University of Southampton

The Sharenting Risk Awareness Checklist (SRAC)

SRAC is based on the findings of an ESRC-funded **interdisciplinary study** and it sets out the ABC of sharenting risks. It also provides safety information. Use the Checklist to gauge your current understanding and develop your knowledge about risks. Click on the three boxes below and the highlighted/underlined items to find out more and access safety tips.

The ABC of sharenting risks:

AUDIENCE | **BASE** | **CONTENT**

AUDIENCE

- ☐ A **public account** increases visibility on and off social media
- ☐ A **private account** is not fully secure
- ☐ Friends and family in your network can **reshare** your posts
- ☐ If you **tag others**, their friends can see your content
- ☐ Others can reshare If you do not disable **automatic reshare**
- ☐ Others can **reuse your content** if you do not disable the feature
- ☐ Others can **download your content** if you do not disable the feature

BASE (Platform)

- ☐ **Two-factor authentication** can restrict unauthorised access to accounts, but not access to shared content
- ☐ **End-to-end encryption** can improve security but it is not a fail-safe feature
- ☐ **Privacy policies** only explain certain security risks
- ☐ Platforms are required **by law** to provide privacy notices and data security

CONTENT

- ☐ Information you share about your child in **online groups or forums** can be misused
- ☐ Sharing your child's **name or birth date** can expose them to harm
- ☐ Sharing your **child's image** is risky
- ☐ **Disabling location tags/sharing** may not conceal you and your child's location
- ☐ Ask your child for their **consent** if they are old enough

AUDIENCE

Consider the audience-related risks of sharing your child's information - The information you share about your child on social media can reach an extensive audience of people you do not know. This can expose your child's information to identity-related crimes, and/or place your child at risk of sexual predators.

A public account increases visibility on and off social media

Anyone can see the content you post about your children in a public account. They can reshare, screenshot, and share it widely.

A 'private' account is not fully secure

Using a private account may not fully protect your children's information. Strangers may still access your posts through various means. The next five items on this checklist explain how this can happen.

Friends and family in your network can reshare your posts

Friends and family in your network can reshare your content and give access to others who can screenshot it and spread it across social media and beyond. Friends and family in your network may also have public accounts or may adopt privacy settings but have hundreds of contacts. In such cases, your content may be accessible to many people outside your network.

If you tag others, their friends can see your content

On some social media platforms, if you tag a friend to the posts you share, their friends can see it. If those in your network have a private account with hundreds of friends or public accounts, many people you do not know may see your content.

Others can reshare if you do not disable automatic reshare

On some social media platforms other users can reshare your posts if you do not disable 'automatic reshare'. Platforms such as Facebook, Instagram, TikTok and X currently allow your 'friends' or 'followers' to reshare your content if you do not disable the feature that allows them to do so. The feature is usually located in the 'settings' section of a platform and you can disable it if you want to restrict your content to a select audience.

Others can reuse your content if you do not disable the feature

Some social media platforms allow other users to reuse your posts and share them far and wide if you do not disable the feature that permits such reuse.

Others can download your content if you do not disable the feature

Some social media platforms also allow other users to download the images, stories and other content you share if you do not disable the download facility. Platforms such as Facebook, Instagram, TikTok and X currently allow 'friends' or 'followers' to download content posted by people they follow. Users can disable this feature.

BASE

Consider that the base or platform you use for sharenting may have specific security risks or loopholes. For example, Instant Messaging apps may seem safer than other social media platforms but when you share updates, members of the groups you have joined can view, screenshot, and reshare your content. To understand these and other security loopholes, you have to familiarise yourself with the privacy policies and security settings of each platform which, as our study found, are not always clear or user-friendly.

Two-factor authentication can restrict unauthorised access to accounts, but not access to shared content

Two-factor authentication can provide added security by requiring users to provide two different pieces of information (such as a password and a code) to gain access to an account. But it does not protect the information you share about your child from misuse.

End-to-end encryption can improve security but it is not a fail-safe feature

Some social media platforms offer end-to-end encryption of information shared between users, to help keep it secure. But it is not fully protective. In some cases, the groups you have joined can view, screenshot, and reshare your content.

Privacy policies only explain certain security risks

The UK GDPR and Online Safety Act require service providers to be transparent about their use of personal data and the implications for users' privacy, but **our study of UK parents** found that the privacy notices issued by the main platform companies are considered inaccessible and should be presented in a clearer, user-friendly way.

Platforms are required by law to provide privacy notices and data security

The UK GDPR and Online Safety Act provide that service providers should offer data security and other cybersecurity measures. Nonetheless, our study shows that users are still exposed to the risks set out in this checklist. This can undermine data security.

CONTENT

Consider the content-related risks of posting your children's information - The type of content or information you post about your child on social media can expose them to harm.

Information you share about your child in online groups or forums can be misused.

Social media groups can provide opportunities to access parenting advice and other useful information such as those related to your **child's health** or their **experiences of parental separation/divorce**. But others can access and misuse the information you share about your child on such groups. For example, predators can use such information to target vulnerable children.

Sharing your child's name or birth date can expose them to harm

Sharing such personal information can expose children to risks such as **identity theft and fraud.**

Sharing your child's image is risky

Studies suggest that sharing children's images across social media can expose them to **identity crimes** and other harms like **digital kidnapping** whereby others steal the images and pass the children off as theirs, or use the images to extort family members by tricking them into believing that the child has been kidnapped. Problematic deepfakes can also be created using the images and this can contaminate the online and digital identities of affected children.

Disabling location/tags sharing may not conceal you and your child's location

Disabling location sharing is not a fully protective security measure. Images contain hidden metadata e.g., location, date, and information about your device. Others can access such information. Even if information such as your child's home address, school, holiday destination, or other location, is not visible in the images you share, metadata embedded in the images can reveal such information.

Ask your child for their consent if they are old enough

Sharenting without your children's consent creates online and digital identities for them without their input. Although Article 3(2) of the United Nations Convention on the Rights of the Child implies that parents may act as the digital custodians of their child's data, Article 12 provides that children have the right to participate in decisions affecting their lives provided they are old enough and of suitable maturity, Article 13 protects their right to privacy.