

St Faith's Church of England Infant and Nursery School

Our vision: Our inclusive St Faith's family strives to enable all to achieve their full potential and inspire a community of hope and friendship.

We seek excellence by ensuring a safe, respectful and flourishing learning community, where differences are celebrated and our genuine love and high expectations make a difference to all.

"Aspire not to have more, but to be more." (Oscar Romero)

SAFEGUARDING NEWSLETTER – NOVEMBER 2026

In this newsletter:

- Electrical Safety while working from home
- Our Safeguarding Governors
- Protecting Personal Data
- Our School Safeguarding Team
- Safeguarding Contact including Local Authority Contacts



School Governor Safeguarding Team

As part of their role, our school governors carry out regular safeguarding monitoring. This can involve auditing records and school processes such as the Single Central Record. They also interview staff and pupils to check the impact of our processes and policies.

The governors will be adding to our monthly newsletter with updates on this work and any outcomes identified.

Our Safeguarding Governor is Ros Garrod-Mason.

St Faith's Church of England Infant and Nursery School

Our vision: Our inclusive St Faith's family strives to enable all to achieve their full potential and inspire a community of hope and friendship.

We seek excellence by ensuring a safe, respectful and flourishing learning community, where differences are celebrated and our genuine love and high expectations make a difference to all.

"Aspire not to have more, but to be more." (Oscar Romero)

At National Online Safety we believe in empowering parents, carers and trusted adults with the information they need to hold an informed conversation about online safety with their children, should they feel it is needed. This guide focuses on one platform of many which we believe trusted adults should be aware of. Please visit www.nationalonlinesafety.com for further guides, hints and tips for adults.

What parents need to know about PROTECTING PERSONAL DATA

Personal data is a storage 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.

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 names 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 popular 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 lulled 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 sceptical 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 for phone calls, 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 universities and governments, is common. If you're using the same password for a hacked site as you do on your Gmail account, for example, your handling data flows on email could leak into your inbox, where they will divulge just about all manner of sensitive information, such as bank emails and contacts. Your email account will often also let them read the password on multiple other accounts. Their shared passwords can be used to create strong, unique passwords for every site.

National Online Safety 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 sending it into risky sites in the first place. For example, Malwarebytes Premium monitors dangerous sites for signs of data such as your email address, debit card numbers, password history 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 thieves a head start by handing them pieces of sensitive information for free. For example, it's very common to see email addresses such as info@nhs.uk or help@nhs.uk - all immediate clues that you were born in that year. If you have a less common name than Owen Smith, those could immediately start using that information to cross-reference against public records or other data sources, allowing them to start building a profile of information about you. Likewise, don't use your date of birth as a password. If that's hacked, you're handed the flowers another day.

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 geo-located to build profiles that could be used to guess your child's online games, or to visit their school, or to visit their club 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 banking, banking in order any login passwords when using shared Wi-Fi. Likewise, if you're using a shared computer at work, for example, as it's very rare for a browser to keep login data 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 or to send imposters convincing 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 remove your child's friends in each game 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

Rory Collier has been a technology journalist and editor for more than 20 years, writing for titles such as The Sunday Times, World PC, PC Pro and Computeractive. He's appeared regularly as a technology pundit on television and radio, including on BBC Newsnight, Radio 4 Live and the ITV News at Ten. He has two children and has written regularly about internet safety issues over the years.

www.nationalonlinesafety.com Twitter - @natonlinesafety Facebook - /NationalOnlineSafety Instagram - @nationalonlinesafety

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 01.07.2020

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

Keeping children safe is everyone's responsibility



St Faith's Church of England Infant and Nursery School

Our vision: Our inclusive St Faith's family strives to enable all to achieve their full potential and inspire a community of hope and friendship.

We seek excellence by ensuring a safe, respectful and flourishing learning community, where differences are celebrated and our genuine love and high expectations make a difference to all.

"Aspire not to have more, but to be more." (Oscar Romero)

Our Safeguarding Team

Designated Safeguarding Lead



Mrs Amanda Konrath
Head teacher

Deputy Safeguarding Lead



Miss Lisa Wright
Deputy Head Teacher

Deputy Safeguarding Lead



Mrs Hayley Palmer
SENDCO and Inclusion Leader and Nursery Teacher

Deputy Safeguarding Lead



Mrs Gemma Simpson
Nurture Lead and ELSA

Contact Number for the Safeguarding Team in School 01522 888988

**Our School Child Protection and Safeguarding Policy can be found on our
School Website**

(Safeguarding Information and Policies | [St Faith's Church of England Infant and Nursery School \(st-faiths.lincs.sch.uk\)](http://st-faiths.lincs.sch.uk))