HILL HOUSE SCHOOL

Bring Your Own Device (BYOD) Policy for Pupils, Staff and Visitors.

Introduction

The school recognises that mobile technology offers valuable benefits from a teaching and learning perspective. Our school embraces this technology but requires that it is used in an acceptable and responsible way.

The below details acceptable behaviour and technical specifications required to take part in the school's BYOD scheme.

Acceptable use policies

This policy works in conjunction with the school's existing acceptable use policies for pupils, staff, parents, governors and visitors.

Details below set out where this policy extends the existing AUP with respect to the school's BYOD scheme.

The right of the school to exclude devices

If a device is deemed not of the correct technical specification, is running prohibited software or settings or used in a manner contrary to any other school policy the device may be confiscated and users asked not to return it to school.

Devices that do not operate at acceptable levels of performance or require disproportionate levels of support from staff may be excluded from use.

Types of devices

The school uses Google Classroom and expects that any devices brought into school should be able to work in this context. As such the school is placing certain restrictions on the types of devices that are acceptable for use in school. Appendix A contains current detailed technical information that should help families, pupils and teachers when choosing devices.

Certain subjects at GCSE or A-Level may have further restrictions on the types of devices that can be used. Please refer to Appendix A for more information.

Cybersecurity

The school takes cybersecurity very seriously. Devices brought into school should comply with all other school policies (notably the school's data protection policies in this respect). In addition, devices are required to have the below cybersecurity measures implemented as a minimum;

- Anti-virus software installed, active and up to date.
- Personal firewall installed and active.
- Access control (authentication methods) such as password, PIN number or biometric technology.

If a device is found to damage the devices of others, by viruses or software etc that has been deliberately placed on it, the repercussions may include suspension or expulsion.

The school provides access to Google cloud technologies and it is expected that wherever possible pupils and staff make use of storage on this platform. Data stored 'locally' on a device may be lost if a device is stolen or damaged. The school cannot backup any BYOD device.

Staff should also carefully adhere to the school's data protection policies with respect to the storage of data on devices. Wherever possible data should be stored in either the school's Google cloud or school servers. If data must be stored locally on a device that device must be protected in adherence with the school's data protection policy; be protected by access control and encryption.

Storage on USB memory devices is strongly discouraged and in the case of personal data must be protected by encryption if used.

In the case of BYOD devices that are shared by more than one user individual accounts should be created for each. This will limit the risk of accidental deletion of data or data breaches.

As final responsibility for the protection of personal data rests with the school, the school demands users adhere to its data protection policies. Where the school believes a user has not adhered to this policy it may take actions to legally rectify and protect its personal data. Staff are required to remove all personal data from devices upon completion of their employment with the school.

Physical security and protection

Pupils, staff and visitors will be responsible for looking after their device while in school. Users should provide adequate protection (such as carry cases etc) to protect the device over the course of the day and transport to and from school. The school will provide locations for devices to be stored while not in use.

While the school will endeavour to help pupils in the care of their device the school will not be responsible for devices being mistreated, lost or stolen.

Pupils who deliberately damage the devices of others will be treated in accordance with the school's current policies covering vandalism, theft etc. The school will not be liable for costs of damages or loss caused by pupils to either their own or others' devices.

Liability & insurance

Families, staff and visitors are expected to provide insurance for their devices. This can be provided under a family's existing home insurance or via products tailored for mobile technology (e.g. via the Post Office or other 'gadget' insurance providers for example).

The school will not cover pupils, staff or visitors devices under its insurance.

Internet access, child protection and monitoring devices

This policy works in conjunction with the school's other policies concerning safeguarding and taking, storing and using images of children.

The school will provide Internet access that is monitored and filtered. This is for the protection of pupils, staff and visitors and to comply with the school's regulatory requirements.

The school will monitor all network traffic by each device to both protect pupils and prevent breaches of its existing policies.

Users must use the school's authentication methods when accessing the Internet at school. Attempts to circumvent the filtering or monitoring technology via proxy avoidance, VPNs, mobile networks or by using other users' credentials is forbidden.

The school reserves the right to inspect pupils' devices if it believes there has been an infringement of this or any other of its policies.

Lease scheme for devices

The school operates a device lease scheme to provide pupils access to devices if required.

Families have the option to lease a device over the course of 3 or 4 years with the option of purchasing the device outright at the end of the term.

The range of devices available and exact details will vary depending on the year group and subjects being studied by the pupil.

Further details can be found by contacting it@hillhouse.doncaster.sch.uk.

Support & access to the school's IT services

The school will provide the required infrastructure and computer accounts to allow access to school curricular content, Internet access etc.

The school will also provide access to its IT services for support. These services will be provided on a 'best effort' basis and operate under the below restrictions;

- The IT department will not invalidate warranties. If a device needs to be fixed in any way that the IT department suspects will invalidate any warranty it will require written notice to do so.
- The IT department can only devote 'reasonable' resources to your device. If the repair of a device is likely to consume excessive physical or human resources the school reserves the right to refuse to carry out the work.
- In such circumstances that a repair cannot be reasonably made by the school, the school will offer a temporary loan of a device. The duration of this loan will be at the school's discretion. Loans that are likely to extend beyond this will be treated under the school's 'device lease' scheme and will be chargeable.

Wellbeing

To support pupil wellbeing devices must only be used when directed by teaching staff. At break and lunchtimes devices are to be safely stored and may only be accessed by pupils in Year 11 and the Sixth Form for the purposes of private study. Exceptional arrangements may be made for younger pupils on a needs basis.

September 2021

Appendix A - Acceptable devices

For lessons to be conducted in an as efficient and effective manner as possible the school is placing certain requirements on devices allowed onto the scheme. These requirements will reduce the impact of solving technical problems and allow teachers to concentrate on lesson content.

The school expects that each device brought into school should be able to access the below services;

Google Cloud Services; • ***Google Classroom*** • ***Google Docs*** • ***Google Sheets*** • ***Google Slides*** • ***Google Meet*** • ***Google Forms*** • ***Google Jamboard***	This is the core set of services used by the school for education. Only an internet browser such as Chrome or Firefox is needed to use these.
The school's OneDrive and Microsoft Office 365 environments.	The school-wide licence covers pupils for usage of Microsoft Office 365. This can be accessed via an internet browser. Pupils with windows or Mac devices can also download Word, PowerPoint and Excel under the school licence.
Access to shared drives via 'foldr' or the online 'shared drives' system	These systems require only a browser to work (Chrome, Firefox, Safari, Edge etc.).
PhotoShop (if taking Art GCSE / A-Level)	If taking Art GCSE or A-Level the device will need to run PhotoShop (the school will provide a license).
Sibelius (if taking Music GCSE / A-Level)	If taking Music GCSE or A-Level devices need to run Sibelius.

Devices should have as a minimum the below technical specifications/features;

Screen	Greater than 12” Screen (touch preferred but not required)
Physical Keyboard	
Pointing device or touch screen	E.g. mouse or trackpad (separate or integrated)
Webcam	
Wifi	
Microphone	
Inbuilt speakers and headphone socket	Pupils should provide their own headphones. Please avoid using bluetooth sets.
Local Storage	Volume is dependent on the device. 32GB minimum for Chromebooks. 128GB minimum for Windows and Mac. SSD Drives are preferred but not required
Processor	CPU is dependent upon device type. Windows 10 - i3 or similar minimum (i5 recommended) Mac devices - i3 or similar minimum (i5 recommended) Chromebook - AMD A4 or Intel N4000 minimum
RAM	Min 4GB RAM. Ideally 8GB
Battery life	8 Hour min.

Prohibited hardware, software and settings;

Cellular networks (3G / 4G / 5G etc)	Devices should use only the school wi-fi when connecting to the Internet at school.
iPads/Android tablets	Tablets present significant overheads in terms of teacher and support staff in enabling them to work effectively in a school environment.
Linux distros designed for hacking	i.e. Kali (running as a virtual machine or as the native OS).
Photosharing	Due to safeguarding concerns pupils must disable photo synchronisation between devices.

Devices should be protected by basic levels of security, including;

Anti Virus	Note that many antivirus software products currently provide VPN technology. While VPN technology does provide protection in public locations its use can prevent content filters from operating both at home (via BT parental controls for example) and at school. The school implements measures to prevent VPNs operating within school where possible for this reason. We recommend parents disable antivirus VPN while at home if you use parental controls and we insist it is disabled while at school.
Personal Firewall	Windows OS, Chrome OS and Mac OS contain built-in firewall features. Please ensure they are configured correctly.
Authentication methods	Password, PIN or biometric.

Settings and configuration.

The below settings should be adhered to for devices entering school;

IPv4	Devices need to use IPv4
DNS	DNS and IP settings need to be set to dynamic.

Proxy Avoidance	Forbidden
Tor Browser	Forbidden
Peer to peer file sharing	Peer to peer file sharing is not permitted (Bittorrent etc)

Devices that adhere to the above requirements;

Microsoft Windows 10 Laptops	No Windows XP, Windows 7 or 8. Must be running Chrome and Firefox.
Apple Devices;	MacBook (Air and Pro). Must run Chrome and Firefox
Chromebooks	

Given the requirements of Art and Music, we would recommend the use of a Microsoft Windows 10 or Mac OS device if taking either of these subjects at GCSE or A-Level.

Example devices

Below are examples of devices that comply with this policy and the school's curriculum requirements.

Please note these are only for illustrative purposes. Prices and deals may not be available and the school has no financial ties with the suppliers listed below.

Windows 10 devices;

HP ProBook 450 G7 15.6" - Core I5 10210U - 8 GB RAM - 256 GB SSD - UK (£680.39 inc vat @ Insight UK)

Lenovo V15-IIL Core i5-1035U 8GB 256GB SSD 15.6 Inch FHD Windows 10 Laptop 82C50075UK - (£ 520 inc vat @ Laptops Direct)

Acer Aspire 3 A315-54 15.6 Inch Intel Core i3 – 1TB HDD (£379.00 PC World) Asus Vivobook i4 – Intel Core i3, 4GB Ram 128GB SSD (£349.99 John Lewis)

Apple Products

Apple MacBook Air and Pro devices.

Chromebooks;

Lenovo 14e Chromebook - 14" - A4 9120C - 4 GB RAM - 64 GB - UK (£ 324 inc vat @ Insight UK)

Antivirus software

The below antivirus software packages will comply with this BYOD scheme;

Trend Micro Antivirus+
Bitdefender
ESET Internet Security
Malwarebytes Premium
Sophos Home
Webroot Antivirus / Internet Security / Internet Security Complete
F-Secure Antivirus
Avast Free Antivirus