Privacy

Contacts relating to online privacy are likely to fall into three broad categories: privacy good practice guidance, issues relating to the abuse of privacy, and concerns relating to 'digital reputation' or 'digital footprints'.

Privacy good practice contacts involve a child looking for advice on how to manage their privacy online – for example, picking passwords, managing profiles on social media, and so on.

Abuse of privacy contacts will relate to breaches of privacy – for example, if they believe someone knows their password or if they are receiving unwanted contact.

A child may also call with concerns about their 'digital footprint' or their 'online reputation' – for example if they or a friend have shared information or content publically that should have been kept private and they have concerns about the impact. This could include sharing of sexual images or 'sexting', or 'revenge porn':

- Sexting: self-generated nude / partially nude / sexually explicit material
- Revenge porn: sexually explicit material that is publicly shared online without the consent of the pictured individual - often uploaded by ex-partners with an intention to shame or embarrass an individual, linking content to the person's other online content, such as social media profiles.

WHEN A CHILD MAKES CONTACT DIRECTLY

Commend the child for making contact and ask questions - by listening to the child you will be able to better understand the reason for the child's contact.

Use questions to understand if the contact relates to privacy 'good practice', to an abuse of privacy, or to the child's digital reputation.

If the child has called with regard to serious concerns about their digital reputation or an abuse of privacy, offer reassurance and a listening ear. They may feel a range of emotions: threatened, ashamed or distressed. Commend the child for making contact and acknowledge their courage for speaking up. Reassuring the young person that they have made the right decision and that you are there to listen and help them is vital. Equally important is making sure that you tell them that it is not their fault and they are not to blame in any way.

Be clear where your helpline stands on confidentiality so the child knows what may happen with information they share. For example, explain that anything they tell you will be private unless they tell you something that makes you think they are in danger and you are able to get them help, in which case you would talk to them about what you are going to do.

Build a relationship and give the child the time and space to open up further and volunteer more information. Remember to acknowledge the emotional impact of what has happened, and take care not to make assumptions about the situation.

Be supportive. As well as gathering information about the nature of the abuse or digital reputation issue, try to understand how the child has been affected emotionally, so that you can support them in that and even escalate or safeguard if necessary. For example, in cases where the child's 'digital footprint' is being used to blackmail them, escalation will be required (see sexual extortion guide).

Questions should be clear and open-ended, for example:

- Can you tell us when this happened?
- Has anyone threatened to you? Have you been asked to produce more images?
- What has been shared? Who with? What devices / social networks have they been shared on?

Try to help them understand that although this may feel like the end of the world, it is not. Talk through strategies that can help put them back in control.

If a child is unwilling to talk about specifics during the contact, encourage them to call back – give them time and space.

Discuss the practical options that are relevant to the specific contact (see below).

WHEN A PARENT / CARER MAKES CONTACT

Commend the parent / carer for coming forward and seeking advice.

Use questions to understand if the contact relates to privacy ‘good practice’, or to an abuse of privacy or the child’s digital reputation, and tailor your response accordingly.

To support discussions on privacy good practice with parents / carers, you could use a framework developed by O2 and NSPCC: Explore, Talk, Agree & Manage

Explore: Help them understand what personal data is.

- Your kids need to protect their personal data, or it could up in the wrong hands. Personal data might include their address, full name, birthday, phone number and school name. This information can all be used for bullying, blackmail, grooming, or to steal their identity.

- When people ask for personal details, it might not always seem dangerous. But you should make sure your child never shares their personal data online. People aren't always who they say they are.

Talk: Help them understand the importance of having conversations with their child

- Explain that anything shared online could be around forever, even if they delete it. There's no telling who's copied or shared the information. Ask your child to think about what could happen if the wrong person got hold of their information. Let them consider the consequences, the lesson is more likely to stick that way.

- Let them know you're there to help if anything goes wrong. You won't be angry and you won't overreact.

Agree: Help them understand the importance of setting ground rules with their child.

- Agree what sites, apps and games are appropriate for your child. If your child wants to use a chatroom, make sure it's moderated and you've checked it out yourself.

Manage: Help your child understand their digital footprint.

- Do an online search for your child's name, their nickname, their school or their address. Check the image results as well. This will show you what information about them is public. If you have any worries, discuss the results with your child and help them edit their profile to make it safer.

For reactive calls about abuse of privacy or issues relating to a child’s digital reputation, you will need to offer reassurance. For example, it is likely that a parent / carer will feel a range of emotions if they discover that their child has shared nude or nearly nude images / videos online. They may feel angry, confused, scared and may blame themselves for what has happened. What is key, is that they understand that it is not their child’s fault and they are not to blame for what has happened.

Encourage the parent to try to remain calm, to be non-judgmental and to avoid any panicky solutions. In particular, advise parents not to remove their child’s internet access – the most likely consequence of such an action would be that the child would not discuss future problems with the parent for fear of being cut-off from their digital lives.

Discuss practical advice (see below) with the parent and remind them that your helpline is available for their child to call for support - but do note that you won’t be able to share the content of the call with the parent without the child’s consent.

It is important that you also discuss the potential emotional impact on the child – this will help the parent be alert to signs to watch out for as well as take a supportive approach to their child. Ask the parent to talk about:

- Any changes they have noticed in their child’s behaviour.

- Whether they have any concerns for the child’s mental health currently or historically.

Gathering this information will help inform you if any subsequent referral to the support services may be required. You should also ensure the parent is looking out for any subsequent changes in their child's behaviour, even if there have been no visible changes reported by the parent to you at this stage.

PRACTICAL ADVICE:

Take some time with the child or parent / carer to explore practical options that might help for the specific context that is being discussed.

Practical steps that can be discussed for keeping control of online privacy include the following:

- **Review privacy policies and settings** of websites / apps you use.
- **Passwords.** Never share passwords. If you think someone knows your password, change it; pick a password that cannot be guessed; use different passwords for different services and activities.
- **Profiles and sharing information.** Actively manage your profile settings so that your posts can only be seen by your chosen group of friends. Bear in mind that anything you post could still be copied and shared beyond your chosen group. Do not share information online that could make you vulnerable to unwanted / inappropriate contact or identity theft (e.g. address, email, phone number, date of birth, etc).
- **Friends**. Consider friend requests carefully – what do you really know about the person who has contacted you?
- **User name.** User names should never include personal information (e.g. the year they were born, address or their full name).
- **History**. Delete your search history and log out of websites when you are away from your computer.
- **Use anti-virus software** on your devices and keep it up to date.
- **Check websites are secure.** Before entering private information such as passwords or payment details, look for the padlock symbol after the web address or 'https' in front of the web address in your browser.
- **Think before you click** – if you receive an email from a stranger, think before clicking on a link or an attachment - it could contain a virus.
- **Cover your webcam** – if you're not using your webcam, unplug it, cover the lens or point it at a blank wall.
- **Blocking**. Use privacy settings or blocking tools to prevent unwanted contact.
- **Stay alert to potential identity theft**. For example, if you receive bills for things you haven't ordered or emails from unknown organisations, it might be that someone is using your identity. Change all your passwords, secret questions and other information you use to identify yourself on online services.

For content that has been shared already and is now regretted, you can discuss options with the child. For example,

- Can the child edit or delete the content, if they uploaded it?

- If someone else uploaded it, or content you uploaded has been shared by someone else, could the child ask them to delete it? Discuss ways the child might make the request.

- Is there benefit to deleting the account from which the content was shared, and setting up a new profile on that website?

If the issue relates to 'sexting' or loss of control of self-generated sexual images / material online, suggest the child / parent contacts the safety centre on the social media site as well as any available services for having content removed, such as the national internet reporting hotline. If blackmail is involved, refer to the sexual extortion guide.

For issues relating to unwanted contact see the unsolicited contact guide.

RED FLAGS:

- The child discloses that he / she is the subject of sexual images produced by a peer or adult

- The child is expressing suicidal thoughts, intentions to self-harm or emotional trauma.

- The child has been threatened or blackmailed.

In the case of red flag issues emerging during your conversation, follow your standard escalation processes for intervention by law enforcement, child protection services, and so on, as appropriate.