
Title:	Guidance on the Privacy and Electronic Communications (EC Directive) Regulations
Status:	Released

1. Purpose

This guidance on the Privacy and Electronic Communications (EC Directive) Regulations intends to support University staff and students in understanding the remit of the Regulations and in implementing appropriate controls to assure compliance to the Regulations.

2. Scope and Responsibilities

2.1. The guidelines applies to all websites:

- controlled by the University
- managed on behalf of the University
- connected to clubs and societies associated with the University

2.2. Responsibility for compliance with the Regulations lies with University staff and students managing, procuring or overseeing any website identified in section 2.1 above

3. The Change in Law

The Privacy and Electronic Communications (EC Directive) Regulations were implemented into UK Law on 25 May 2011. The government gave organisations until 25 May 2012 to implement this new law, which is fast approaching.

Under the old law it was adequate to tell website users about cookies and then give them the option to 'opt out' of the use of cookies.

3.1. What is a Cookie?

A cookie is a piece of information in the form of a very small text file that is placed on an internet user's hard drive. It is generated by a web page server, which is basically the computer that operates a web site. The information the cookie contains is set by the server and it can be used by that server whenever the user visits the site. A cookie can be thought of as an internet user's identification card, which tell a web site when the user has returned and can store personal information about the user.

Therefore compliance usually involved putting information about cookies in privacy policies/website terms and giving users the possibility of 'opting out'.

3.2. Consent

However, under the new law cookies (and other similar technologies) can only be used where the user has been provided with information and has given their consent. Therefore, the fundamental change is that inaction by the user in failing to opt out of cookies is no longer enough, the web **users must take affirmative action to give consent to the use of cookies.**

Implied consent is a valid form of consent and can be used in the context of compliance with the revised rules on cookies. However, the following expectations should be taken into account:

- If you are relying on implied consent you need to be satisfied that your users understand that their actions will result in cookies being set. Without this understanding you do not have their informed consent.
- You should not rely on the fact that users might have read a privacy policy that is perhaps hard to find or difficult to understand.
- In some circumstances, for example where you are collecting sensitive personal data such as health information, you might feel that explicit consent is more appropriate.

4. **Exception – ‘Strictly Necessary’**

There is an exception to the requirement to obtain consent if the use of the cookie (or other technology) is ‘strictly necessary’. This is a very narrow exception and only likely to apply to a small range of situations, such as when a cookie is used to remember the goods in a basket/checkout, or if a cookie is required for legal compliance, or if a cookie is required to distribute a website’s workload across numerous computers.

5. **Intention behind the law**

The Information Commissioner’s Office (ICO) have surmised that the aim of the law is not to restrict the use of particular technologies as such, but to prevent information being stored on people’s computers, and used to recognise them via the device they are using, without their knowledge and agreement.

Therefore, in order to comply with the law, the University and any associated web providers or website owners must:

- 1. Tell people that the cookies are there***
- 2. Explain what the cookies are doing; AND***
- 3. Obtain their consent to store the cookies***

6. What practical steps will the University be taking towards compliance?

6.1. On Sitebuilder sites

IT Services have identified the following cookies in operation on the University provided web platform 'Sitebuilder' and has published this information on the website':

- Only first party cookies, i.e. those implemented by University website owners, are in use
- The University sitebuilder pages use Google Analytics and is not required to provide a University-specific opt-out for that, since Google provide an opt-out which works everywhere that Google Analytics is in use (<http://tools.google.com/dlpage/gaoptout>)
- Other cookies are deployed on pages requiring Single Sign-On and consent will be gathered for these cookies on Single Sign-On pages and when specific presentational preferences, such as 'display text only' or 'set this page as my homepage', are selected by signed-in users.

6.2. On other University websites (non-Sitebuilder and third party managed sites)

In line with the guidance provided by the Information Commissioner's Office (ICO), departments or activities running non-Sitebuilder sites and/or third party provided websites must carry out the following steps towards compliance:

6.2.1. *Cookie Audit*

Check what type of cookies and similar technologies you use and how you use them.

Department web owners or third party website providers should carry out an audit of the website(s) to see what cookies are being used and why. It should investigate:

- o What cookies are operating
- o The purpose of the cookies
- o Whether the cookies link to other information held about users
- o What data the cookies hold
- o Whether they are session cookies or persistent cookies. If it is persistent how long does it last?
- o Whether they are first party or third party cookies. If it is a third party cookie who is setting it?

Some cookies may be strictly necessary and might not need consent – although this is a very narrow exception (see section 2 above) so may not apply to the website(s).

This will be a good opportunity to clean up any web pages and stop using any cookies that are unnecessary.

6.2.2. *Assess how intrusive the use of cookies is*

The Regulations cover all types of cookies. However, the intention behind the law is to add to the level of protection afforded to the privacy of internet users. Therefore the more intrusive your use of cookies is the more priority you will need to give to either changing these practices or gaining meaningful consent. It is cookies that are used for behavioural advertising that are of most concern, rather than just the use of analytical cookies.

6.2.3. *Decide what solution is best to provide the information and gain consent?*

(A) Tell people that the cookies are there

- You must provide clear and comprehensive information about the cookies you are using.
- The information must be easily accessible to website users - so not hidden away in privacy policies or website terms that are hard to find. The ICO have suggested flagging up the cookie information by having a link to 'Privacy Policy and Cookies' or 'New Cookie Information' on your website.

(B) Explain what the cookies are doing

- The information should be sufficiently full and intelligible to explain to users what the cookies are and help them understand the potential consequences of allowing the cookies should they wish to do so.
- This could be in the form of a table setting out the type of cookie e.g. 'Performance Cookie', 'Functionality Cookie', 'Targeting Cookie' and an explanation of each. The International Chamber of Commerce is currently producing a guide which will contain examples of the types of descriptions websites could give to explain the different types of cookies and their uses.

(C) Obtain their consent to store the cookies

There are various methods which can be used to gain consent for the use of cookies (see Section 3 above). Neither the Regulations, the University or the ICO have given a prescriptive way of gaining consent. Examples include:

- **Pop ups and similar techniques** e.g. a light box that appears over the whole screen when someone logs in. For an example see <http://www.allaboutcookies.org/>.
- **Website footer or header bars** – as you noted the ICO was using a prominent header on their website. However, reports suggest that only 10% of people were actually ticking this box so it may not be the most effective technique.
- **Terms of Use** – if there is an online registration process then this could be used to ask users to sign up to the use of cookies at the same time – the information regarding cookies would need to be prominent and clear.
- **Settings/Feature led consent** – consent for cookie use could be linked in with other decisions the user may have to make about their use of the website – e.g. the language, or if they are about to watch a video.

These types of consent mechanisms could then link to the comprehensive Privacy Policy which would set out the cookie information.

It is important to ensure that any form of consent mechanism also complies with Accessibility obligations – i.e. that the cookie consent boxes can be read by screen readers etc.

It is important to find a balance between gaining consent without ruining the website experience for the users.

7. Connected Websites

The ICO have suggested that an organisation with several connected websites could in theory obtain consent for cookies set on each site in one place, for example when the user logged in on one site. In order for this consent to be valid it would have to be absolutely clear which websites the cookies in question were set on and very clear what the use of the cookies was for. This may be useful for departments or activities which have a number of connected websites. However, any sites that can be accessed independently e.g. not via the University of Warwick homepage in case the user has not visited the main University website first. Similarly, if a department or activity redirects users to a site managed by a third party i.e. not controlled by the University, additional consent for any cookies in use on this site would need to be sought and users should be informed that they are being directed away from the University of Warwick site.

8. Contacts

8.1. IT Services can provide further advice on the technical aspects of compliance to the Regulations. Contact the IT Services Service Desk (helpdesk@warwick.ac.uk).

8.2. The Deputy Registrar's Office can advise on the wording for Privacy Policies or consent gathering mechanisms (see section 7.2.3 above).

Document History

22	May	2012	(J. Findlay)	Began first draft
30	May	2012	(J. Findlay)	Updated to clarify ICO guidance around implied consent (v1)
10	August	2012	(J. Findlay)	Released (v1.1)

The official version of this document will be maintained online. Before referring to any printed copies please ensure they are up to date.
--