



Well-Being & Safeguarding Newsletter for Families

May 2022

**Keeping
children safe
is everyone's
responsibility**



In this issue:

- Car Seat Shopping Check list
- Kooth
- Yubo explained
- What parents need to know...
Protecting Personal Data
- Electrical Safety while working from home

Car seats shopping checklist

What's your child's weight?

What's your child's height?

What's your child's age?

Does the shop assistant explain about staying rear-facing for longer?



What vehicle will you use the seat in?

Will you be using it in any other vehicles?

Does your car have Isofix?

Does your car have underfloor storage?

Does the shop assistant offer a demo?

Does your car have a top tether?

Does the shop assistant need to check a fit list?

Check out our list of Don't Buy car seats we'd recommend you avoid:
[which.co.uk/dontbuycarseats](https://www.which.co.uk/dontbuycarseats)

Kooth Online Counselling

Kooth is a safe and confidential online counselling and support service for young people aged 11-18 years old (up to 25 for Care Leavers or young people with SEND).



Kooth is staffed by fully trained and qualified counsellors and is available free to young people across the Lincolnshire area. You can have live online conversations with professionals about your personal and educational problems or concerns, including emotional and mental health.

Counsellors are online:

- Monday - Friday 12 noon till 10pm
- Weekend 6pm till 10pm

Yubo explained...



Yubo is a live-streaming platform designed to help users 'meet new people' from all over the world. Users can then connect with others based on interests, location, or gender. It is available to download on Google Play Store with a rating of 'Teen' and IOS App Store with a rating of 17+.

Once set up, they are sorted into two groups – aged 13-17 and 18+. Users are then able to send messages, video chat and livestream. The platform is designed to promote the feeling of 'Fear Of Missing Out' (FOMO).

To find out more about the risks and how to prevent these click the link, which will take you straight to the INEGE website.

[What is Yubo? - Inege Safeguarding Group](#)



Personal data is a strange commodity. Cyber thieves can buy huge quantities of personal data on the black market for very little, yet your own personal data is hugely valuable to you. If your personal data falls into the wrong hands, it could lead to identity theft, bank fraud or something even more sinister such as stalking. The severity of that threat is multiplied when it comes to the personal data of children, when threats such as internet grooming begin to emerge. The bad news is that children aren't always great at safeguarding sensitive information, which is why they need parents' help and guidance. That's why we've created this guide to show you how you can protect your own and your family's personal data.



What parents need to know about

PROTECTING PERSONAL DATA



EVERY DETAIL IS KEY

Which info should you be wary of sharing online? Aside from the obvious, such as full names, date of birth and address, think of the type of information you're asked for when answering security questions for services such as online banking. The name of your first school, your mother's maiden name, the names of your pets, your favourite band. Data thieves will harvest as much of this information as possible, so don't make it easy for them by publishing it anywhere online.



SOCIAL MEDIA VISIBILITY

Social media sites, such as Facebook, encourage us to share sensitive information in order to build our online profiles. Many people are lulled into thinking that only their friends can see such information, but that's rarely the case. Such information can easily be shared with 'friends of friends' or even anyone searching for you online because privacy settings are opaque. Keep social media profiles to the bare minimum. If you wouldn't be comfortable hanging a sign with that information on your front door, don't enter it into social media sites.



DANGEROUS GAMES

Online games are a particular risk for children. Many of the most popular games – such as Fortnite, Minecraft or Roblox – have voice or text chat facilities, allowing them to talk to fellow gamers. Or, sometimes, people pretending to be fellow gamers. It's very easy for children to be seduced into divulging personal data such as their address, birthday or school. It's critical parents both educate children on the dangers on online chat in games and take safeguards to protect children.



IMPOSTERS AND PHISHING ATTACKS

Even if you're scrupulous about keeping your data private on social media, it's easy to be lulled into handing it over to imposters. There are two golden rules for you and your children to follow: 1. Never divulge personal information to phone callers, unless you can be absolutely certain you know who they are. 2. Never click on links or open attachments in emails or social media, unless you're 100% certain they are genuine. So-called phishing emails are growing ever-more sophisticated, with fraudsters able to replicate the exact look of bank emails and even include details such as account numbers and IDs.



THE RISKS OF PASSWORD SHARING

Password sharing – using the same password for multiple sites – is one of the easiest ways to lose control of your personal data. Hacking of major websites, including usernames and passwords, is common. If you're using the same password for a hacked site as you do on your Gmail account, for example, you're handing data thieves an easy route into your inbox, where they will doubtless find all manner of sensitive information, such as bank emails and contacts. Your email account will often also let them reset the password on multiple other accounts. Don't share passwords; use password managers to create strong, unique passwords for every site.



National Online Safety

#WakeUpWednesday

Safety Tips for Parents & Carers

LOOK OUT FOR LEAKS

Many security software packages have features that look for personal data leaks or prevent people from entering it into risky sites in the first place. For example, Bullguard Premium monitors dangerous sites for usage of data such as your email address, debit card numbers, passport number and more, and then sends you email alerts and details of how to take remedial action if it spots them being used. Such software also issues warnings if it sees personal data being entered into unprotected, high-risk sites.



KEEP DATA GUARDED

Don't give the thieves a head start by handing them pieces of sensitive information for free. For example, it's very common to see email address such as davesmith1976@gmail.com – an immediate clue that you were born in that year. If you have a less common name than Dave Smith, thieves could immediately start using that information to cross reference against public records or other database breaches, allowing them to start building a profile of information about you. Likewise, don't use your date of birth in a password. If that's hacked, you've handed the thieves another big clue.



DON'T OVERSHARE ON SOCIAL MEDIA

The biggest threat to your child's privacy is you. Parents often overshare personal information on social media: full names, names of schools, children's birthdays, names of their friends. All of this can be easily gleaned to build profiles that could be used to groom your child in online games or in real life. Exercise extreme caution with social media posts concerning your children.



BE WARY OF SHARED NETWORKS/SYSTEMS

Avoid entering any personal data into a web browser when you're using public Wi-Fi (in a coffee shop or airport, for example) or when using shared computers. Shared Wi-Fi connections are much easier to eavesdrop on than your home network, especially if they are not password protected or the password is shared freely with customers. Don't do online shopping, banking or enter any logins/passwords when using shared Wi-Fi. Likewise, if you're using a shared computer at work, for example, as it's very easy for a browser to save logins that could be used by others.



PLAY SAFE IN ONLINE GAMES

Children must be taught to treat strangers in online games with the same caution as they would treat strangers in the street. Don't allow children to use their real name as their username in games to prevent imposters conning kids into thinking they are real-life friends, and only allow them to add friends in the game that they know in real life. Regularly ask to monitor your child's friends list in such games and ask them to identify who the players are. With younger children in particular, ask them to only use voice chat in family rooms, so that you can hear conversations.



Meet our expert

Barry Collins has been a technology journalist and editor for more than 20 years, working for titles such as *The Sunday Times*, *Which?*, *PC Pro* and *Computeractive*. He's appeared regularly as a technology pundit on television and radio, including on *BBC Newsnight*, *Radio 5 Live* and the *ITV News at Ten*. He has two children and has written regularly about internet safety issues over the years.





School Governor Safeguarding Update May 2022

The safeguarding governors have been busy! We have carried out a monitoring visit to check the School Central Record is up to date. This is a very important school document and a key part of our safeguarding procedures. It is a document that will also be reviewed by Ofsted on their visit to ensure we are compliant with safeguarding requirements. The outcome was that it is regularly monitored and updated and showed the correct detail for all staff. However, we identified a that new Governor induction and information needed to be processed quicker, which has now been addressed.

We also met staff to discuss on-line safety and how COVID led to an increase in on-line usage for our pupils. The visit demonstrated that clear policies regarding IT are in use for pupils and staff within school and at home. The school are in the process of updating their pupils acceptable use agreements to roll out across school. The school keeps abreast of changes and is proactive in identifying new issues and resolving them promptly. All of the pupils have recently completed online safety workshops with, John Jeffries, a local ICT consultant. Our next visit in school is to attend one the school's Computing Ambassadors meetings.

Update provided by the Safeguarding Governors May 2022

Our Safeguarding Team

Designated Safeguarding Lead:

Catherine Stratton



Deputy Safeguarding Leads:

Alice Cowles



Designated Wider safeguarding Team:

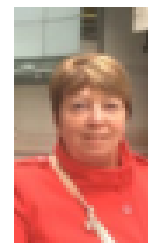
Family Support worker:

Theresa Miller



Safeguarding Governor:

Linda Hawbrook



Contact Number for the Safeguarding Team in school

(01522) 702669

Our Updated Safeguarding Policy September 2021

Please scan the QR code or click the link to find our most recent policy.

[Link](#)

<https://www.saxilby.lincs.sch.uk/wp-content/uploads/2021/09/LCC-School-Child-Protection-Safeguarding-Policy-v16-September-2021-FIN....pdf>



The Importance of Attendance for Safeguarding

Attendance monitoring is a key part of our safeguarding processes in school. We take non-attendance and lateness seriously. School will maintain records of where children are and reasons for non-attendance or late arrival. We are a duty to investigate non-attendance - see [section 175 Education Act 2002](#),

Please keep the school informed of any changes to your contact details

**Keeping
children safe
is everyone's
responsibility**

