

Report to:	SMT
Report by:	Erin Gray (Head of Policy & Information)
Meeting Date:	12 May 2021
Subject/ Title: (and VC no)	Website Cookies (VC 144142)
Attached Papers (title and VC no)	2021 01 06 FYI Observation note on the Commissioner's website cookies (VC 143911)

Purpose of report

1. To seek Senior Management Team (SMT) approval to update the Scottish Information Commissioner's website cookie practice and banner.

Recommendation and actions

2. It is recommended that the SMT:
 - (i) Note the content of this report
 - (ii) Agree the recommendations and which cookies need consent and which do not as set out in paragraph 17 and the subsequent table
 - (iii) Agree to publish the report and observation note in line with the Publication section at the end of this report.

Executive summary

Background

3. As described by the ICO, a cookie is: "a small text file that is downloaded onto 'terminal equipment' (eg a computer or smartphone) when the user accesses a website. It allows the website to recognise that user's device and store some information about the user's preferences or past actions"¹. Cookies are used by many websites and can do a number of things, for example remembering preferences, recording what you have selected on the website and counting the number of people looking at a website.
4. The rules on cookies are covered by the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR). PECR also covers the use of similar technologies for storing or accessing information, such as "flash cookies" and device fingerprinting. The ICO is responsible for enforcing these rules.
5. Cookies are placed on users' devices when they use the Scottish Information Commissioner's website www.itspublicknowledge.info. They allow the website to recognise the user's device between visits to improve the user's experience of using the site, as well as to provide information to us, as the owners of the website.

¹ <https://ico.org.uk/for-organisations/guide-to-pecr/cookies-and-similar-technologies/>

6. Cookies currently on the Commissioner's website² are:
- (a) **__utm*** - Google Analytics cookie
 - (b) **Personalization_id** – Twitter personalisation cookie
 - (c) **Style** - Used to keep a consistent text size for users who have selected a smaller or larger text size
 - (d) **Content** - Created when the cookie banner at the top of the page is read and closed, and is used to stop this message from appearing on other pages after the message has been closed.
 - (e) **SIC** - A user session cookie, used for keeping a user logged in as they navigate around the website.
 - (f) **Editor_PinTBActive** – Added only for Commissioner's staff who are website editors, used to indicate if the page editor is pinned in place or not.
 - (g) **ASP.NET_SessionID** - used to identify the user's session on the server and keep it anonymous.
7. The use of cookies on the Commissioner's website must comply with the Data Protection Act 2018, the UK GDPR and PECR. Our website needs to be updated in order to comply with the relevant legal requirements.
8. The ICO has produced detailed guidance on what is required³. Consent is required for cookies unless they are subject to an exemption. There are two exemptions, only one of which may be relevant here: the "strictly necessary" exemption, and this is available only where the cookies in question are in place in relation to an 'information society service'.


Advice sought

9. An observation note, setting out a suggested approach to our cookie practice, was provided by FYI in January 2021. That note is attached for reference. The primary purpose was to establish which cookies required consent and which were subject to the strictly necessary exemption. The note set out that consent could be sought for cookies a), b) and c) (if cookie b) is still felt to be required), and that the "strictly necessary" exemption be used for the remainder.
10. The note considers the definition of "information society services" as set out in article 2(a) of the E-Commerce Directive and article 1(2) of the Technical Standards and Regulations. It sets out that while this term is defined in these as relating to services normally provided for remuneration, the ICO does not make any distinction between commercial online services and those provided by the public sector in their guidance or practice, and there is no policy or case law regarding how this definition relates to online services provided by the public sector which are not normally provided for remuneration. In practice, the ICO itself uses the strictly necessary exemption (meaning it considers its website as being an information society service) and FYI state in their note that they are not aware of any authorities which do

² Where cookies are used on the website in relation to videos, the approach in use by the ICO is followed.

³ See <https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/> and <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/>

consider their websites as not constituting an information society service and so which do not use the strictly necessary exemption where appropriate.

11. Following receipt of the observation note internal advice was provided which stressed that:
 - (i) The Commissioner's website should not be classed as an information society service solely in order to utilise the "strictly necessary" exemption
 - (ii) The main definition of "information society services" is that provided in article 2(a) of the E-Commerce Directive and article 1(2) of the Technical Standards and Regulations, and this relates to services normally provided for remuneration
 - (iii) If it was determined that the Commissioner's website was an information society service, any other relevant requirements for such services should be considered and complied with (such as the Age Appropriate Design Code).
12. Internal discussion in response to this advice further highlighted that while there are challenges in relation to the definition of information society services as applied to public sector websites not provided for remuneration, the only alternative with the Commissioner's current website would be to ask for consent – and given the essential nature of some of the cookies in question (such as cookie e) 'SIC' which is required for public authorities to submit statistics returns) and the nature of the relationship between the Commissioner's office and those using this function, consent may not be an appropriate mechanism to use.
13. Further research has since also highlighted that ICO guidance on the Age Appropriate Design Code ("the Code") sets out that public authority services provided via a website may be both information society services as relevant to PECR, but not 'normally provided for remuneration', and therefore such a website may be an information society service, but would not be subject to the Code.
14. It is set out in s123 of the DPA 2018 that the Code applies to "relevant information society services which are likely to be accessed by children". The ICO guidance on the Code⁴ sets out that some services provided by public authorities are not classed as "relevant" information society services in this context: "If you are a public authority which provides an online public service then, as long as the type of service you offer is not typically provided on a commercial basis your service is not a relevant information society service. This is because it is not a service 'normally provided for remuneration'."
15. Further, as subsequently shared via internal advice, section 123 simply defines "relevant information society services" as those involving "processing of personal data to which the GDPR applies".
16. 

⁴ <https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/services-covered-by-this-code/#code3>

Conclusion

17. Following consideration of the above, I propose that:

- (i) The Commissioner’s website be considered as an information society service
- (ii) Relevant requirements be researched and complied with as a result (this does not include the Age Appropriate Design Code, as set out in paragraph 13 above)
- (iii) The “strictly necessary” exemption be applied to cookies d through g in the table below (since they are essential for the utilisation of the website, from the user’s perspective, as well as for the Commissioner)
- (iv) The Commissioner’s website contractor be asked to update cookie placement on our website to reflect the detail set out in the above table, and to create a new cookie banner (which will link to the cookies page on our website) to provide site users with correct, compliant and up to date information and choices in relation to the placement of cookies on their devices
- (v) The Commissioner’s Privacy Notice and web page providing detail on cookie usage are updated to reflect the above changes
- (vi) The possibility of cookie-free analytics solutions are explored in development of any future website for the Commissioner

	Cookie name	What cookie does / business need	Approach recommended
a	__utm*	<p>Google Analytics cookie, used to track a user’s visits to the website (pages visited, files downloaded etc). These are created and controlled by Google Analytics, and presented in aggregate form to monitor website traffic and use. This supports the Commissioner’s team to make ongoing improvements to the site and measure use and problems with it.</p> <p>At the recommendation of the Scottish Government Digital First team the Commissioner uses AnonymizeIP code to ensure only anonymised versions of users IP addresses are used. Google cannot share or use information on specific individual users as a result.</p>	<p>Consent required.</p> <p>Build into new cookie banner so that consent is obtained for this cookie before it is placed on user’s device.</p> <p>As this is a third party cookie, clearly and specifically name who the third party is and explain what they will do with the information.</p>
b	Personalization_id	<p>Put in place by Twitter to allow personalisation of twitter feeds.</p> <p>No longer required.</p>	<p>Remove the cookie and seek assurance from the website provider that it is not loaded on any user’s device anymore.</p>
c	Style	<p>Used to keep a consistent text size for users who have selected a smaller or larger text size using the "AAA - Text Size up Down" links.</p>	<p>Consent required but can be obtained via ‘settings led consent’.</p>

			Implement a settings dialogue which clearly explains the use of cookies before the user selects a setting. Explain to user that by allowing their choice to be remembered they are giving consent to set the cookie.
d	Content	Created when the cookie banner at the top of the page is read and closed, and is used to stop this message from appearing on other pages after the message has been closed.	<p>No consent required.</p> <p>Necessary to the function and to ensure (in compliance with UK GDPR) that consent requests are not unnecessarily disruptive.</p> <p>Explain to user that this cookie is being used and is necessary for the functioning of the site, and also that their computer knows they have seen it and not to show it again, as well as storing it in settings.</p>
e	SIC	<p>A user session cookie, used for keeping a user logged in as they navigate around the website.</p> <p>NOTE: this is only created when a user logs in to the website (this is not restricted to Commissioner staff).</p>	<p>No consent required.</p> <p>Explain to user that this cookie is being used and is necessary for the functioning of the site.</p>
f	Editor_Pin TBAActive	Added only for Commissioner's staff who are website editors, used to indicate if the page editor is pinned in place or not.	<p>No consent required.</p> <p>Explain to user that this cookie is being used (for Commissioner staff who are web editors only) and is necessary for the functioning of the site.</p>
g	ASP.NET_SessionID	Used to identify the user's session on the server. Used to maintain an anonymised user session by the server.	<p>No consent required.</p> <p>Explain to user that this cookie is being used and is necessary for the functioning of the site. Also that this information is stored on the web server via a unique identifier, which is stored in the cookie. However, if no information is generated during the session, no cookie is sent to the browser so this cookie is only created when required. The information expires at the end of the session as defined by the configuration of the application, usually 20 minutes.</p>

Risk impact

18. Taking the actions recommended in this report will mitigate the risk of non-compliance with the relevant legislative requirements. The decisions and approach set out in this paper will also mitigate strategic and operational risks regarding ensuring the Commissioner's website is maintained as a key communications tool in order to effectively engage with stakeholders, and will support efforts to ensure the Commissioner demonstrates robust and defensible decisions.

Equalities impact

19. No equalities impact has been identified in relation to the proposal, though it is noted that cookie c above ("Style") is required in order to meet website accessibility requirements.

Privacy impact

20. This work is required in order to comply with privacy requirements (the DPA 2018, UK GDPR and PECR).
21. The Commissioner's Privacy Notice should be updated to reflect the points set out in the table above.

Resources impact

22. If the approach recommended in this paper is approved, the work to create a cookie banner will be carried out by our current website provider (we cannot complete it in-house).
23. While no budget was assigned to cover this work at the outset of the year, it is anticipated that website maintenance resource assigned during the course of the year will be sufficient to deliver the required outputs.

Operational/ strategic plan impact

24. The action proposed in this Committee Report is required to ensure the website is maintained and up to date, which is in line with activity set out in the Commissioner's operational and strategic plans.

Records management impact (including any key documents actions)

25. No key document actions or records management impact has been identified.

Consultation and Communication

26. The GDPR Working Party has been consulted on a draft of this report. Members have been made aware of the observation note and internal legal advice has also been provided.

Publication

27. This CR should be published, subject to the redaction of the legal advice in paragraph 16 (section 30(c) of Freedom of Information (Scotland) Act 2002 (FOISA)).

28. The attached observation note should be published subject to the redaction of third party personal data (section 38(1)(b) of FOISA).