



UK COLLEGE OF IT LTD.

COOKIE POLICY

Document status	Public Policy
Version	2.0
Effective date	11 August 2026
Review cycle	At least annually and whenever website technologies, suppliers or applicable requirements change
Policy owner	Data Protection / Digital Services
Applies to	UK College of IT website, digital services and other online services using cookies or similar storage/access technologies

1. Purpose and Scope

UK College of IT Ltd. (“UK College of IT”, “the College”, “we”, “us” or “our”) uses cookies and similar technologies on its website and digital services.

This Cookie Policy explains what cookies and similar technologies are, why they may be used, which categories may be used, how consent is obtained and how users can control their preferences.

The Policy should be read together with the College’s Privacy Policy and Terms & Conditions.

The term “cookies” in this Policy is used broadly where appropriate to include similar technologies that store information on, or access information from, a user’s device. The ICO’s final April 2026 guidance expressly covers cookies, tracking pixels, device fingerprinting and other storage and access technologies.

2. What Are Cookies?

A cookie is a small file or data item placed on a computer, smartphone, tablet or other device when a website is accessed. Cookies can allow a website to remember information, maintain a session, support security or understand how a service is used.

Cookies may be:

- session cookies, which normally expire when the browsing session ends; or

- persistent cookies, which remain on the device for a defined period or until deleted.

Cookies may also be first-party or third-party depending on which organisation places or accesses them.

3. Similar Technologies

Cookie rules may also apply to technologies that do not use traditional cookies but store or access information on a user's device.

Depending on how the College's website is configured, this may include local storage, pixels, tags, scripts, software development kits, device identifiers or similar technologies.

The College will assess relevant technologies according to their actual function rather than relying solely on the technical label used by a supplier.

4. UK Legal Framework

UK College of IT operates its website in accordance with applicable UK privacy and electronic-communications requirements.

Under the Privacy and Electronic Communications Regulations (PECR), users generally need to be informed about storage/access technologies and consent must be obtained before using technologies that are not covered by an applicable exemption.

The ICO's current guidance states that organisations must tell users that cookies are present, explain what they do and why, and obtain consent unless an exemption applies. The ICO also states that the same rules can apply to other technologies that store or access information on a user's device.

Where cookies or similar technologies involve personal data, applicable UK GDPR requirements must also be considered.

5. Strictly Necessary Technologies

Some cookies may be strictly necessary to provide a service requested by the user or to enable essential website functionality.

Examples may include cookies required for:

- security and fraud prevention;
- authentication or secure access;
- maintaining a user session;
- load balancing;
- remembering essential technical settings necessary to deliver a requested service; or
- other functions that genuinely cannot be provided without the relevant technology.

The ICO distinguishes technologies that are genuinely necessary from technologies that are merely convenient or useful. A technology does not become exempt simply because it benefits the website operator.

Where an exemption applies, the College will still provide clear information about the relevant technology where appropriate.

6. Analytics and Performance Technologies

Analytics technologies may help the College understand how visitors use the website, identify technical problems, measure engagement and improve website performance.

Examples may include information about pages viewed, approximate usage patterns, device/browser information, referral sources or interaction with website features.

Unless an applicable exemption clearly applies, analytics technologies will not be activated until the required consent has been obtained.

Analytics data should be configured to minimise unnecessary personal information and should be reviewed periodically.

7. Functional and Preference Technologies

Functional technologies may remember choices made by a visitor, such as language, display preferences or other settings.

Some preference technologies may qualify for an applicable exemption depending on their precise purpose. Others may require consent.

The College will assess each technology according to whether it is genuinely necessary for a service requested by the user rather than automatically classifying all functionality cookies as essential.

8. Marketing and Advertising Technologies

Where the College uses marketing, advertising, retargeting or conversion-measurement technologies, these may collect information about website interactions or link website activity to marketing campaigns.

Such technologies will only be activated where the required consent has been obtained or another applicable legal basis/exemption clearly permits their use.

The College will not describe a marketing or advertising technology as “necessary” merely because it helps measure or promote the College’s services.

The ICO’s 2026 guidance includes specific provisions concerning online advertising and expectations for meaningful user control.

9. First-Party and Third-Party Technologies

First-party cookies are generally placed by the website domain operated by UK College of IT.

Third-party technologies may be placed or accessed by another organisation whose service is integrated into the website.

Third-party services may include analytics, video, payment, social-media, security, embedded content, customer-support or advertising providers.

Third-party providers may process information under their own privacy terms. The College will take reasonable steps to identify relevant third-party technologies and provide appropriate information to users.

10. Cookie Categories

The College's cookie-consent mechanism should, where applicable, distinguish at least the following categories:

- Strictly Necessary;
- Preferences / Functional;
- Analytics / Performance; and
- Marketing / Advertising.

The live cookie inventory should determine which categories actually exist on the website. Categories must not be used merely as labels; they should reflect the real purpose of each technology.

11. Consent Requirements

Where consent is required, it must be actively and clearly given.

The College will not rely on silence, continued browsing, pre-ticked boxes or similar passive behaviour as consent where the law requires active consent.

The ICO's current guidance states that consent must be actively and clearly given and that organisations should implement a mechanism allowing users to control non-essential cookies.

Where a user rejects non-essential technologies, the website should respect that choice and prevent those technologies from being activated, subject to any lawful technical limitations that are clearly explained.

12. Cookie Banner and Consent Management

Where non-essential cookies are used, the College should provide a clear cookie banner or consent-management mechanism when a user first visits the relevant service.

The consent mechanism should provide meaningful choices and should not make rejection substantially more difficult than acceptance.

Users should be able to:

- accept relevant non-essential categories;
- reject non-essential categories where applicable;
- manage individual categories or preferences; and
- change their choices later.

The consent mechanism should not activate non-essential technologies before the required consent is obtained.

13. Rejecting Non-Essential Cookies

The College will provide an accessible method for refusing non-essential cookies.

Rejecting non-essential cookies should not prevent a user from accessing the basic website unless a particular service genuinely requires the relevant technology. Where functionality is affected, the reason should be clear.

14. Withdrawal and Changing Consent

Where consent has been obtained, users should be able to withdraw or change their preferences without unreasonable difficulty.

The website should provide an accessible “Cookie Settings”, “Privacy Settings” or equivalent mechanism that can be accessed after the initial consent decision.

Withdrawal of consent should not affect the lawfulness of processing or storage/access that occurred before withdrawal.

15. Consent Records

Where consent is required, the College should maintain an appropriate record of the consent decision.

Records may include the date/time, consent status, categories selected and relevant consent-management information.

The ICO recommends keeping records of cookie consent for an appropriate period and documenting cookie use and review.

16. Cookie Duration

Cookies may be session-based or persistent.

The College should ensure that persistent cookies have an appropriate duration for their stated purpose and are not retained longer than reasonably necessary.

The live cookie register should identify the duration of each cookie or technology.

17. Cookie Register

The College should maintain an internal, up-to-date Cookie and Storage/Access Technology Register.

For each technology, the register should identify, where applicable:

- name;
- provider;
- domain;
- first-party or third-party status;
- technology type;
- purpose;
- category;
- duration;
- data or identifiers collected;
- whether personal data is involved;
- whether consent is required;
- consent mechanism;
- destination/recipient information;
- applicable privacy documentation; and
- date last reviewed.

18. Website Scanning and Verification

The College should periodically scan or otherwise inspect the website to identify cookies, scripts, pixels and other storage/access technologies.

Testing should be performed before major website launches and following significant changes to analytics, advertising, consent-management, forms, embedded media or other third-party services.

Automated scanning is useful but should be supplemented by manual review because some technologies may be loaded conditionally or through scripts.

19. Third-Party Supplier Management

Before integrating a third-party service that may place cookies or access device information, the College should consider:

- the purpose of the technology;
- whether consent is required;
- what information is collected;
- where information is processed;
- the supplier's privacy documentation;
- retention periods;
- security measures;
- whether a data-processing agreement or other contractual arrangement is required; and
- whether the service creates an accessibility or user-experience issue.

20. International Transfers

Where third-party cookie or tracking providers process personal information outside the United Kingdom, the College will consider applicable UK data-protection requirements concerning international transfers.

Where required, an appropriate transfer mechanism and safeguards will be implemented.

21. Cookies and Personal Data

Not every cookie is necessarily personal data. However, identifiers, online identifiers, IP addresses and information linked to an identifiable person may constitute personal data depending on the circumstances.

Where cookie or similar-technology information constitutes personal data, the College will process it in accordance with applicable data-protection law and the Privacy Policy.

22. Security

The College will take reasonable technical and organisational measures to prevent unauthorised access to cookie-consent records and associated personal information.

Third-party scripts should be reviewed proportionately for security and privacy risks.

23. Accessibility of Cookie Controls

Cookie banners and preference centres should themselves be accessible.

The College aims to ensure that cookie controls can be used with keyboard navigation, assistive technology and appropriate text resizing, and that controls have meaningful labels and understandable instructions.

Accessibility of the consent mechanism forms part of the College's wider Accessibility Statement.

24. Children and Young People

UK College of IT's professional programmes are generally designed for adult learners unless a specific programme states otherwise.

If the website or a particular service is intentionally directed at children or young people, the College will apply appropriate age-related privacy and consent considerations.

25. Social Media and Embedded Content

Embedded social-media content, video players, maps, forms or other external services may use cookies or similar technologies.

Where an embedded service requires consent, the College should prevent the service from loading in a way that sets non-essential technologies until the relevant choice has been made, where technically practicable.

Where possible, privacy-enhanced or no-tracking configuration options should be considered.

26. Payment and Security Services

Payment or authentication services may use technologies that are necessary for secure transactions or access.

Where such technologies are strictly necessary for a service requested by the user, an applicable exemption may apply. Other tracking or marketing technologies operated by the same provider may still require separate consent.

27. Managing Cookies Through a Browser

Users can also control or delete cookies through their browser settings.

Browser controls may allow users to block cookies, delete stored cookies or receive notifications when cookies are being set.

Blocking all cookies may affect the operation of some websites and services, particularly essential authentication or security functions.

28. Changes to Cookie Use

The College may introduce new technologies, remove existing technologies or change third-party suppliers.

If a material change affects the categories of non-essential technologies or the purposes for which they are used, the College will update this Policy and, where required, seek fresh consent.

The ICO notes that fresh consent may be required where the use of cookies changes over time.

29. Policy Review

This Policy will be reviewed at least annually and whenever there is a significant change to the website, cookie inventory, tracking technologies, third-party providers or applicable law.

The College's 2026 review should take account of the ICO's final Storage and Access Technologies guidance published on 29 April 2026.

30. Contact

Privacy / Data Protection: info@ukcollegeofit.uk

Cookie enquiries: info@ukcollegeofit.uk

General enquiries: info@ukcollegeofit.uk

Registered office: Suite 3.2 Litchurch Plaza, Litchurch Lane, Derby, DE24 8AA

Appendix A – Cookie Register Template

Name	Provider	Type	Category	Purpose	Duration	Third party?	Consent?	Last reviewed
------	----------	------	----------	---------	----------	--------------	----------	---------------

Appendix B – Cookie Compliance Checklist

- ☐ All cookies and similar technologies have been identified
- ☐ First-party and third-party technologies have been distinguished
- ☐ Session and persistent technologies have been identified
- ☐ Purpose of each technology has been documented
- ☐ Strictly necessary technologies have been assessed individually
- ☐ Non-essential technologies are blocked before required consent
- ☐ Accept and reject choices are meaningfully available
- ☐ Preference management is accessible after the initial choice
- ☐ Consent records are retained appropriately
- ☐ Cookie duration has been reviewed
- ☐ Third-party suppliers have been reviewed
- ☐ International transfers have been considered where applicable
- ☐ Privacy notices accurately describe relevant processing
- ☐ Cookie banner and preference centre are accessible
- ☐ Website scan/manual review completed
- ☐ Changes are documented and policy updated when necessary

Appendix C – Recommended Website Cookie Banner Wording

“We use strictly necessary cookies to operate and secure our website. With your permission, we may also use analytics, preference and marketing technologies to understand website use, improve our services and measure communications. You can accept, reject or manage non-essential cookies. You can change your preferences at any time through Cookie Settings. For more information, please see our Cookie Policy and Privacy Policy.”

Appendix D – Related Policies

- Privacy Policy
- Accessibility Statement
- Terms & Conditions
- Data Protection & Data Retention Policy
- Quality Assurance Policy