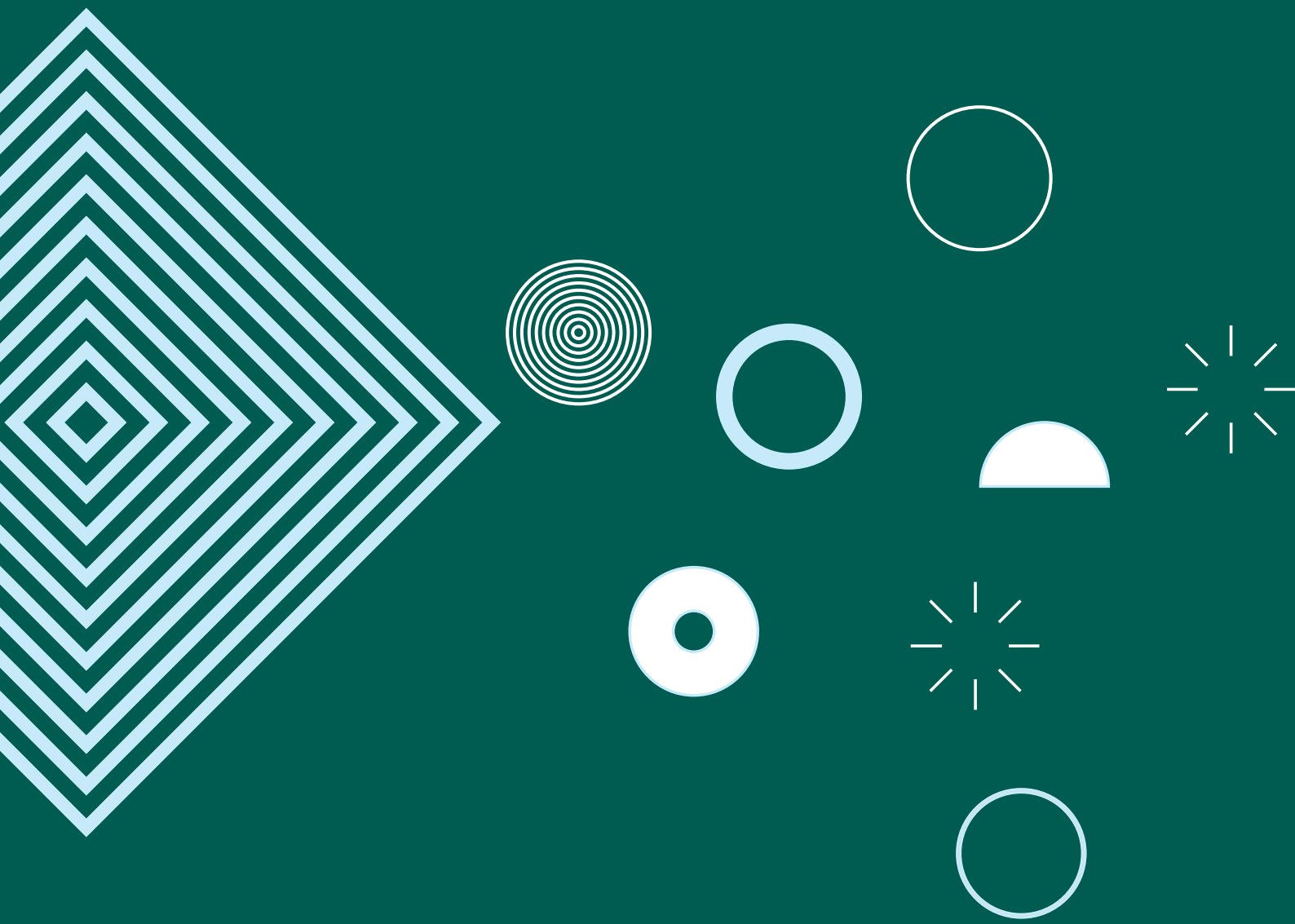
Data Protection Commission

Protecting my child's data



An Coimisiún um Chosaint Sonraí
Data Protection Commission

DATA PROTECTION COMMISSION,
21 FITZWILLIAM SQUARE, DUBLIN 2

Protecting my child's data

As a parent, you may find from time to time that you need to step in to protect your child's data or make a complaint on their behalf, for example to their school, sports club or to a social media platform on which they have an account. The purpose of this guidance note is to help parents understand the rights that they have over their children's data in different contexts and to outline steps to follow when raising a data protection concern on behalf of their child.

Can I raise my concern directly with the DPC?

As a general rule, you should always raise your concern with the organisation that has your child's data first rather than going straight to the DPC. It may be that there's an innocent explanation for your concern and it's important to give that organisation an opportunity to resolve the matter themselves. If you don't hear back within a reasonable period or are not satisfied with their response, you can raise it with us. We will ask you to enclose copies of your correspondence with the organisation, as this will help us assess your complaint more quickly. Visit our website for more information on **the type of complaints we accept and our complaint handling procedure**.

There will be situations where you can skip this step and raise your concern directly with us if it is particularly serious. For example, if you have evidence that your child's personal data has been mislaid, improperly disclosed or used for an inappropriate purpose, you can and should notify the DPC straight away.

Will I have to prove that I am my child's parent or guardian?

This will depend on the circumstances. In some cases, you may have to prove your identity if doing so is proportionate and reasonable in the circumstances. Under data protection law, any organisation that has your child's data has to make sure it is kept safe and secure. This includes ensuring that your child's information is shared only with people who are entitled to see it. Otherwise, anyone claiming to be you could easily get a copy of your child's personal data.

However, this does not mean you must always prove who you are with absolute certainty. The organisation needs to pick methods that are reasonable and proportionate to protect the data they hold about your child. In many cases, they will not need further proof as they should already have enough information about you to confirm your identity.

For example, if you are making a request to your child's school for a copy of their data, and the school already has you down as the child's parent or guardian, then additional proof shouldn't be necessary, as they already know who you are and can check your identity against the information they have about you on file.

If you are making a request to a social media or gaming company for information about your child's account, and you already have a paired account or parental dashboard for supervising your child, then it should be enough to have you log in to confirm your identity – the company already knows who you are and has evidence of

your relationship with your child. Similarly, if they have your credit card details, the company should already have enough information to confirm your identity.

However, if your request concerns an online account that your child has set up legally but without your involvement (e.g. a personal email, social media or messaging account) then the organisation will probably have to verify your identity in some way before agreeing to deal with you as the child's parent. The difference here is that the company doesn't know who you are, and can't just hand out your child's information to anyone claiming to be their parent.

These examples also illustrate the importance of **keeping your passwords, phone numbers, email addresses and other personal information safe and secure, particularly if they can be used to access your child's data**. Always use complex and unique passwords when setting up parental supervision tools, always log out when you are done checking up on your child, and never leave your devices unattended in a public place.

When do I need my child's permission?

It's always a good idea to involve your child if they are old enough to understand data protection and to give you permission to act on their behalf. This is because your child has an individual right to privacy and parents don't have an absolute right to exercise their children's data protecting rights. While it can be presumed that parents will act on behalf of very young children, the older your child is, the more likely it is that you will need their permission before stepping into their shoes.

This is particularly the case as regards your child's digital footprint. Many of the most popular online platforms allow teenagers to create accounts without their parents' permission. As a general rule, if your complaint concerns an online account that your child has properly created by themselves, then there will be a limit to what you are allowed to do without your child's involvement. It might be possible for you as a parent to access the account only if your child gives you the log-in details. This is why **it's always a good idea to make these sorts of requests together with your child where possible, particularly if your child is legally old enough to use social media on their own**. This will help you to protect your child in a way that empowers them. It will also help to resolve any concerns the company may have about failing to respect your child's right to privacy.

Of course, if your child is for some reason incapable of giving you permission and you have proof of that inability, then you should be allowed to act on behalf of your child.

When can my child start signing up for online services without my permission?

Although the age of digital consent in Ireland is set at 16, many online services can legally allow children as young as 13 to sign up without parental consent depending on the legal basis upon which the service is offered. For more information about when parental consent is and isn't needed under the GDPR, please see our guide entitled **"Consent and my child's data"** .

This means that sign-up ages for the most popular social media apps, messaging services and email providers range between 13 and 16. Once your child reaches 13, they can start signing up for some social media and other online services without your

permission. A lot of the online services popular with children have parental oversight tools such as parental dashboards, 'family account' or 'kids' account' features that can help you to supervise your children online. But if your child is old enough, and has already created their own email and social media accounts, you will need to persuade them to let you to set up these supervision tools. That is often easier said than done.

This is why parents **should think in advance about how they want to supervise and protect their children online**. If you leave it too late, you might sleepwalk into a situation where you have less oversight over your child's digital life than you would like. Before you buy your child their first phone, tablet, laptop or other internet-enabled device, **do some research on parental control software and web filters, and think about the protections that you want your child's devices to have**. If possible, talk to your child about the social media apps they are interested in before they reach the signup age. When they are old enough, offer to set up your child's profiles together so that you can switch on any parental controls and ask your child for the password for emergencies.

What if my child is too young to be on social media?

If your child has created an account that they should not have been able to (e.g. by lying about their age) then you should contact the company directly and have their account deleted. Social media platforms have contact forms or other tools for this purpose. It's very important that you don't help your child access age-restricted apps and services before they are old enough to use them.

Can't I just take away my child's phone if they won't listen to me? It's my money, after all.

While you have that option, there is the risk that this will simply drive your child's online activities into the shadows. It's very easy on many social media platforms for your child to create accounts under a fake name and date of birth. Even if you take their devices away, your child can find other ways of accessing their social media, such as by using school computers, visiting internet cafés, or borrowing their friends' devices. Even if that weren't the case, taking away your child's devices is obviously not a long-term solution. The best approach will always be to find a way to help your child understand the importance of protecting their privacy online, and to work out ways to do so that they can – and want to – use for themselves when you are not with them.

This is why **parents have to be pragmatic when supervising their children online and respectful of their child's right to privacy**. Talk to your child about any concerns you have about their social media and online habits, listen to what they have to say, and try to persuade them to your point of view rather than simply laying down the law. The more heavy-handed you are, the more likely it is that your child will start covering their tracks online, which will make them less safe.

None of this is to say that your child has a right to have social media or their own devices before you think they are ready. You don't have to be flexible or give in to your child when it comes to deciding when and under what conditions they can have their own phone, tablet or games console, for example. You don't have to be guided by what other parents are doing and you certainly shouldn't go underneath the minimum

age ratings. What matters is that you talk to your child about these issues so that, if you decide that you want to wait until they are a bit older, they will understand and respect your decision and feel heard.

KEY TAKEAWAYS FOR PARENTS

- Keep any email addresses, phone numbers, passwords and other information that can be used to access your child's data safe and secure. Always use strong passwords when setting up parental dashboards and other monitoring tools.
- Always try to involve your child when exercising their data protection rights if they are mature enough, as this will help them understand data protection and why it's important.
- Talk to your child in advance about social media and the apps and games they are interested in using when they are older, and do your own research. When they are ready, offer to set up their devices and social media accounts together so that you can have more oversight.
- Try to be pragmatic and respectful of your child's right to privacy when supervising them online. But at the same time don't feel pressured into letting them use different online services or devices before you think they are ready.
- Recognise that using social media and other online services will almost certainly be a part of your child's life as they grow up. Help them recognise and respect their rights and privacy, and learn how to protect them themself.

www.dataprotection.ie

An Coimisiún um Chosaint Sonraí
21 Cearnóg Mhic Liam, BÁC 2,
DO2 RD28, Éireann.

Data Protection Commission
21 Fitzwilliam Square, Dublin 2,
D02 RD28, Ireland