Cheadle Hulme School

CHS Online Safety Guidance for Parents 2018-19

"Children want their parents to be part of their online life and to talk to them about it, just as they do about their day at school. To children, online friends are real friends. Online life is real life. There is no distinction. Just like in real life, children need our help to stay safe online." - Amanda Azeez, NSPCC Associate Head of Child Safety Online (June 2017).

Not since the printing press has the world seen a technological development as profound as the internet. The ability to access the knowledgebase of humankind from the palm of our hands is remarkable; the ability to communicate on a global stage from the comfort of our homes is shaping minds and societies in ways that are only just beginning to become clear.

Yet like all ubiquitous technologies that weave themselves into the fabric our lives, there are drawbacks as well as advantages.

The concerns held by parents about their sons' and daughters' experience of the internet range from simple overuse to addiction; from distraction to disturbing intrusion; from lack of personal contact to exposure to inappropriate content. Couple this with the lack of technological understanding that many parents freely admit to having and it's no surprise that wonder and anxiety exist in equal measure.

At CHS, we teach students of all ages how to engage with technology in a safe and productive manner, all the while encouraging them to reflect upon the impact technology has upon their lives and the lives of others. We believe students must embrace technology to become more independent and more collaborative learners and we recognise this must be done in a safe and supervised environment.

At school, we monitor closely students' use of technology. Our systems are robust and our teachers and technical services skilled and proactive. Yet we cannot cover every possible eventuality. Be it students' smartphones, tablets or laptops - or their lives beyond our care - there are always going to be times where oversight is minimal.

We seek to address this concern by playing to our strength: *education*.

The School recently formed an Online Safety Forum and conducted online safety surveys with pupils, parents and staff. This, in addition to the technological and pastoral expertise of our staff, has lead to developments with staff training, the Wellbeing and Computing curriculums and the advice and guidance we communicate to parents.

What follows in this document is both a culmination of the work completed thus far and a starting point upon which to build. We hope you find it valuable and welcome any feedback or queries you may have.

Contents

---

1. The School's Online Safety Curriculum

The main risks young people are exposed to when online are:

- Content: being exposed to illegal, inappropriate or harmful material;
- Contact: being subjected to harmful online interaction with other users; and
- Conduct: personal online behaviour that increases the likelihood of, or causes, harm.

Through both the Wellbeing and Computing curriculums, CHS ensures students are exposed to age-appropriate, timely, expert guidance using a comprehensive range of resources and teaching strategies.

The Wellbeing curriculum focuses on the impact technology has on young people; the Computing curriculum focuses on its safe and savvy use - although in practice, there is much crossover. School assemblies may also, where appropriate, tackle relevant issues and reinforce themes covered in the classroom.

There is a great deal of 'implied' good practice embedded into life at the School from strong password requirements to the use of WiFi access keys and mobile-device-management strategies. These combine with the taught curriculum to create a professional and robust culture.

If you would like more information about the specific online safety topics covered in each year group, please contact the relevant *Head of Year* at CHS.

2. The School's Technological Infrastructure

The School monitors use of its network closely, tracking user activity and device activity in a professional, controlled and measured manner. Be it school computers or personal devices connected to the School's network; a broad range of policies, procedures, technologies and staff are in place to ensure the environment students operate within is safe and controlled, without being oppressive or unduly restrictive.

The School's network is protected by a variety of hardware and software measures to ensure data held about staff and pupils is kept safe and secure. Any cloud-based platforms upon which data is held are checked rigorously to ensure they comply with the latest data protection guidelines. Regular data protection guidance is provided to all staff.

If you would like more information about specific technologies the School uses, please contact either the *Director of Technology* or the *Technical Services Manager*.

3. Parental Controls and Device Restrictions Guidance

We understand many parents would like to know which third-party app or software is best to control which device, yet there is unfortunately no simple answer to that question. As devices and their software diversify and evolve, so too do the options for monitoring use of said devices. Some devices are more controllable than others and some products more effective than others. Some solutions are hardware based, others are device-specific and yet more are are able to monitor several devices at once. And, to be clear: some children are more adept at avoiding control methods than others.

What we do advise *strongly* is that parents spend time investigating options in relation to their specific situation and engage in regular and healthy conversation with their children.

The NSPCC have produced **this** excellent page dedicated to the issue of parental controls, with links to various resources related to specific devices. **This** overview by PCMag of current products is also a good starting point.

In terms of very basic yet powerful control methods parents can deploy on their children's devices, we recommend you investigate the options *already built into them*. It is, for example, entirely possible within the Restrictions menu in an Apple iOS device to disable web browsing, iMessage, FaceTime, AirDrop, iTunes, installing apps, in-app purchases etc. Whilst many of these options may seem draconian, they are available and cannot be overridden without a specific password that does not need to be shared with a child. For more detailed guidance, please see Apple's support page **here**.

Similar restrictions on Android devices are a little more complicated to configure and will vary depending on the specific manufacturer of the device e.g. Samsung or HTC. They involve creating a specific account on the device that is hardwired with parental control options. For more detailed guidance, please see Google's support page **here** and **this** comprehensive guide from PC Advisor.

4. Home Network Configuration Guidance

Many internet service providers (ISPs) provide parental control features as part of their monthly package. These vary in terms of features and configuration and we advise you consult your ISP about their specific product. ISP filters are usually 'light touch' and involve blocking access to clearly inappropriate websites. Even high-end web filters are prone to errors, so 'free' ones provided by ISPs should not be seen as infallible.

Please see **here** for more information about ISP web-filters.

For a stricter approach, you may wish to consider using **Media Access Control** (MAC) filtering on your home router. This does require a ***mid-level amount of technical skill*** and there are numerous online resources designed to support such an endeavour.

A MAC address is a device's unique code, rather like a registration plate on a car. It is usually found in the settings menu of a device, although the specific location will vary. If you are unsure, search the internet e.g. "find MAC address iphone". It this scenario, you will notice Apple refer to MAC as 'WiFi Address' in the settings menu, but it means the same thing.

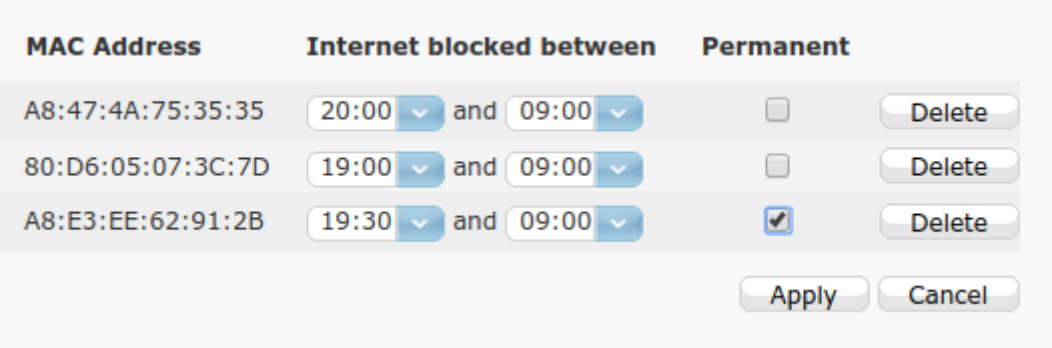
Whatever it is called and wherever it can be found on your device, all MAC addresses look the same: twelve characters appearing in pairs, separated by colons e.g. 26:F6:87:AF:8D:90. Once you have found the MAC address of a device, make a note of the device name, who uses it and the MAC address.

Once you have audited all of the devices in your home, search the internet to find the Internet Protocol (IP) address of the **admin panel** of your *specific* home router. So if you have, say, a BT Home Hub 5, search the internet for "IP address admin home hub 5". If that is your router, you will find the following IP address: 192.168.1.254.

Enter the IP address into the address bar of a web browser on a computer connected to your home network. You will be taken to a login page for that router's admin panel. The admin username and password can usually be found printed on a sticker on the back of your router.

Once you have logged-on to your router's admin panel, look for options that relate to 'access control' or 'MAC filtering'. Again, this will vary from router to router and you may need to search online for guidance.

With the list of MAC addresses from your audit and access to the router's admin panel, you should be in a position to set specific access rules on a device-by-device basis. These rules can usually be timed or permanent. MAC filtering is extremely useful and avoids having to negotiate access times on a daily basis with your child.



You should also consider the devices your child has that have their **own** internet connection via a separate service plan e.g. a mobile phone contract. These devices can connect to the internet **independently** using mobile broadband provided by a cellular network e.g. Three or EE. Any parental controls set by your domestic ISP or set on your home router will **not** apply to these devices if they are connected to the internet using mobile broadband as opposed to your home WiFi signal.

Most parents see the clear benefit of a mobile broadband plan for their child, yet the greater freedom this affords should be considered. You should also consider the fact most mobile broadband plans enable phones to be used as WiFi hotspots, thereby granting internet access to other devices in the home 'through' the mobile phone. Please see the guidance above on parental controls for links to possible options for monitoring internet access on mobile devices using mobile broadband connections.

5. Tips for a Healthy Relationship with Technology

Every home and every family has to find its own balance with technology. What works in one environment may not work in another. It would be unwise for us to lecture parents on what they should or should not do with regards to their child's use of technology.

From the surveys we have conducted, however, we have noted several trends that merit further reflection. We believe the following are points all families should consider in addition to the guidance already provided:

- Review the devices that remain in your child's room overnight and consider making upstairs (where possible) a 'no device zone'. Numerous studies have concluded that use of internet-enabled devices overnight can have a negative impact upon sleeping patterns and, therefore, ability to perform at school.

  "The results demonstrate a negative relation between use of technology and sleep, suggesting that recommendations on healthy media use could include restrictions on electronic devices" - ***http://bmjopen.bmj.com/content/5/1/e006748***

- Be mindful of age ratings on video games. Whilst most parents would naturally not let young children watch an 18-rated film, 18-rated games do tend to fall under less scrutiny. Games used to be rated by the British Board of Film Classification (**BBFC**) and ratings were awarded on a case-by-case basis by experts at the BBFC. Consequently, they were almost always accurate.

New games are rated by Pan European Game Information (**PEGI**) and are done with a self-assessment tick list that game developers complete. If one area of the game falls under a 16 or 18 rating, the entire game is rated at that level.

The net effect is many more games being rated highly, which would perhaps have been rated as 12 by the BBFC. This makes it harder to distinguish between those that really *should* be rated a 16 or 18 and those that are being caught in a bureaucratic dragnet. In other words: just because one 16 or 18-rated game may not '*seem that bad*', please don't think this is the case for all of them. We therefore recommend parents monitor the games their children play beyond a cursory glance or checking the age-rating alone.

- Be mindful and aware of the blogs, vlogs and social media feeds your child subscribes to. In addition to ensuring strict **privacy settings** have been applied on any social media platforms your child uses, it is worth reflecting on the nature of content they follow. The recent online safety survey highlighted the fact many parents are not familiar with the risk of **pro-lifestyle** content, which can have a huge impact upon young people's perception of themselves and of what constitutes 'normality'.

  Pro lifestyle is a broad area covering topics such as **pro-anorexia** and **bigorexia**. All are related to the complex issue of body dysmorphia. Whilst this is not a new phenomenon, the internet and access to blogs, wikis and social media has given rise to greater exposure of this issue - for better and for worse.

  Whilst no small amount of feedback or guidance here could serve to answer all of your questions on this challenging issue, we recommend you engage in healthy discussions with your child about the blogs and feeds to which they subscribe. If you have any concerns, please contact the School's *Pupil Progress and Welfare* team.

6. External Agencies and Further Support

If you would like further information about the issues raised in this document, we recommend the following as excellent, comprehensive resources:

NSPCC - Online Safety Portal
Think U Know - Online Safety Resources
CEOP Parent Zone - Digital World Guidance
UK Safer Internet Centre - Advice Centre
Comparitech - Privacy Guidance

If there any areas of this document you would like further support or guidance on, please don't hesitate to contact the *Director of Technology* or the *Deputy Head (Pupil Progress & Welfare).*