Holmewood House Device Advice

Bring Your Own Device (BYOD) September 2023

This guidance is provided to support parents with ensuring that the device they supply their child with for September 2023 is safe and suitable for use in school and at home as a key tool to support their learning. Should you have any further questions, please contact your child's form teacher.

1. Device compliance – standard modern hardware

a) Windows based devices should have a minimum of:

Intel Core i5 8th Gen processor or AMD Ryzen 5

8GB RAM

Windows 10 ver 21H1 (May 2021) & securely updated to present day security fixes

b) MacBooks should have a minimum of:

macOS Sierra – Version 10.12.06

Processor: Intel Core i5 8th Gen or Apple M1

c) iPads should have a minimum of:

iOS 14

32GB storage with 16GB free

A keyboard cover

The following devices are not supported:

Android tablets

Chrome Books or devices running ChromeOS

2.

a) Security Compliance – Standard Anti-Virus/Anti-Malware

In terms of Anti-Virus and/or Malware, the Windows Defender app built-in to Windows 10 & 11 will be sufficient. Apple products are far less susceptible to malware and so this is not a requirement.

b) Security Compliance – Standard Operating System Updates

Other devices need only have the latest updates from their respective providers. For example:

Apple devices:- IOS version update/Apple Store for app updates

Microsoft:- Microsoft Store Updates, Microsoft Security Updates (usually automatic), Microsoft platform updates.

3. Parental Controls

In order to support our pupils in complying with the school's acceptable use policy when they are using their device in school, we strongly recommend that parents apply parental controls on pupil devices to ensure that the material accessed at home is appropriate. We would recommend the following options:

a) Apple Parental Controls - With Content & Privacy Restrictions in Screen Time, you can block or limit specific apps and features on your child's device. You can also restrict the settings on your iPhone, iPad or iPod touch for explicit content, purchases and downloads, and privacy.
https://support.apple.com/en-gb/HT201304
b) Microsoft Family Safety - Set screen time limits that apply to devices, apps, and games. When screen time runs out, choose to add more or not, based on what's right for you and your family. App and game limits (Windows, Xbox, Android), Device limits (Windows, Xbox), Screen time requests, Activity summaries.
https://www.microsoft.com/en-us/microsoft-365/family-safety
c) Google Family Link - Allows parents to control and monitor any device that uses sharing access to your child's Gmail account. It helps you to monitor their internet browsing via Chrome, what apps or games they can install and allows scheduled time limits per app with a scheduled device lockout at bedtime.
https://families.google.com/familylink/

Overall Compliance

VPNs
The use of devices offers significant opportunities for the children's learning, but we also have to be mindful of all the potential safeguarding concerns associated with individual device usage. We want all the children to be responsible and safe online and there is a collective responsibility to protect them, educate them and to safely provide a secure experience of the

'online' world. We will continue to teach internet safety and support pupils with developing these key online safety skills.

Holmewood has a very secure 'Smoothwall' web filter to help protect and monitor what the children can access online and to help them adhere to the guidelines outlined in the 'Acceptable Use of Technology – ICT policy'.

Some pupils may add their own VPN (Virtual Private Network) to their device, allowing them to circumnavigate the school 'Smoothwall' and freely access the internet. We ask that parents frequently check pupil devices to ensure VPNs have not been downloaded at home so that pupils are accessing the internet safely via the school network when in school. Similarly, the school will carry out spot checks of devices to review that device are being safely used via the school network only. This is further supported by a daily check of searches filtered by the school's Smoothwall.

4G access

Some pupils' devices have their own 4G connection. If your child's device has 4G, we would ask that this is disabled so that the device accesses the internet via our secure network only. We ask that devices with 4G are accessed in a 'sim only' manner as 4G usage means we cannot safeguard pupils online, monitor access to inappropriate websites or material and protect pupil devices from malware.

If your child is found to be using a VPN or their own 4G (or remote) connection, the School will need to remove the pupil device.

For children to abide by our acceptable use policy when they use their devices in school, it is important that we work in partnership with parents to help monitor the material accessed and downloaded on pupil devices and then bought into the school on the device. Devices in school will be used with an adult in the room but ensuring reduced access to potentially harmful content at home will be crucial to us facilitating the safe use of devices to further pupil learning when in school. If you require further support with this, please contact your child's form teacher.