Cheadle Hulme School

Online Safety Guidance for Parents 2025-26

"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. 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 have we seen technological development as profound as the internet. The ability to access humankind's knowledge base from our hands is remarkable. Likewise, the ability to communicate globally from the comfort of our homes shapes minds and societies in ways that are only beginning to become apparent. Yet, like all ubiquitous technologies that weave into the fabric of our lives, there are drawbacks and advantages.

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

At CHS, we teach pupils of all ages how to engage with technology safely and productively while encouraging them to reflect upon technology's impact on their lives. We believe pupils must embrace technology to become more independent and collaborative learners, and we recognise this must be done in a safe and supervised environment.

At the School, we monitor pupils' use of technology closely. Our systems are robust, and our teachers and the Technical Services team are skilled and proactive. Yet, we cannot cover every eventuality. Be it pupils' smartphones, tablets or laptops or their lives beyond our care, there will always be times when oversight is minimal.

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

The School has conducted several online safety surveys with pupils, parents and staff, most recently in late 2021. These data inform developments with staff training, the curriculum, 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 platform 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
2. The School's Technological Infrastructure
3. Parental Controls and Device Restrictions Guidance
4. Home Network Configuration Guidance
5. Tips for a Healthy Relationship with Technology
6. External Agencies and Further Support

---

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 dangerous online interaction with other users and
- **Conduct**: personal online behaviour that increases the likelihood of or causes harm, either now or in the future, due to **reputational damage from historical activity**.

Via tutor periods, The Waconian Programme and external speakers in the Senior School and via L4L and Computing lessons in the Junior School, CHS ensures pupils are exposed to age-appropriate, timely, expert guidance using a comprehensive range of resources and teaching strategies. School assemblies may also, where appropriate, tackle relevant issues.

In addition to the taught components of our online safety provision, good practice is embedded into all aspects of digital life at the School, from solid password requirements to the use of WiFi access keys and mobile device management strategies, which together create a professional, secure and robust digital culture.

2. The School's Technological Infrastructure

The School monitors its on-site network and systems closely, tracking user and device activity in a professional, controlled, and measured manner. Whether 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 pupils operate within is safe and controlled without being oppressive or unduly restrictive.

The School's network and systems are protected by various hardware and software measures to ensure the safe and secure storage of data about staff and pupils. Any cloud-based platforms on 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.

3. Parental Controls and Device Restrictions Guidance

We understand many parents would like to know which third-party app or software is best for controlling which device. Unfortunately, there is no simple answer. As devices and their software diversify and evolve, so do the options for monitoring their use. Some devices are more controllable, and some products are more effective. Some solutions are hardware-based, others are device-specific, and others can monitor several devices

simultaneously. To be clear, some children are more adept at avoiding control methods than others.

We **strongly advise** that parents spend time investigating options concerning their specific situation and engage in regular, healthy conversations with their children about their use of technology.

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

Regarding fundamental 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 vary depending on the device's specific manufacturer, e.g. Samsung or Sony. They involve creating a particular account on the hardwired device with parental control options. Please see Google's support page **here** and **this** comprehensive guide from PC Advisor for more detailed guidance.

4. Home Network Configuration Guidance

Many Internet Service Providers (ISPs) offer parental control features as part of their monthly packages. These vary in features and configuration, and we advise you to consult your ISP about their specific product. ISP filters are usually 'light touch' and block 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.

You may consider using **Media Access Control** (MAC) filtering on your home router for a stricter approach. This requires a ***mid-level technical skill,*** but numerous online resources are designed to support such an endeavour.

A MAC address is a device's unique code, 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". In this scenario, you will notice Apple refer to MAC as 'WiFi Address' in the settings menu, but it means the same thing.

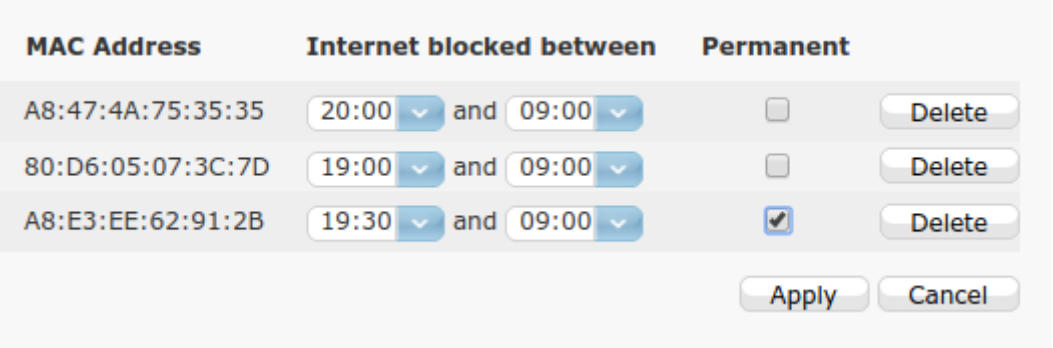
Whatever they are called and wherever they can be found on your device, all MAC addresses look the same: twelve characters appearing in pairs, separated by colons, e.g. 26:F6:87:AF:8D:90. Once you have found a device's MAC address, note the device name, who uses it, and the MAC address.

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 are usually printed on a sticker on the back of your router. We recommend you change this password so children cannot override any settings you apply!

Once you have logged in to your router's admin panel, look for options for '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 able to set specific access rules on a device-by-device basis. These rules can usually be timed or permanent. MAC filtering is advantageous and avoids negotiating access times daily with your child.



You should also consider your child's devices with an internet connection via a different 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 ISP or on your home router will **not** apply to these devices if they are connected to the internet using mobile broadband instead of your home WiFi signal.

Most parents see the clear benefit of mobile broadband plans for their children, yet this affords greater freedom and should be considered. You should also consider that 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 internet access monitoring on mobile devices using mobile broadband connections.

5. Tips for a Healthy Relationship with Technology

Every home and family has to find its 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 concerning their **child's use of technology**.

From our surveys, 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:

- Use this guide to set screen-time limits on Apple devices using **this** guide or on Android devices using **this** guide. We also recommend reading **this** article from the BBC, which contains some very balanced and objective views. Experts say that while there is no evidence to prove that screens are harmful, their use mustn't replace sleep, exercise, and time with family.

- Review the devices in your child's room overnight and consider making upstairs (where possible) a 'no device zone'. Numerous studies have concluded that using internet-enabled devices overnight can harm sleeping patterns and, therefore, the 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***

- We also recommend that students, particularly younger ones, do their homework in the kitchen or other family space to ensure appropriate supervision and support at home.

- 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 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 that many more games are rated highly, which would have been rated as 12 or 15 by the BBFC. This makes it harder to distinguish between those that *should* be rated an 18 and those caught in a bureaucratic dragnet. In other words, just because one 18-rated game may not '*seem that bad*', please don't think this is the case for all of them. We, therefore, recommend that parents monitor the games their children play beyond a cursory glance or by 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 the content they follow. The recent online safety survey highlighted that many parents are not familiar with the risks of **pro-lifestyle** content, which can significantly impact young people's perception of themselves and 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 have 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
UK Safer Internet Centre - Advice Centre

Who should I contact if I have any queries?

Technical enquiries:	Mark Smith **marksmith@chschool.co.uk** *Technical Services Manager*
Teaching & Learning enquiries:	Luke Dunn **lukedunn@chschool.co.uk** *Director of Technology*
Pastoral enquiries:	Susan James **susanjames@chschool.co.uk** *Deputy Head (Pupil Welfare)*