

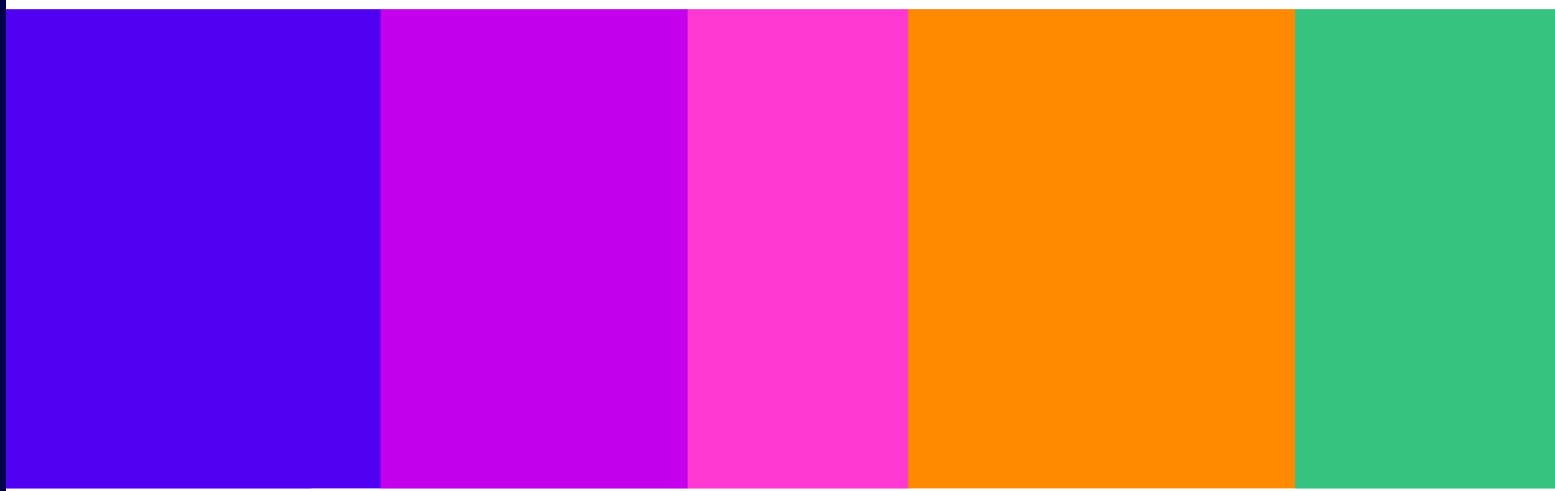
A Safer Life Online for Women and Girls

Call for evidence

Published: 9 September 2026

Closing date for responses: 4 November 2026

For more information on this publication, please visit [ofcom.org.uk](https://www.ofcom.org.uk)



Contents

Section

1. Overview.....	3
2. Women and girls' online safety.....	5
3. Evidence we are seeking	9
A1. Responding to this call for evidence	11
A2. Call for evidence coversheet	14

1. Overview

Women and girls' online safety is a priority for Ofcom, and we want to understand how their experiences have changed since our Guidance was published in November 2025.

This Call for Evidence invites interested stakeholders to provide Ofcom with evidence and insights about women and girls' online experiences since the publication of our Guidance in November 2025. We are particularly interested in understanding what, if any, changes women and girls have experienced online during this period.

- 1.1 Ofcom is the United Kingdom's (UK) communications regulator, overseeing sectors including telecommunications, post, broadcast TV and radio. Under the Online Safety Act 2023 ("the Act"), Ofcom is also the regulator for online safety in the UK.
- 1.2 Under the Act, Ofcom's job is to make online services safer for the people who use them. We do this by making sure tech companies have effective systems and processes in place to protect users from illegal content and content that is harmful to children, and to address harms that disproportionately affect women and girls online.
- 1.3 In November 2025, Ofcom published guidance for online services providers ("service providers") titled: [A Safer Life Online for Women and Girls](#) ("the Guidance"). The Guidance sets out how service providers can tackle online gender-based harms that disproportionately affect women and girls, including image-based sexual abuse, misogynistic abuse and sexual violence, stalking and coercive control, and pile-ons and coordinated harassment.
- 1.4 The Guidance brings together relevant measures outlined in our Codes of Practice ("Codes")¹ and risk assessment guidance² to support service providers in complying with enforceable duties under the Act, alongside additional good practice steps to strengthen protections for women, girls and others affected by these harms. Since the publication of the Guidance, Ofcom has continued to prioritise women and girls' online safety and drive improvements (see Section 2 for more detail on our work).
- 1.5 Ofcom is committed to monitoring how service providers choose to protect their users, including women and girls, and how they are implementing the good practice steps set out in the Guidance.
- 1.6 As part of this commitment, we will publish a report in Q2 2027 to shine a light on what service providers are doing – or not doing – to create a safer life online for women and girls since we published the Guidance. The report will highlight areas of progress as well as where we think further improvements are needed. It will also provide a snapshot of whether women and girls' experiences of the online gender-based harms covered by the Guidance have changed since November 2025, based on the information available to us at the time.

¹ Our [Illegal Content and Protection of Children Codes](#) set out measures recommended by Ofcom for service providers to comply with their safety duties and other duties specified under the Act.

² [Illegal content risk assessments](#) and [children's risk assessments](#)

- 1.7 Questions for stakeholders are listed in Section 3 of this document. Through this Call for Evidence, we are seeking evidence in the form of research, data, and insights, **for the period from November 2025 to date**, on the following:
- > evidence of changes in the prevalence, incidence, nature or severity of the online gender-based harms covered in the Guidance,
 - > evidence of how women and girls' experiences of these online gender-based harms have changed, and
 - > evidence of actions taken by services, including implementation of the good practice steps or alternative approaches, and the impact these actions have had on users' experiences.
- 1.8 We welcome responses from interested stakeholders, especially from civil society, researchers, and academia. This Call for Evidence is open for 8 weeks and will close at 5pm on 4 November 2026.
- 1.9 We are also currently engaging with a range of service providers to understand how they have implemented our Guidance since November 2025. While we are particularly interested in hearing from civil society, researchers, and academia in responses to this Call for Evidence, we also welcome submissions from regulated services. All responses received will be used to inform our report.
- 1.10 Stakeholders only need to respond to questions that are relevant to them. If evidence has already been provided to Ofcom, it does not need to be submitted again.
- 1.11 **Responses can be submitted via [our online form](#) or to womenandgirlscfe@ofcom.org.uk. This Call for Evidence closes on 4 November 2026.**
- 1.12 Our report will also be informed by our programme of research and engagement with those with lived experiences of online harms. After we have considered the evidence from all available sources, we will then prepare our report. We will publish the report on Ofcom's website.

2. Women and girls' online safety

- 2.1 The evidence and research that fed into our [Guidance](#) showed that women and girls face unique and serious risks online. They are more likely to have intimate images depicting them, including sexualised imagery shared without their consent; be targeted by co-ordinated harassment; and be targeted by stalking and coercive control.³ Some service features, including the ways content is amplified and monetised, can also push men and boys towards content that normalises, glorifies, and encourages misogynistic abuse and sexual violence.⁴
- 2.2 **Improving women and girls' online safety therefore is a priority for Ofcom.** Through our implementation of the Act, our Codes and guidance for services, and our ongoing efforts to drive compliance and stronger protections, we continue to work to address the harms that disproportionately affect women and girls online.

Duties on services

- 2.3 There is a range of online gender-based harms women and girls can experience which are covered by the Act. These include illegal content and activity, as well as content harmful to children under the Act.
- 2.4 The Act places clear requirements on service providers⁵ to address illegal content, which includes online gender-based harms such as intimate image abuse, stalking and controlling or coercive behaviour. The Act also requires service providers to protect children from content harmful to them, including certain aspects of online gender-based harms such as abuse and hate content and violent content, and to prevent them from accessing pornographic content.
- 2.5 Ofcom has published [Illegal content Codes](#) and [Illegal content Risk Assessment Guidance](#) and [Protection of Children Codes](#) and [Children's Risk Assessment Guidance](#), setting out how we expect service providers to tackle illegal content and to protect children.

A Safer Life Online: Ofcom's Guidance

- 2.6 Section 54 of the Act requires Ofcom to produce dedicated guidance on women and girls' online safety. We [published](#) our Guidance in November 2025. The Guidance was developed with insights from survivors and victims, safety experts, and civil society groups, following an extensive consultation process. The Guidance sought to reflect the real experiences of women and girls and give voice to their calls for better protections online.
- 2.7 Our Guidance provides practical steps that service providers can and should take to better protect women and girls online. It sets out nine actions that service providers can take to

³ Chapter 2 of [A Safer Life for Women and Girls Online](#) provides an overview of key evidence sources on harms to women and girls online. For a more detailed overview of how harms manifest online, including risks to women and girls, see our [Illegal Harms Register of Risks](#), and our [Children's Register of Risks](#).

⁴ Women's Aid, 2023. [Influencers and Attitudes: How will the next generation understand domestic abuse?](#). [accessed 29 October 2025]; Vera-Gray, F., McGlynn, C., Kureshi, I., Butterby, K., 2021. [Sexual violence as a sexual script in mainstream online pornography](#), The British Journal of Criminology, 61 (5). [accessed 29 October 2025]; Vodafone, 2024. [AI 'Aggro-rhythms': young boys are served harmful content within 60 seconds of being online](#). [accessed 29 October 2025].

⁵ Such services are defined under Part 3 of the Act and include user-to-user and search services.

tackle online gender-based harms across each stage of designing and operating their service. The Guidance applies to all search and user-to-user services including dating, social media and gaming sites.⁶

2.8 The Guidance focuses on four overlapping forms of harm which disproportionately affect women and girls: misogynistic abuse and sexual violence; pile-ons and coordinated harassment; stalking and coercive control; and image-based sexual abuse. Definitions of these harms set out in the Guidance, alongside the nine actions for tackling them, are outlined below.

Online gender-based harms

2.9 Ofcom’s Guidance is focused on addressing the following four categories of online gender-based harm, which evidence suggests disproportionately affect women and girls. We refer to these collectively as **online gender-based harms**.

Table 1: Online gender-based harms

Online Gender-Based Harms	Definition
Misogynistic abuse and sexual violence	This describes the circulation – or promotion – of abusive, hateful and violent content that actively encourages or cements misogynistic ideas or behaviours, including through the normalisation of sexual violence. This includes both illegal content (e.g. illegal threats and abuse) and content harmful to children (e.g. abusive, hateful and violent content), which is often algorithmically amplified and targeted towards young men and boys.
Pile-ons and coordinated harassment	This describes cases where groups of coordinated perpetrators target a specific woman or girl, or groups of women and girls with abuse, hate and threats of violence. As with misogynistic abuse and sexual violence, this can include both illegal content (e.g. threats and intimate image abuse) and content harmful to children (e.g. abusive, hateful and violent content). While pile-ons can happen to any user, they often target women in public life, such as journalists and politicians.
Stalking and coercive control	This describes criminal offences that involve using technology for (a) stalking; or (b) coercive and controlling behaviour in the context of an intimate or family relationship
Image-based sexual abuse	This refers to the criminal offences of (a) intimate image abuse (the non-consensual sharing of intimate images) and (b) cyberflashing (sending explicit images to someone without their consent). We also cover self-generated indecent imagery. ⁷

⁶ The Guidance does not apply to Part 5 services (providers that publish or display pornographic content themselves, with no user-to-user interactions or search content).

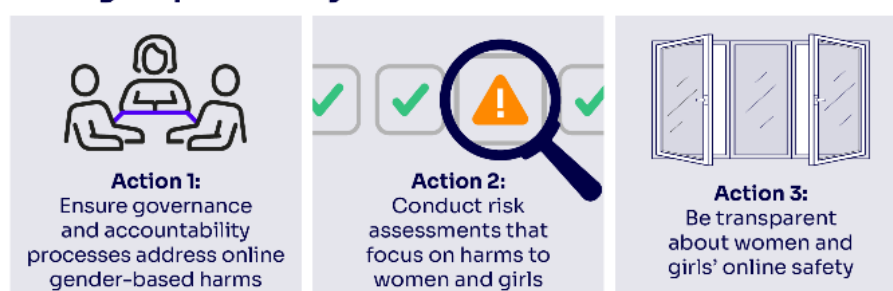
⁷ Self-generated indecent imagery (SGII) refers to sexual imagery created by a child of themselves. All SGII is classified as child sexual abuse material and is therefore illegal.

Action areas for services

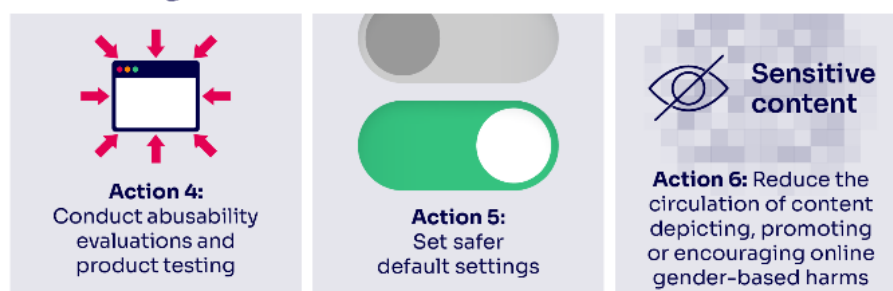
- 2.10 Our Guidance adopts a safety-by-design approach. Using this approach, our Guidance sets out nine actions providers can take to address the challenge of online gender-based-harms across each stage of operating and designing their service, as follows:

Figure 1: Action Areas

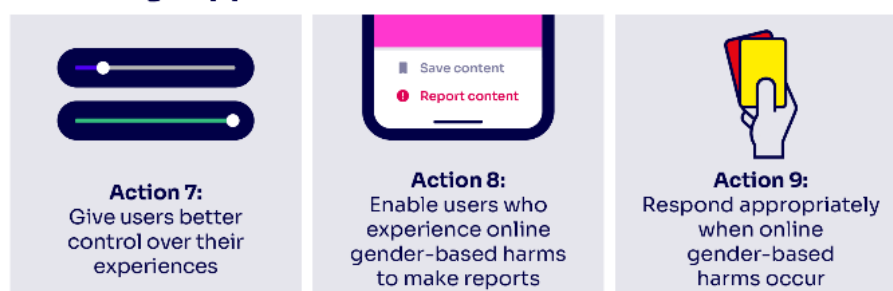
Taking responsibility



Preventing harm



Providing support



- 2.11 The Guidance brings together both foundational and good practice steps that service providers can take to tackle online gender-based harms. The **foundational steps** bring together the measures set out in our existing [Illegal Content Codes](#) and [the Illegal Content Judgements Guidance](#), [Protection of Children Codes](#) and the [Guidance on Content Harmful to Children](#) and [Transparency Reporting](#) that could help address online gender-based harms.
- 2.12 The additional **good practice steps** included in the Guidance set out practical ways in which service providers can go further to demonstrate a commitment to responding to online gender-based harms. These include features, tools and processes that service providers can adopt to deliver ambitious, meaningful changes towards a safer life online for women and girls and others affected by these harms.
- 2.13 We recognise in the Guidance that not all service providers will need to – or will be able to – introduce all the good practice steps and some may only be relevant or applicable to

certain services due to their user base size, risk level, user demographics, the design of the service or business model.

What we are doing next

- 2.14 We are now seeking to understand how industry has responded to our Guidance and what changes women and girls have experienced online since it was published in November 2025. At that time, we [called for service providers](#) to take the recommended actions in our Guidance.
- 2.15 We are now engaging with a range of service providers to find out how they have engaged with and applied the Guidance. In addition to this Call for Evidence, we will also continue to monitor the experience of women and girls through our programme of research, and our engagement with those with lived experiences (including young people).
- 2.16 We will publish a report in Q2 2027, which will summarise the progress we have observed to date, and shine a light on where more could be done to protect women and girls ⁸. ⁹

Our broader programme

- 2.17 We have worked to keep pace with changes in online safety legislation. We have [updated](#) our Risk Assessment Guidance, Illegal Content Codes and other regulatory documents ¹⁰ to reflect the Government's creation of cyberflashing as a priority offence under the Act, ¹¹ requiring services to proactively assess and mitigate cyberflashing as a specific illegal harm.
- 2.18 Given the urgent need for better online protections for women and girls, we also fast-tracked [our decision](#) to recommend the use of 'hash matching' technology to detect intimate image abuse and reduce its spread online.
- 2.19 Once the measure comes into force we will assess service providers' compliance with the measure, taking enforcement action where necessary. This builds on investigations opened by Ofcom into sexualised imagery, [image-based sexual abuse](#) and [enforcement action](#) taken against a nudification site.
- 2.20 We are also [working to implement new duties](#) arising from the Crime and Policing Act 2026, including duties on service providers to take down non-consensual intimate imagery within 48 hours, ¹² which received Royal Assent at the end of April. We will provide an update to our policy roadmap by the end of the year. However, work is already under way, and we are aiming to consult on the new duty on services to take down non-consensual intimate images within 48 hours, by the end of 2026.

⁹ As set out in our [statement when the Guidance was published](#), Ofcom has a broad power under section 164 of the Act to produce and publish reports about online safety matters. Also, in accordance with section 1(3) of the Communications Act 2003, we consider the preparation and publication of such a report is incidental or conducive to the carrying out of Ofcom's online safety functions.

¹⁰ These are the Register of Risks, Illegal Content Judgements Guidance and Record Keeping and Review Guidance.

¹¹ In December 2025, the Government added cyberflashing to the list of priority offences in the Act.

¹² See [Section 100 Crime and Policing Act 2026](#), which amends sections 10, 21, 27 and 32 of the OSA, as well as inserting new sections 20A and 31A and the [Crime and Policing Act 2026: overarching factsheet](#) which sets out further detail of the offences and duties.

3. Evidence we are seeking

- 3.1 Please respond using [this webform](#).
- 3.2 We are seeking evidence from interested stakeholders on the questions set out in this document. We are particularly interested in hearing from civil society, researchers, and academia, although we welcome responses from any interested parties. We are also engaging directly with a range of service providers to understand how they have implemented the Guidance.
- 3.3 We are particularly interested in evidence or insights that have been collected since November 2025 that can help us understand:
- a) how actions taken by service providers, including implementation of the Guidance, may have affected women and girls' online experiences, and
 - b) how the online gender-based harms covered by the Guidance may have changed.
- 3.4 Respondents are not required to respond to every question or bullet point. We welcome evidence that addresses any of the areas covered by this Call for Evidence.
- 3.5 Evidence could include, for example, the findings of relevant investigations, transparency reports or research papers. If you have gathered quantitative data, please provide this in your response. Please include a working hyperlink to any evidence provided (if appropriate).

Questions

- 3.6 As a reminder, the online gender-based harms covered by the Guidance are:

- Misogynistic abuse and sexual violence
- Pile-ons and coordinated harassment
- Stalking and coercive control
- Image-based sexual abuse

What actions are services taking?

Question 1: What action has been taken by service providers since the publication of the Guidance in November 2025 to address online gender-based harms?

Where possible, please refer to the good practice steps from the Guidance in your response. We are particularly interested in evidence relating to:

- implementation of the good practice steps set out in the Guidance,
- other alternative steps adopted by services, and
- the effectiveness of any action, including:
 - > evidence that interventions have reduced harm or improved user experiences, and
 - > evidence that interventions have had limited impact.

What is different for women and girls online?

Question 2: What evidence is available on women and girls' experiences of the online gender-based harms identified in the Guidance since its publication in November 2025?

We are particularly interested in evidence relating to:

- changes (positive and negative) in women and girls' experiences of these harms and their impacts,
- changes in how women and girls engage with online services,
- changes in the ways other users engage with online services that may increase or reduce women and girls' experiences of online gender-based harms
- differences in experiences across services or types of services, and
- whether any changes appear to be associated with actions taken by service providers.

Are online harms changing for women and girls?

Question 3: What new evidence is available on the online gender-based harms identified in the Guidance since its publication in November 2025?

We are particularly interested in evidence relating to:

- the prevalence, incidence, nature, or severity of the harms covered in the Guidance, including how these may have changed (if at all) since the publication of the Guidance, and
- the services or types of services where these harms occur.

A1. Responding to this call for evidence

How to respond

- A1.1 Please submit your response and any supporting evidence by **5pm on 4 November 2026**.
- A1.2 You can respond using [this webform](#).
- A1.3 You can also respond by email or post to the address provided in the response form.
- A1.4 If your response is a large file, or has supporting charts, tables or other data, please upload it at the end of the webform. Alternatively, email it to: **womenandgirlscfe@ofcom.org.uk**, as an attachment in Microsoft Word format, together with the cover sheet.
- A1.5 We welcome responses in formats other than print, for example an audio recording or a British Sign Language video. To respond in BSL:
- > send us a recording of you signing your response. This should be no longer than 5 minutes. Suitable file formats are DVDs, wmv or QuickTime files; or
 - > upload a video of you signing your response directly to YouTube (or another hosting site) and send us the link.
- A1.6 We will publish a transcript of any audio or video responses we receive (unless your response is confidential)
- A1.7 We do not need a paper copy of your response as well as an electronic version. We will acknowledge receipt of a response submitted to us by email.
- A1.8 You do not have to answer all the questions in this call for evidence; a short response on just one point is fine. We also welcome joint responses.
- A1.9 Please clearly indicate on the title page or covering email if your response contains content or material that could be distressing. If you want to discuss the issues and questions raised in this call for evidence, please contact the team by email at:
womenandgirlscfe@ofcom.org.uk

Confidentiality

- A1.10 In the interests of transparency and good regulatory practice, and because we believe it is important that everyone who is interested in an issue can see other respondents' views, we usually publish responses on the Ofcom website after the call for evidence period.
- A1.11 If you think your response should be kept confidential, please specify which part(s) this applies to and explain why. Please send any confidential sections as a separate annex. If you want your name, address, other contact details or job title to remain confidential, please provide them only in the cover sheet, so that we don't have to edit your response.
- A1.12 If someone asks us to keep part or all of a response confidential, we will treat this request seriously and try to respect it either by not publishing the response at all, or by only publishing the parts that are not confidential. Sometimes we might think it is important to disclose parts of a response that have been marked as confidential for reasons of transparency, but we will consult you before we do. Occasionally we might have a legal obligation to publish information or disclose it in court but again as far as possible we will let you know.
- A1.13 Even if your response is not marked as confidential, we might still decide not to publish all or part of it in certain circumstances. For example, if we have concerns about the impact on your privacy or the privacy of others, that the content of the response might facilitate the commission of crime, or about the sensitive nature of the content more generally. If we decide not to publish all or part of your response, we will still take it into account in our consideration of the matter.
- A1.14 To fulfil our pre-disclosure duty, we may share a copy of your response with the relevant government department before we publish it on our website.
- A1.15 Please also note that copyright and all other intellectual property in responses will be assumed to be licensed to Ofcom to use. Ofcom's intellectual property rights are explained further in our [Terms of Use](#). Please also see our [Privacy Statement](#).

Next steps

- A1.16 If you wish, you can register [to receive mail updates](#) alerting you to new Ofcom publications.

Ofcom's consultation processes

- A1.17 Ofcom aims to make responding to a call for evidence as easy as possible.
- A1.18 If you have any comments or suggestions on how we manage our calls for evidence, please email us at consult@ofcom.org.uk. We particularly welcome ideas on how Ofcom could more effectively seek the views of groups or individuals, such as small businesses and residential consumers, who are less likely to give their opinions through a formal consultation.
- A1.19 If you would like to discuss these issues, or Ofcom's consultation processes more generally, please contact the corporation secretary:

Corporation Secretary
Ofcom
Riverside House

2a Southwark Bridge Road
London SE1 9HA
Email: corporationsecretary@ofcom.org.uk

A2. Call for evidence coversheet

Basic details

Call for evidence title:

To (Ofcom contact):

Name of respondent:

Representing (self or organisation/s):

Address (if not received by email):

Confidentiality

Please tick below what part of your response you consider is confidential, giving your reasons why

- > Nothing ☐
- > Name/contact details/job title ☐
- > Whole response ☐
- > Organisation ☐
- > Part of the response ☐

If you selected 'Part of the response', please specify which parts:

If you want part of your response, your name or your organisation not to be published, can Ofcom still publish a reference to the contents of your response (including, for any confidential parts, a general summary that does not disclose the specific information or enable you to be identified)?

Yes ☐ No ☐

Declaration

I confirm that the correspondence supplied with this cover sheet is a formal call for evidence response that Ofcom can publish. However, in supplying this response, I understand that Ofcom may need to publish all responses, including those which are marked as confidential, in order to meet legal obligations. If I have sent my response by email, Ofcom can disregard any standard e-mail text about not disclosing email contents and attachments.

Ofcom aims to publish responses at regular intervals during and after the call for evidence period. If your response is non-confidential (in whole or in part), and you would prefer us to publish your response only once the Call for Evidence has closed, please tick here.

Name

Signed (if hard copy)