply, or has been involved in a particularly privacy-intrusive use of cookies without advising the user or obtaining any consent, the use of formal regulatory powers would be considered in accordance with [ICO Regulatory Action Policy.](https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf)

# Summary

This policy has been raised to support staff at Arch Health CIC and provide clear information regarding cookies.

Should there be any uncertainties with the content of this policy then detailed advice can be sought within the linked ICO documents.

1. [Network contract Directed Enhanced Service (DES) Contract Specification 2020-21](https://www.england.nhs.uk/wp-content/uploads/2020/03/network-contract-des-specification-pcn-requirements-entitlements-2020-21.pdf) [↑](#footnote-ref-0)
2. [www.investopedia.com](https://www.investopedia.com/terms/d/data-analytics.asp) [↑](#footnote-ref-1)
3. [www.legislation.gov.uk](https://www.legislation.gov.uk/uksi/2003/2426/contents/made) [↑](#footnote-ref-2)
4. [www.legislation.gov.uk](https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted) [↑](#footnote-ref-3)
5. [www.gov.uk](https://www.gov.uk/government/publications/guide-to-the-general-data-protection-regulation) [↑](#footnote-ref-4)
6. <https://techterms.com/definition/http> [↑](#footnote-ref-5)
7. <https://techterms.com/definition/https> [↑](#footnote-ref-6)