ST. ANNE'S CATHOLIC HIGH SCHOOL

"Act Justly, Love Tenderly, Walk Humbly With Your God"

Cyber Safe

ONLINE SAFETY NEWSLETTER

FEBRUARY 2026

WELCOME TO THE THIRD EDITION OF CYBERSAFE!

Dear Students, Families, and Colleagues,

This edition explores the important topics of radicalisation, privacy and identity theft. This issue looks into why these areas are increasingly relevant for young people using the internet, social media, gaming platforms and messaging apps.

We examine how online content, peer influence and digital communication can sometimes expose students to harmful or extreme viewpoints, and we highlight the warning signs that young people and families should be aware of. This issue of *CyberSafe* also explains the ways in which personal information can be collected, shared or misused online, and the potential consequences if this information falls into the wrong hands.

Included is practical advice for students on how they can recognise online risks, protect their personal data, create strong passwords, manage their privacy settings, and think critically about the content they view and share. Students are also encouraged to seek help from trusted adults if they encounter concerning or unsafe online situations.

We encourage you to read this *CyberSafe* newsletter with your child and use it as an opportunity to discuss safe and responsible online behaviour.

Enjoy!

Mrs Claudia Duarte, Head of Online Safety

Are YOU Worried?

If you have a concern about your daughter or another student's online activity or safety you can reach out to your child's Learning Support Coordinator or contact Kaylea Vevers, the Designated Safeguarding Lead, by emailing dsl@st-annes.enfield.sch.uk

RADICALISATION

Radicalisation is the process by which individuals, particularly young people, move from holding moderate and widely accepted beliefs to adopting extreme ideological views. This may occur online through exposure to violent extremist material, or offline through contact with extremist groups or networks. Radicalisation can increase the likelihood that individuals will support terrorism and violent extremism, and in some cases may lead them to commit criminal acts.

How could your child become radicalised?
Young people may be vulnerable to a range of risks as they pass through adolescence. They may be exposed to new influences and potentially risky behaviours, influence from peers, influence from older people, or the internet as they may begin to explore ideas and issues around their identity. There is no single driver of radicalisation, nor is there a single journey to becoming radicalised. The internet creates more opportunities to become radicalised, since it's a worldwide 24/7 medium that allows you to find and meet people who share and will reinforce your opinions. Research shows that the internet and face-to-face communications work together, with online activity allowing a continuous dialogue to take place.

The process of radicalisation may involve:
- being groomed online or in person
- exploitation, including sexual exploitation
- psychological manipulation
- exposure to violent material and other inappropriate information
- the risk of physical harm or death through extremist acts

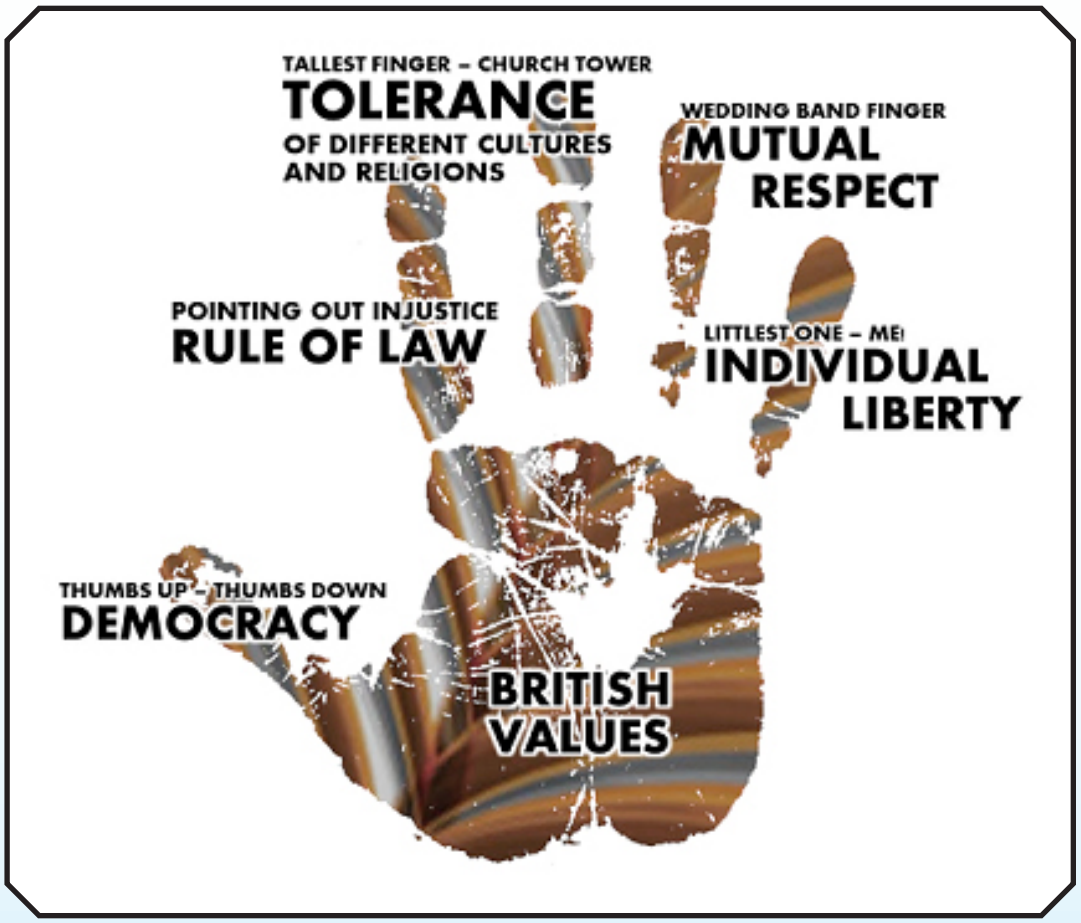
Radicalisation happens gradually so children and young people who are affected may not realise what it is that they are being drawn into.

What are the signs you should look out for?
There are a number of signs to be aware of (although a lot of them are quite common among teenagers). Generally, parents should look out for increased instances of:

- Being secretive about who they have been talking to online and what sites they visit
- A move from expressing moderate views to following more extreme views
- A sudden conviction that their religion, culture or beliefs are under threat and treated unjustly
- A conviction that the only solution to this threat is violence or war
- Lack of feeling of belonging or a desperate need to find acceptance within a group
- Displaying intolerant views to people of other races, religions or political beliefs

How to help protect your child:
f you believe your child, or another child, is in immediate danger, poses a risk to others, or may be taken out of the country, contact the police straight away and make sure their passport is kept secure. Any concerns about online grooming can be reported to the National Crime Agency's **CEOP** Command or to **Act Early**, a service run by Counter Terrorism Police.

- Talk to your child calmly and try to understand why they hold these views, using alternative perspectives to challenge and undermine them.
- Stay alert of negative influences, both online and offline.
- Watch for changes in behaviour, whether subtle or significant, especially if they become more frequent or intense.
- Trust your instincts, if you're concerned seek support and advice.
- Share your concerns with trusted people, such as school staff or community leaders.



Find out more here:

Learn About Radicalisation | Internet Matters

How Do I Know If My Child is Vulnerable to Radicalisation Online? | Internet Matters

Radicalisation and Extremism | Educate Against Hate

Signs of Radicalisation in a Teen: Do You Know the Indicators? | Action Counters Terrorism

Radicalisation | NSPCC Learning

Spot the Signs of Radicalisation | GOV•UK

PRIVACY AND IDENTITY THEFT

Children are at risk of identity theft just as much as adults, so it's important to ensure they understand the importance of personal data privacy. Child identity theft is when someone steals a child's personal information or data and uses it to open credit cards or bank accounts, apply for loans, commit scams and more.

Why is privacy online important?

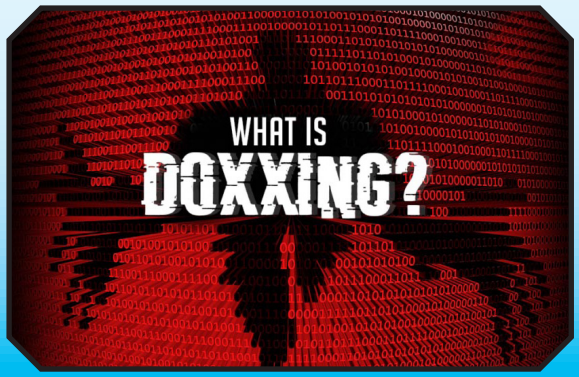
Every time we share something online, we add a bit more information about ourselves to the online world. This includes posting a photo, writing a comment or liking someone's video. The trail of information we create when we share things online is known as our 'digital footprint'. People we know, and people we don't know, can see our digital footprint and use it to learn more about us. You can take control of your **digital footprint** by using privacy settings. Privacy settings help you to choose who can see what you post and share. Privacy settings are usually located under 'Settings' or 'My Account' on devices, apps and websites.

Tips for protecting your privacy online

- Be mindful of who you share your information with and think carefully about who you want to see your posts.
- Be aware of how you appear online by searching for yourself to see what others can find.
- Remember that posts made by your friends can affect your privacy too—anything they share about you becomes part of your digital footprint.
- Regularly review your social media profiles and remove anything you no longer want others to see.
- Delete old accounts, as they may contain photos, videos, or information you no longer wish to share online.

How do children get their identity stolen?

- **Phishing** – is an attack where cyber criminals act as trusted senders to 'fish' for information. They may send fraudulent emails, texts or social media messages to do this. Because attackers can reach millions of people both directly and instantly, this technique is very popular.
- **Doxxing** – is when someone on the internet has posted private information about someone else for the world to see. This information is personally identifiable and therefore sensitive. As such, someone can use it to figure out who someone really is, where they live and how to



contact them.
- Data breaches on the platforms, sites or apps they use.
- Parents oversharing information about their child.
- Children oversharing their own information.
- Sharing passwords or logins with friends.

How to help protect your child

- **Report Identity Theft** - If your child is a victim of identity theft, cyber-crime or fraud, report it to **Report Fraud**. This service is operated by the City of London Police, and it is available for those in England, Wales and Northern Ireland.
  Report Fraud Link: UK's Home for Reporting Cyber Crime & Fraud - Report Fraud
- **Request Image Removal** – If a scammer uses your child's image, contact the social media platform to get it removed. Each social media website has set community guidelines. They outline what actions they take if someone impersonates someone else on the platform. You can also contact the **Report Harmful Content (RHC)** website, which is a national reporting centre that has been designed to assist anyone in reporting harmful content online. RHC is provided by the UK Safer Internet Centre and operated by the South-West Grid for Learning Trust Ltd (SWGfL).
  RHC Link: Submit a Report of Harmful Content for Review
- **Contact Your Child's Bank** – Contact banks, credit card companies or other organisations that hold your child's information to notify them.
- **Track Their Credit** - Contact a credit reference agency (CRA) to request your child's statutory credit report. Most children won't yet have one. However, victims of identity theft might. In the UK, the main CRAs are Equifax, Experian and TransUnion.

Find out more here:

How Can I Help My Teen Not Overshare on Social Media? | Internet Matters

What is Doxxing? Keeping Children Safe Online | Internet Matters

Keeping Kids Safe: Phishing and Ransomware | Internet Matters

COEP Education | Staying Private Online

TEST YOURSELF
PRIVACY AND SECURITY QUIZ

Internet Matters have created a quiz for families to test their knowledge on the subject of privacy and security, and learn how to keep your information and identity from those who would abuse it.

Find out more here:
Introduction to Protecting Personal Information Online | Digital Matters