E-safety Special Feature Newsletter

11 December 2020

WHAT IS ONLINE SAFETY?

Online safety concerns staying safe whilst using online and communication technology. This means not only computers but other ways in which children and young people communicate using electronic media, e.g. smartphones and tablets. This allows children to access and benefit from technology like the internet in the safest way possible without risk to themselves or others.

The aim of promoting online safety is to protect young people from the potential adverse consequences of access or use of electronic media.

HOW DOES HIGHLANDS SCHOOL PROMOTE ONLINE SAFETY?

Students are given guidance on online safety in computing lessons at the start of years 7, 8 and 9. This allows us to establish rules within the classroom and to give age-appropriate advice to the risks and benefits of this type of communication. E-Safety remains an important part of the GCSE Computer Science and IT curriculums and students opting to continue with the subject receive further guidance in key stage 4.

All students and parents/carers at Highlands School sign up to an acceptable user policy for the use of school computers and email accounts. This clearly states what constitutes as acceptable behaviour and the consequences for going against the policy.

Highlands School uses internet filtering and monitoring software to keep students safe online, this technology allows us to prevent access to inappropriate and unsafe websites and to monitor the use of school computers.

We retain the ability to monitor any messages sent from school email accounts and have classroom management software, which allows us to remotely monitor students' screens and to set trigger words or phrases that create alerts. This means we can instantly monitor possible inappropriate or unsafe student behaviours.

Being aware of the specific threats your child might encounter by being online at home can help to keep them safe. These threats include:

- **cyberbullying (bullying using digital technology)**
- **invasion of privacy**
- **identity theft and other online 'scams' - for example "phishing"**
- **your child seeing offensive images and messages**
- **the presence of strangers who may be there to 'groom' other members on social media sites**

Top 5 questions on cyberbullying

1

What is cyberbullying anyway?

For the most part, cyberbullying is bullying, only it happens online or on phones or other connected devices. As for what bullying is, that depends on whom you ask, but most experts agree that it involves repeated harassment and some type of power imbalance and when young people are involved, it usually has something to do with what's happening with peers at school. It's important to remember that not every mean comment or unpleasant interaction rises to the level of bullying. Sometimes it's just what kids call "drama." We mention this because too many kinds of behaviour are called "cyberbullying," which can cause overreaction and inappropriate responses.

2

How likely is it that my child will be cyberbullied?

Some studies say only 4.5% of teens have ever been cyberbullied and others say the figure's as high as 24% (more on this below). Either way, too many students have experienced cyberbullying, but it's important to note that most have not, and most don't bully others. We point this out not to minimize a serious problem, but to emphasize that bullying is not a norm. Kindness, not cruelty, is the norm and, just as with other social problems, communicating the facts reinforces positive behaviours and actually reduces the problem. As for anyone child, it depends so much on the person, his or her peer group and their context. Positive school culture can make a difference, especially for higher-risk populations, such as special-needs students or lesbian, gay, bisexual and transgender (LGBT) youth. For just about all kids, "online" is social – a shared experience – so no single individual has complete control over what happens in digital spaces. Research has found that a child's emotional makeup and home and school environments predict online risk better than any technology he or she uses. Treating others (and oneself!) with respect and kindness can really help keep social media use positive.

3

How do I know if my child is being cyberbullied?

Even if you have a good feel for your kids' emotional state, social skills, and peer relations are key factors in how well their online (as well as offline) experiences go. It's a good idea to ask whether cyberbullying is going on with them or any of their friends. You may not get a clear answer right away, but engage your kids in occasional conversations about how things are going online as well as offline. See what they know about cyberbullying, ask if they know others who have experienced it, if it's a problem at their school and what they would do if they were cyberbullied or knew about others who were. If they seem obsessed about checking text messages and social apps, it could be because they're worried about what's being said about them. It may not be bullying, but it may be a sign your child needs a little extra support. The federal government's StopBullying.gov website suggests that parents be on the lookout for signs such as difficulty sleeping, frequent nightmares, declining grades, not wanting to go to school, feelings of helplessness or decreased self-esteem.

4

What do I do if my child is cyberbullied?

Cyberbullying cases are as individual as the people involved. So the general advice that's all over the Web is not to react or retaliate, block the "bully," and print out and keep evidence in case it'll be needed. But the most important thing to do is talk to your kids about what's going on, help them think through what happened, how they feel about it, and what they're going to do about it. No one knows how to resolve a situation without understanding it fully. It's important to involve your child in the process, not just take over yourself because the main goal is to help them strengthen their self-confidence that might have been shaken and restore a sense of physical and/or emotional safety.

5

5. What if my child witnesses cyberbullying or bullies others?

If your child does experience cyberbullying as a witness or bystander, it's important to talk through some strategies as to how they can help their peers. Being kind goes a long way. Suggest your child sit with a child who's being bullied or invite them to hang out. Your child can reach out to the other child via social media by being positive and supportive. It's not helpful to retaliate online as that rarely influences the person doing the bullying and can put your child at risk. If your child is bullying or cyberbullying others, get them to stop the bullying but try not to overreact. Talk with your child, get all the facts and consider probing further in their devices and accounts. Look for underlying issues and problems that might be affecting your child. While there should be consequences, solutions are more important than punishment.

Digital wellbeing

Young people are growing up in a technological age that brings exciting online opportunities and experiences but it can also bring challenges. It is important that children understand how to use technology in a safe way and appreciate that it can have both a positive and negative impact on their wellbeing. Childnet has produced guidance on how you as a parent/carer can support your child with their digital wellbeing. Click **HERE** for the childnet guidance.

Balancing screen time

Top tips to support children 11-14 (Key stage 3)

HOW ARE CHILDREN USING SCREENS?

As children start secondary school and take advantage of their independence, it's likely that they'll be spending a lot more time on their devices. This is a crucial time to talk to them about how to manage their screen time and give them strategies to find a healthy balance between their life on and offline. Find tips and advice to help them do just that.

5 TOP TIPS TO BALANCE SCREEN TIME

HOW ARE CHILDREN USING SCREENS?

1 Set boundaries to help them build good online habits

Children seek out rules to follow so its best these come from you and not their peers. Set up a family agreement that you all sign up to, to manage expectations of what they should and shouldn't be doing online. These boundaries should help them prioritise sleep, face to face interactions and family time to strike a healthy balance.

2 Stay engaged in what they do online

Take an interest in their digital world to better guide them as they become more socially active online and start to draw from friends and online sources to build their identity. Give them the space to be more independent and build their resilience online to ensure they make smart choices about how they use tech. The more you understand how your child interacts online and check-in with them about their interests and challenges online, the easier it will be for them to come to you if they are concerned or worried about something.

3 Equip them with know-how to manage risks online

Have regular conversations with them about ways to deal with a range of risks that they may be exposed to such as seeing inappropriate content or being cyberbullied. Make sure they know when and where to seek help if they need it and what tools they can use to deal with it. Try to reassure them that you won't overreact if they get something wrong.

4 Give them the space to become digitally resilient

As they get older and more confident in their digital world, it's important to encourage them to be more responsible and aware of how their screen use can impact them and others. Give them the space to thrive online, while also keeping the channels of communications open and being on the lookout for any differences in behaviour that might suggest something isn't quite right is key. It's a tricky time for young people so it's important to equip them with the tools to make smart decisions and ensure they are able to seek support when they need it most.

5 Encourage children to review when and how they use their screen time with tools

Help young people to make use of the screen-time tools that come with their phone. Most children at this age will say that being more aware of how much time they spend is helpful. They will still need some encouragement to make changes to what they are doing and the amount of time they are spending but it's better that they start to discover and monitor this for themselves where possible.

Online challenges and peer pressure

There are frequently online challenges that circulate on social media sites and many raise money or promote good causes such as the 'Ice Bucket Challenge'. However, some of the challenges are more sinister and can entice users into daring, frightening and sometimes harmful activities. Children can be drawn into a challenge through peer pressure, thinking all their friends are completing the challenge so they themselves also need to do so. It can be hard to tell at times if such challenges are real or rumoured but it is important to have a conversation with your child about the importance of saying 'no' to pressure, even from friends, to complete inappropriate and risky challenges and the consequences of taking part in challenges, whether offline or online. Children need to report online content that is dangerous and encourages harm.

TikTok

TikTok, which used to be called Musical.ly, is a social networking app that young people can use to generate and share their own short videos and lip sync to popular audio clips. The app allows users to create and upload videos, remix existing videos using in-built editing tools, and also to view and comment on videos created by other users. On TikTok there is the ability to live stream, users can directly interact with online audiences through chat and live video. Profiles on TikTok are automatically set to public so that any content posted can be seen by anyone within the app. To sign up for TikTok, young people must be at least 13 years of age.

Step Up, Speak Up! Defining online sexual harassment

26% of 13-17 year olds have had rumours about their sexual behaviour shared online in the last year, with 65% saying that girls are judged more harshly for this than boys.

47% of 13-17 year olds have witnessed their peers editing photos of someone to make them sexual e.g. placing sexual emojis over them or adding different faces to pornographic images.

31% of 13-17 year olds have seen their peers create fake profiles of someone they know to share sexual images, comments or messages.

"There was a girl in a photo cuddling a different boy to who she was going out with and its got sent around 2 different schools and everyone was screenshotting it and posted it to their story's saying "slut" or "slag" or "cheater" or "she cant keep her hands off boys lol" - Girl, 13 years

Online sexual harassment is **unwanted sexual conduct** on any digital platform and it is recognised as a form of sexual violence. Online sexual harassment encompasses a wide range of behaviours that use digital content (images, videos, posts, messages, pages) on a variety of different platforms (private or public).

What does the law say?

Protection of Children Act 1978

To take, share or possess a nude or sexually explicit photo of someone under 18 is illegal.

Malicious Communications Act 2003

Sending any form of message, including online, that is extremely offensive, obscene, menacing or indecent can break the law if sent on purpose.

Computer Misuse Act 1990

It can be illegal to impersonate or steal someone's identity online.

Posting photographs of your children

Many parents want to share photographs of their children online with friends and family but it is important to remember that photographs can reveal a lot of information about your child. Ensure that photographs are taken with the location setting disabled. Parents can help children build a positive digital footprint, stressing the importance of only posting photographs and comments that are positive. Many employers and further education leaders do look at candidates' online presence before offering places on a course or a job opportunity.

Setting parental controls

Along with the many positive things which young people may see or experience online, they may also encounter things which may worry or upset them. This could be anything from a scary picture or hateful comment to something which is intended for an adult audience or potentially even illegal content. Setting parental controls can help create a safer online experience for younger children. Internet Matters have created a step by step guides to help parents set up the right controls and privacy settings on networks, gadgets, apps, and sites popular with children. Visit the Internet Matters website for guidance on setting parental controls **HERE**.

Conversation starters for parents and carers

Parental controls and privacy settings can be very effective tools to help minimise the risks your children may face, but they are not 100% effective. It's really important to teach your child skills such as critical thinking and resilience, so they can be aware of online risk and know what to do and where to go for help when needed. Always encourage them to talk to you if anything happens online that worries them or doesn't feel right. Don't miss opportunities to have a conversation with children about using the internet safely, responsibly and positively. Have a look at the conversation starters on the Safer Internet website for ideas **HERE**.

WHAT IS 2 STEP VERIFICATION?

Did you know that 65% of people use the same password everywhere! Leaving themselves wide open. 2 step verification helps you become more secure online. So let's take a look. Firstly it's not new and has been kicking around for a number of years. Most, if not all of the major social media platforms like Facebook, Twitter, Instagram, Snapchat and WhatsApp have a feature within their account security features called 2 step verification or two-factor authentication. In a nutshell, when you enable both parts on your account you add an extra layer of necessary security.

So when you sign in or log in with something you know (the first part of 2 part verification) this is normally your password and something which you nearly always have with you. A code which is sent to your smartphone is the second step of the 2 step verification.

Is 2 step verification only available on social media websites?

Nope. More and more everyday websites which we regularly use, even your email provider, will most likely offer a 2 step verification features you can enable on your account to make it more secure.

How do I set it up?

It differs depending on the website or social media platform you are trying to enable it on. For the most part, it should be available within your account. The idea is, once you have it set up, if you or anyone else signs into or tries to access your account from another PC or device which it doesn't recognize, you will be sent a unique code to your smartphone device which will allow you to log in.

What are the benefits of 2 step verification?

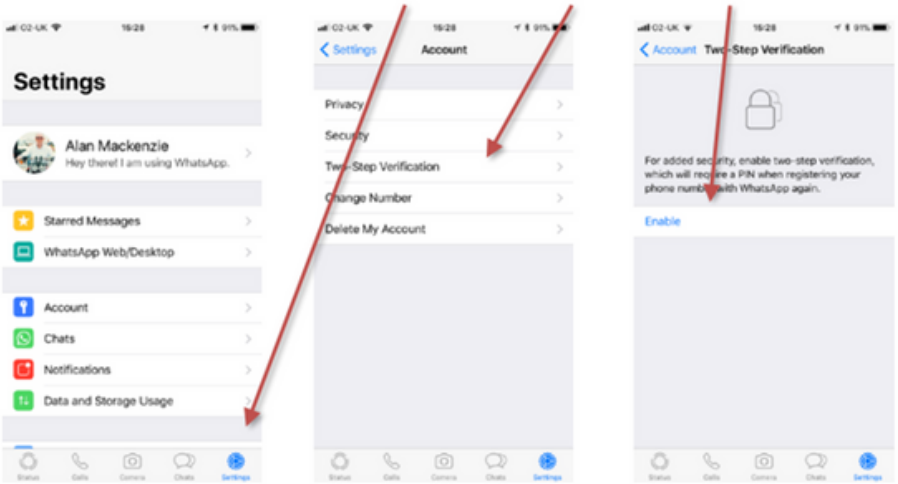
Google 'recent data breaches' and you'll see they're on the rise, particularly for the Under 21's. It's really very necessary to take proactive steps to help keep your accounts as secure as possible and protect your personal information. Hackers, for example, who have gotten your login name and password still can't get access to your account unless they've stolen your smartphone too.

Now don't go thinking that 2 Step Verification is bulletproof. It just makes life harder for hackers and online criminals to breach your account. So that makes it worth doing.

WhatsApp is a hugely popular messaging service, so here is a guide to enabling 2-factor authentication. The following information has been reproduced from the WhatsApp FAQ page (link at the bottom of page):

Two-step verification is an optional feature that adds more security to your account. When you have two-step verification enabled, any attempt to verify your phone number on WhatsApp must be accompanied by the six-digit PIN that you created using this feature.

To enable two-step verification, open WhatsApp > Settings > Account > Two-step verification > Enable.



Upon enabling this feature, you can also optionally enter your email address. This email address will allow WhatsApp to send you a link via email to disable two-step verification in case you ever forget your six-digit PIN, and also to help safeguard your account. We do not verify this email address to confirm its accuracy. We highly recommend you provide an accurate email address so that you're not locked out of your account if you forget your PIN. Important: If you receive an email to disable two-step verification, but did not request this, do not click on the link.

Someone could be attempting to verify your phone number on WhatsApp. If you have two-step verification enabled, your number will not be permitted to re verify on WhatsApp within 7 days of last using WhatsApp without your PIN.

Thus, if you forget your own PIN, but did not provide an email to disable two-step verification, even you will not be permitted to re-verify on WhatsApp within 7 days of last using WhatsApp. After these 7 days, your number will be permitted to re-verify on WhatsApp without your PIN, but you will lose all pending messages upon reverifying - they will be deleted. If your number is verified on WhatsApp after 30 days of last using WhatsApp, and without your PIN, your account will be deleted and a new one will be created upon successfully reverifying.

Note: To help you remember your PIN, WhatsApp will periodically ask you to enter your PIN. There is no option to disable this without disabling the two-step verification feature.

WhatsApp FAQ Link **HERE**.

HELPFUL LINKS

Think U Know: This website contains information for ages 5-7, 8-10, 11-16 as well as parents/carers.

CEOP (the Child Exploitation and Online Protection Centre): A part of the Police Service which helps children stay safe online. If you feel uncomfortable or know someone has also been made to feel uncomfortable when using the internet, you can report it to CEOP.

Childnet: Advice for supporting young children online.

Safer Internet Centre: A website with sections for parents/carers, teacher and young children as well as a hotline advice and to report concerns.

Childline: Offers help to young people who are having problems of any sort, for example: exam stress, bullying, neglect, alcohol, family relationships, school gangs, racism, eating problems, homework and is there if you need to speak to someone. It offers specific advice on coping with the current covid situation.

Advice for Parents/Carers on Cyberbullying: Government advice on how to protect children and steps to take to tackle cyberbullying

HIGHLANDS SCHOOL SUPPORT WITH INTERNET USE AND ONLINE LEARNNG

If you're struggling to help your child with google classroom, click this link **HERE**.
If you need technical, IT or other online learning support email **itstudent@highlearn.uk**.

If you or your child has encountered any issues with online safety, including cyberbullying, or online predators you can:

- Email the schools' safeguarding email outlining your concerns **staysafe@highlearn.uk**. A member of the safeguarding team will contact you within 24 hours to discuss your concerns and to arrange support.
- Safeguarding concerns can also be reported to the enfield MASH (multi agency safeguarding hub) on 0208 378 5555. For further information on how to contact MASH online please click this link **HERE**.
- If your child or someone else is in immediate danger call 999.
- If you need to report a non-urgent criminal matter to the police, call 101.
- Call Childline on 0800 1111.